01 Nov 2008

Localizing Sensor Networks in Un-friendly Environments

Sriram Chellappan
Missouri University of Science and Technology, chellaps@mst.edu

Vamsi Paruchuri

Dylan McDonald

Arjan Durresi

Recommended Citation

S. Chellappan et al., "Localizing Sensor Networks in Un-friendly Environments," *Proceedings of the IEEE Military Communications Conference, 2008*, Institute of Electrical and Electronics Engineers (IEEE), Nov 2008.
The definitive version is available at https://doi.org/10.1109/MILCOM.2008.4753635

LOCALIZING SENSOR NETWORKS IN UN-FRIENDLY ENVIRONMENTS

Sriram Chellappan, Vamsi Paruchuri, Dylan McDonald and Arjan Durresi

Abstract— **In this paper, we study the issue of defending against a Wireless Sensor Network (WSN) that has been deployed by a malicious enemy agent in an area of interest to us. While there can be many approaches to defend against maliciously deployed WSNs, we propose the design of a localization centric approach. Specifically, the problem we address is: Given an enemy deployed WSN in an area of interest to us, how can we determine locations of the sensors without co-operating with the sensors themselves during localization. In our approach, we employ a physically mobile agent called the *localizer* (e.g., a mobile robot) to move in the sensor network and detect raw sensor-to-sensor communication signals. However, the *localizer* has no information on the message content or the sensor id of any signal (possibly due to message encryption) since the sensors belong to an enemy agent. Based on estimating the angle of arrival and the received signal strength, we design a protocol for the *localizer* to determine sensor positions. The salient features of our protocol are efficient association of signals with sensors, and filtering many likely false locations over time. Sound theoretical analysis and extensive simulations are used to demonstrate the performance of our protocol from the perspective of localization accuracy.**

Index Terms— **Sensor Networks, Localization, Security.**

I. INTRODUCTION

Wireless sensor networks (WSNs) have become a critical component of many military missions today. Some canonical instances include battlefield monitoring, border patrol, installations protection, seismic monitoring etc. A vast amount of theory has already been invested in WSN technologies, and numerous test-beds have been designed and practically validated in military settings. The unifying conclusion after all these efforts is the clear and patent viability of WSNs to fulfill numerous military needs in the near future and beyond. While this is clearly an encouraging development, a view from the other side of the military fence is still lacking today. In other words, the issue of how a network of sensors can be deployed and operated by malicious adversaries, and how to defend against such threats has so far lacked enough attention.

Sriram Chellappan and Dylan McDonald are with The Dept. of Computer Science, Missouri University of Science and Technology (formerly University of Missouri - Rolla), Rolla, MO 65409, U.S.A. E-mail: {chellaps, dlmyr8}@mst.edu. Vamsi Paruchuri is with The Dept. of Computer Science, University of Central Arkansas, Conway, AR 72035, U.S.A. E-mail: vparuchuri@uca.edu. Arjan Durresi is with The Dept. of Computer Science, Indiana University Purdue University, Indianapolis, IN 46202, U.S.A. Email: durresi@cs.iupui.edu.
978-1-4244-2677-5/08/$25.00

A. Our Contributions

1. A case for defending against maliciously operated WSNs: Our first contribution in this paper is the illustration of the threat imposed by maliciously operated WSNs. In many missions of late, military personnel are being routinely employed in enemy battlefields with minimal prior knowledge of threats imposed in such fields. Traditional threats included landmines, IEDs, sniper fires etc. However, with the advances in sensor network technologies, and coupled with their wide dissemination and acceptance, it is quite reasonable to envisage a wireless sensor network employed as a threat against military personnel in terms of monitoring their movements, triggering explosives, notifying enemy agents etc. Another representative threat occurs when enemy agents seize control over critical infrastructures in war zones like oil-fields, airports, power plants etc. and deploy a sensor network to guard such infrastructures. How to defeat such types of maliciously deployed WSNs is our focus in this paper.

We point out that there is more than one approach to defeat a maliciously operated WSN. In simple terms, the network can be bombed with missiles, hence destroying the whole network. Alternative approaches include driving a tank through the network to crush sensors, sending soldiers to hand-pick sensors etc. Such approaches suffer from two fundamental problems. First, there is a lack of sufficient stealth during defense. Attempts to bomb a network, or to physically destroy/ remove sensors can be easily exposed to adversaries and may incur counter-reactions which must be avoided. Secondly, bombing a network incurs a large amount of physical force, which is cost-prohibitive and also may cause irreparable damages to the deployment field which we may need to protect (e.g., oil-fields, airports, power-plants etc.). On the other hand, a passive countermeasure is to listen to the message content of the sensors and leverage it to design subsequent defense strategies. However, it may be likely that the sensors (that belong to an enemy agent) encrypt their messages. Discovering keys and encryption protocols must entail breaking into and capturing sensors which

again violates the stealth requirement. The crux of this paper is the design of a mechanism that can cause a high degree of destructive potential to maliciously operated sensor networks, while still maintaining a sufficient degree of stealth during execution.

2. A localization centric defense approach: In this paper, we design a localization centric approach to defend against maliciously deployed sensor networks, where the goal is to determine the locations of adversarial sensors in the network. Many advantages are present when locations of adversarial sensors are known. For instance, number of nodes in the network can be estimated which can help gauge adversary strength; optimal intrusion paths involving minimal detection through the network can be determined, the topology of the network can be estimated which can assist in coordinated and maximal impact counter-measures against the network.

In this paper, we employ a physically mobile agent called the *localizer* (typically a mobile robot), which will stealthily move in the network listening for sensor-to-sensor communication signals. The *localizer* will attempt to measure the Angle of Arrival (AoA) and the signal strength of the sensor signals (RSSI). However, the *localizer* will have no information on the message content or the id of the sensor sending the message (potentially due to message encryption). Using this information, we design a protocol for the *localizer* to estimate sensor locations in the network. At the initial stages of the protocol execution, crude location estimates are derived. Since, the *localizer* does not know which sensor is sending which signal, there will be many false estimates during localization. We then incorporate a novel location scoring mechanism with a corresponding score translation mechanism, such that with the reception of more and more sensor signals, the protocol will filter out many false positives and gradually converge to real sensor locations.

3. Theoretical analysis and simulations: We conduct a detailed theoretical analysis and extensive numerical simulations to demonstrate the performance of our protocol. Our analysis demonstrates that the localization protocol can effectively determine adversarial sensor locations. Also, we demonstrate that when the *localizer* has additional information on network behavior like transmission ranges and communication model, the localization accuracy dramatically improves.

The rest of our paper is organized as follows. In Section II, we review important work most related to the work in this paper. The sensor network and localizer model are presented in Section III. In Section IV, we present our localization protocol, and detailed theoretical analysis. Our performance evaluations are presented in Section V. We conclude our paper with final remarks in Section VI.

II. Comparison with existing works on security in WSNs

As we can see, defending against maliciously deployed WSNs clearly falls under the purview of security. A pertinent question to ask here is how different are existing works in sensor networks security from the work in this paper. In all existing works on WSN security, the unifying framework is that the sensor network belongs to benign entities. The role of the adversary is to disrupt the network operations. Typically, the standard attack model used in existing WSN security works is where the adversary captures a small percentage of network nodes that then behave maliciously. How to harness the potential of a relatively large number of benign sensor nodes to defeat the malicious operations of a few compromised sensors is the major theme in existing WSN security research. Instances of works in the framework include secure key management [1], [2], [3], [4], [5], [6], location verification [7], [8], [9], [10], [11], secure localization [12], [13], [14], [15], [16], secure routing [17], maintaining integrity of sensor identities [18] etc.

Differences between the above works and ours: In this paper, the sensor network under consideration belongs to the adversary. Our problem is to defeat the operations of an *entire network* of sensors and not just a few sensors in the network. Furthermore, we will have virtually no information on any aspect of the network or its operation characteristics. Consequently, approaches that leverage knowledge of the network behavior, and/ or the presence of a large number of benign entities cannot be leveraged as a defense mechanism. An added challenge is the requirement of stealth in the defense mechanism which makes our problem quite harder from existing problems in WSN security.

Recently though, Yang et. al. in [19] have studied a similar problem where the goal is to localize sensors in a network deployed by an adversary. In their solution, a set of monitors are deployed at the boundaries of the network to receive sensor signals and localize sensors. Deploying such monitors can be an expensive operation. Furthermore, it is assumed that *all* monitors can listen to *all* the communication signals of *all* sensors which is impractical for large area networks. Furthermore, in [19] it is assumed that the monitors are aware of the initial transmission power of all sensors in the network. This information is possible to obtain only if the monitors have insider information on the sensor network (obtained possibly by breaking into sensor nodes) which violates the stealth concept that we believe is critical. In this paper, we design a new approach for localizing maliciously deployed sensors using a physical mobile agent moving in the network, and collecting sensor signals. Our approach does

not need any expensive equipment, global network view, or *insider* information on the sensors/ the network.

III. Localizer and Network Model

In our problem there are two competing entities: the sensor network and the localizer. In this section, we present the models of both entities from the perspective of their features and capabilities.

A. Sensor Network model

In our problem, we consider a sensor network that has been arbitrarily (not necessarily uniformly) deployed with N sensors by an adversary in the area of interest. For simplicity, we assume that the network is square shaped of dimensions $L \times L$. The sensors in the network communicate with each other via encryption, with the communication messages either being *Hello* messages or other network activities. Each sensor is assumed to transmit at the same initial transmit power, P_{tx}. Note that P_{tx} is unknown to the localizer.

The traffic model of the sensors depends on the network application and the behavior of sensed events. The data reporting process in WSNs is usually classified into three categories: event-driven, time-driven and query-driven [20]. In the time-driven case, sensors send their data periodically to the sink. Event-driven networks are used when it is desired to inform the data sink about the occurrence of an event. In query-driven networks, sink sends a request of data gathering when needed. In this paper, our main focus will be on the event-driven networks with Poisson model for packet generation. Suppose that the events are independent (both temporally and spatially) and occur with equal probability over the area. In this case, Poisson distribution can be used effectively to model the generation of data packets [21]. When the average rate of packet generation, λ, is known, the distribution of the number of data packets, Z, generated by each node, from time 0 to T is

$$P\left(Z=z\right)=\frac{e^{-\lambda T}\left(\lambda T\right)^{z}}{z!} \tag{1}$$

where z is a nonnegative integer. In the case of the packet generation distribution obeying the Poisson model, the time duration between two consecutive packet transmissions, t, has an exponential distribution with mean $\frac{1}{\lambda}$:

$$f_{t}\left(x\right)=\lambda e^{-x\lambda}u\left(x\right) \tag{2}$$

where $u(x)$ denotes the unit step function. We will consider a Poisson sensors traffic model in this study. In this paper, we assume that the sensors are all static. Studying the issue of localizing mobile sensors is a part of future work.

B. Localizer Model

The localizer in our problem is a mobile agent that can physically move from one location to another. For practical purposes a miniature robot serves this purpose. The localizer is equipped with the capability to measure angle of arrival (AoA) and received signal strength (RSSI) of a source signal. Note that AOA measurements typically require either an antenna array, or several ultrasound receivers. This is currently available in small formats in wireless nodes such as the one developed by the Cricket Compass project [22] from MIT. We assume that the localizer can detect any signal it receives provided the received power level is $\geq \bar{P}_{rx}$, the localizer's receiver threshold. We assume that the localizer is aware of the network boundary within which it wishes to localize sensors. In this paper, we assume that the sensors deployed are not equipped to track mobile intruders. Localizing sensors that are equipped with the ability to track intruders is part of our future work.

IV. Our Localization Protocol

In this Section, we present our localization protocol. The protocol is executed in three phases: The estimation phase, measurement phase and the localization phase. Each phase is discussed in detail below. For reader's convenience, important notations and their terminologies are presented in Table I.

TABLE I
Important Notations and Terminologies

Term	Description
θ	Sensor angle of arrival measured by Localizer in $degrees$
ϵ	Error bound in angle of arrival measured by Localizer in $degrees$
$L \times L$	Total network area in m^2
$M \times M$	The area to be localized m^2
$g \times g$	Total number of grids in the network
$d=\frac{M}{g}$	Grid size in m
N	Number of Sensors
T_x	Actual transmission range of sensor
$\bar{T}_x$	Estimated transmission range of sensor
λ	Packet inter arrival rate

A. Initiation phase

Without loss of generality, we assume that the localizer has to localize a square area of size $M \times M$. Note that when $M = L$, the area to be localized is the entire sensor network deployment area. The *localizer* initially divides the area of interest into a $2-$D rectangular grid ($g \times g$)

where each grid is a square of dimension of size $d = \frac{M}{g}$. The objective of the localizer is to eventually determine those grids that contain atleast one sensor in them. The size of the grid is an application parameter and is variable. For high accuracy of localization, d can be set quite small, while for lower accuracies, d can be set correspondingly larger.

Observation time

The localizer traverses the entire network area, stopping at each intersection of vertical and horizontal grid lines. The time spent at each observation point (T_{obs}) is chosen such that the localizer can observe at least one transmission from each node in the neighborhood. Thus, T_{obs} depends on the underlying traffic pattern. For instance, for a Poisson model with rate λ, a $T_{obs} = \frac{10}{\lambda}$ would ensure that the localizer is able to observe messages from a particular sensor in the neighborhood with a probability of atleast 0.99995 (from equation 1). Waiting for longer durations improves this probability further. For scenarios where λ is not know apriori, we outline a simple method for obtaining a rough estimate. The localizer at various random locations observes the packet intervals from multiple sensors. This average packet interval multiplied by the average number of neighbors (which is again an estimate at different locations using the AoA) gives an approximate value for λ. We again note that waiting for longer durations only improves the accuracy of localization; thus, overestimating inter-packet arrival time is more helpful than harmful and an accurate estimate is not required.

Note that it is not compulsory that the sensor traffic model is Poisson. In scenarios where the traffic model is not Poisson, similar to the above approach, the localizer can estimate mean (μ_T) and standard deviation (σ_T) of inter-packet arrival times. We can then use Chebyshev's inequality, which states that "in any data sample or probability distribution, no more than $\frac{1}{k^2}$ of the values are more than k standard deviations away from the mean" [23]. Thus, the localizer waits for $T_{obs} = \mu_T + k \times \sigma_T$ (where $k = 6$), ensuring it observes a message from a sensor in the neighborhood atleast 97.2% of the time, where μ_T and σ_T are the means and standard deviations of the distribution respectively.

Transmission power and Range of the sensors

Recall that the the $Localizer$ is un-aware of the initial transmission power (P_{Tx}) of the sensors. To estimate P_{tx}, the following approach is used. The $Localizer$ as usual traverses the entire network, listens to various messages and collects information regarding angle of arrival and received power P_{Rx}. We note that the observation points of the localizer are randomly chosen with respect to the locations of the sensors. We compute the probability of receiving a message from a node very close to the localizer. We note that $closeness$ here is relative to the sensor's *transmission range* T_x, which is again an unknown. First, when a message is received, the probability that the source is within 5% of T_x (again, T_x is unknown) can be computed as

$$P_{5\%} = \frac{\pi \left(0.05T_x\right)^2}{\pi {T_x}^2}. \tag{3}$$

Thus, the probability that the source is not within 5% of T_x is $\bar{P}_{5\%} = 1 - P_{5\%}$. Further, if the localizer receives m messages, then the probability that atleast one message was transmitted by a node within $0.05T_x$ can be computed as $1 - \bar{P}^m_{5\%}$. For example, if 1000 messages were observed during the entire process of localization, then the probability that atleast one message was transmitted by a node within $0.05T_x$ is 0.92. For a network of sufficient scale, these many number of messages is actually quite reasonable for the localizer to have listened to during the entire process of localization. Finally, based on the above reasoning, we use the maximum receiving power observed over all the messages as approximate receiving power at a distance of $5\%T_x$, based on which the transmission range T_x can be estimated.

Once, the transmission power is estimated, the upper bound of the transmission range ($\bar{T}_x$) of the sensors can be estimated. We note that, in practice, wireless transmissions are not circular and for several uncontrollable reasons, the attenuation cannot be accurately estimated [24]. However, from our protocol's perspective, we are only interested in the upper bound. Again, if the attenuation is varying drastically, the upper bound might not be tight; however, this will only cause a slight drop in protocol performance. Further, to improve the performance, we propose to consider only the messages received with a signal strength above a given threshold. We elaborate on this later in this Section.

B. Localization phase using only AoA

Our localization protocol is comprised of two phases: A grid score assignment phase and a score translation phase, as described in Algorithm 1.

First, the *localizer* starts by traversing the entire grid, stopping at each intersection of vertical and horizontal lines. At each stop, the localizer listens for messages. In this paper, we propose the localizer to listen for a duration of $10/\lambda$ to ensure that atleast one transmission from each sensor in the neighborhood is observed with high probability, where λ is the packet arrival rate assuming Poisson distribution.

For each message received, the *localizer* stores the following information: the angle of arrival, received signal strength (RSS) and *localizer*'s location. Based on AoA information (i.e., θ) and the estimated transmission range

($\bar{T}_x$, as estimated earlier in the section), the *localizer* computes the sector that would enclose the transmitting node. We also refer to this sector as the *zone* that would enclose the transmitting node.

Once a $zone$ is computed, the *localizer* assigns grid scores as follows: For each grid $G_{i,j}$ that overlaps with the $zone$ Z_k corresponding to a message transmission k, the grid score $p_{i,j,k}$ is the probability that the node corresponding to message k is located in the grid $G_{i,j}$ and is computed as

$$p_{i,j,k} = \frac{Area\ of\ overlap\ between\ G_{i,j}\ and\ Z_k}{Area\ of\ Z_k} \quad (4)$$

Finally, the cumulative score $P_{i,j}$ represents the probability that a grid $G_{i,j}$ consits of atleast one sensor. Initially, $P_{i,j}$ is set to zero. Subsequent values are computed using,

$$P_{i,j} = 1 - \prod_{\forall k} (1 - p_{i,j,k}) \,. \quad (5)$$

C. Improving accuracy by using RSS

Using only AoA information might generate several false positives. For instance, consider a scenario where the transmitting sensor is very close to the localizer. In this case, the localizer wrongly assigns higher probability to farther grid cells (since, farther the grid, the wider is the sector/zone, and hence larger the area of overlap). To reduce the number of false positives, we propose to use RSS information. We note that RSS might vary significantly even for messages from same node and hence, the distance estimates using RSS might also vary significantly. So, instead of using RSS directly, we propose to use RSS only to filter some messages rather than for computing distances. In other words, the localizer would consider a message for score computation, only if the RSS for the message is greater than a threshold - $\bar{P}_{Rx-Th}$. $\bar{T}_{Rx-Th}$ would then be the corresponding maximum distance a transmitting sensor could be from the localizer, beyond which the message would not be considered for localization. This limits the width of the sector (hence decreasing the numerator in Equation 4) and thus reduces the false positives as illustrated through simulations. We also note the tradeoff in choosing $\bar{P}_{Rx-Th}$: a high value would mean that large fraction of messages are filtered out and localizer might have to stop at several more locations to ensure all sensors are localized; smaller values would increase false positives. We further study the choice of $\bar{T}_{Rx-Th}$ through simulations.

D. Localization phase

Finally, the localizer uses the aggregate scores (i.e., $P_{i,j}$) for each grid cell to check if it consists a node or not.

Algorithm 1 Grid Score Assignment Algorithm executed by the Localizer

```
for each grid G_{i,j} in the network do
    Grid_Score P_{i,j} = 0
end for
for each grid intersection point in the network do
    Listen to messages for a duration of T_obs
    for each received message k do
        Measure AoA/ RSSI of k
        Determine Localized_Zone of k
        Area of Localized_Zone = Z_k
        for each grid (i,j) overlapped with Localized_Zone do
            A_{i,j,k} = Area overlapped between grid G_{i_j} and Z_k
            P_{i,j} = 1 - ∏_{∀k} (1 - p_{i,j,k})
        end for
    end for
end for
Return Grid_Score P_{i,j} for all grids
```

We propose a simple approach for score translation. A grid cell is assumed to consist a sensor if its score is greater than a certain threshold. If score is lesser, it is assumed not to contain a sensor. For illustration, assume a grid cell size of $d = \bar{T}_x/5 = 1$. Then, the maximum overlap area for a grid cell is approximately 0.39 (when it is farthest from the localizer). Thus, the maximum score is the overlap area divided by the sector area i.e. 0.179. We note that during every observation interval, at each corner of the grid cell (total of four corners), the localizer receives an average of 10 messages from each sensor, since it waits for $10/\lambda$ duration. The localizer receives more than 40 messages as it might receive messages from other locations as well. Now, assuming an average score of around 0.09 (half the maximum) and 40 messages, the aggregate score would be $1 - (1 - 0.09)^{40} \approx 0.98$. Thus, a grid containing a sensor should get an aggregated score very close to 1. In this paper, we assume a grid contains a sensor if $P_{i,j} > 0.95$.

V. Performance Evaluations

In this section we evaluate the performance of our protocol. We developed a C++ simulator. Varying number of nodes are randomly placed in an area of $1000m * 1000m$ and have no mobility. The transmission range of the sensors is 100m and the transmission rate λ is 0.05. The observation time $T_{obs} = \frac{10}{\lambda}$. For each set of parameters, we repeat the experiment for 20 different seeds for statistical reasons. We vary the number of nodes from 250 to 1000. We categorize a grid cell to contain a sensor if $P_{i,j} > 0.95$. Further, we introduce additional

random attenuation/noise factor that could reduce the RSS signal strength by up to 40% [24]. We also assumed an error bound in angle of arrival degrees of $\epsilon = 6\,\mathrm{deg}$ [22].

We specifically study two metrics:

- Percentage of False Positives (P_{fp}): A grid cell is treated as a False Positive (FP) if the protocol incorrectly concludes that it contains a sensor while it does not. The percentage of FPs is computed as number of FPs divided by total number of grid cells i.e, $g \times g$.

- Percentage of False Negatives (P_{fn}): A grid cell is treated as a False Negative (FN), if the protocol concludes that the cell does not contain a sensor while the cell indeed contains atleast one sensor. The percentage of FNs is the number of FNs divided by total number of grid cells.

We note that the aim to minimize both N_{fp} and N_{fn}. First, we study the tradeoffs between the grid size and false positives/negatives when only AoA is considered. Later, we analyze the performance for various RSS Thresholds. To elaborate, we study the improvement in the performance by selectively ignoring the messages with RSS below $\bar{P}_{Rx-Th}$.

Figure 1 presents the performance of our localization protocol for varying number of nodes in the network with only AoA information. We simulated the performance for various accuracies i.e., grid sizes (i.e., d). Firstly, we note that the number of false negatives is very less than the corresponding number of false positives. In other words, if a node is present in a grid, the localizer correctly identifies it to contain a sensor with high probability. On the other hand, the localizer might incorrectly identify grids as containing a sensor even though they do not. We attribute this high number due to scenarios where a sensor is located closely to the horizontal/vertical grid lines, i.e., close to the border of a grid. In such cases, most of the times, a false positive is produced. This is because, the protocol cannot accurately identify in which grid the sensor is located in, and assigns high scores for multiple grids adjoining the borders of the grid where the sensor is located. Furthermore, one can observe that FPs reduce with increasing d, as higher d reduces number of sensors that are close to grid borders.

Figure 2 presents the results for different $\bar{P}_{Rx-Th}$, i.e., when we use RSS information to filter messages received from farther sensors. Here $d = 20m$. For ease of presentation, we use the term 'maximum sensor distance threshold' ($\bar{T}_{Rx-Th}$) to represent a corresponding maximum distance the filtering would permit. In other words, for a given $\bar{P}_{Rx-Th}$, $\bar{T}_{Rx-Th}$ is the distance that corresponds to a RSS of $\bar{P}_{Rx-Th}$. We can see that choosing a high $\bar{P}_{Rx-Th}$ that corresponds to a low $\bar{T}_{Rx-Th}$ drastically reduces the number of FPs. The reason for this behavior (as explained in the previous section) is the shrinking of sector widths (to minimize far away grids

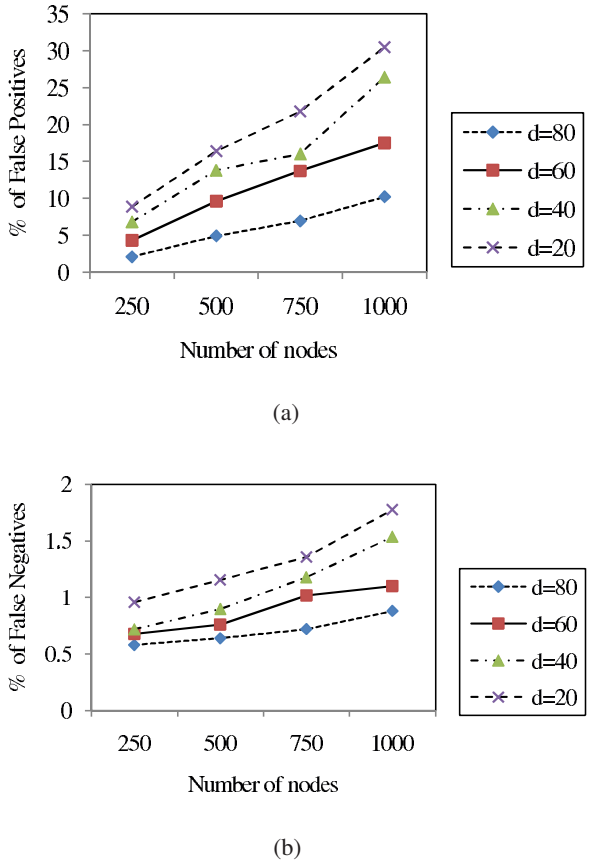
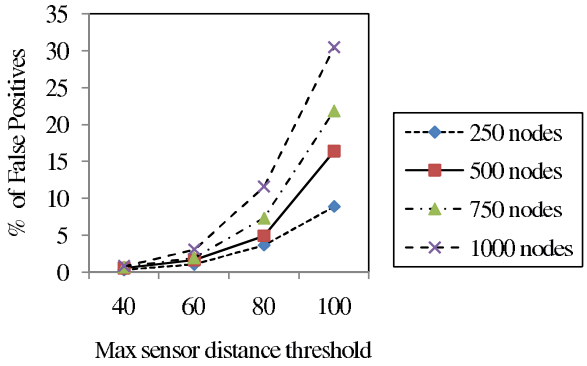


Fig. 1. Percentage of False Positives and False Negatives for different scenarios with only AoA

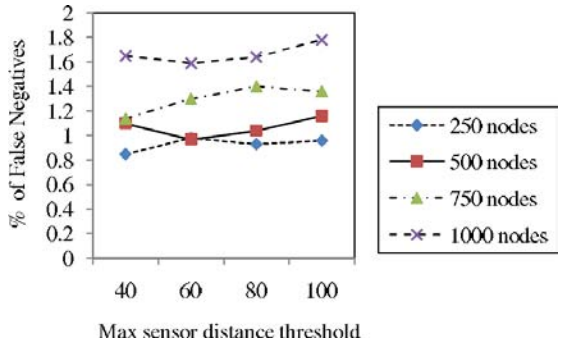
from receiving higher scores) with RSS information that was not the case with pure AoA. This enforces better fairness in eliminating far away unlikely locations, hence reducing the percentage of False Positives. The number of False Negatives does not change appreciably with RSS, since RSS filtering only helps eliminate potentially unlikely sensor locations; potentially correct locations are still retained.

VI. Final Remarks

This paper studies the problem of localizing maliciously deployed sensor networks without cooperation from sensors themselves. This is an important problem in scenarios like battlefields to ensure safety of personnel, and military installations. We employ a *localizer* to physically move in the network and detect raw sensor communication signals, while measuring AoA and RSS. Depending on desired accuracy, our protocol can achieve very low false positives and false negatives. Our on-going work addresses the issue of extending our approach in cases where sensors are deployed to specifically track mobile intruders. Another on-going extension is the issue of localization when the sensors are also mobile.



(a)



(b)

Fig. 2. Percentage of False Positives and False Negatives for different scenarios with AoA and RSS

REFERENCES

[1] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proceedings of the ACM Conference on Computer and Communication Security (CCS)*, November 2002, pp. 41–47.

[2] W. Gu, X. Bai, S. Chellappan, and D. Xuan, "Network decoupling for secure communications in wireless sensor networks," in *Proceedings of IWQoS*, New Haven, June 2006.

[3] D. Liu and P. Ning, "Efficient distribution of key chain commitments for broadcast authentication in distributed sensor networks," in *Network and Distributed System Security Symposium (NDSS)*, San Diego, February 2003.

[4] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Proceedings of IEEE Symposium on Research in Security and Privacy*, May 2003.

[5] Q. Huang, J. Cukier, H. Kobayashi, B. Liu, and J. Zhang, "Fast authenticated key establishment protocols for wireless sensor networks," in *Proceedings of ACM international conference on Wireless Sensor Networks and Applications (WSNA)*, 2003.

[6] S. Chan, R. Poovendran, and M. Sun, "A key management scheme in distributed sensor networks using attack probabilities," in *Proceedings of IEEE Global Telecommunications Conference (Globecom)*, November-December 2005.

[7] E. Ekici, S. Vural, J. McNair, and D. Al-Abri, "Secure probabilistic location verification in randomly deployed wireless sensor networks," in *Ad Hoc Networks Journal (Elsevier)*, January 2007.

[8] D. Al-Abri, J. McNair, and E. Ekici, "Location verification using communication range variation for wireless sensor networks," in *Proceedings of IEEE Military Communications Conference (Milcom)*, Washington D.C., October 2007.

[9] N Sastry, U. Shankar, and D. Wagner, "Secure verification of location claims," in *Proceedings of the ACM workshop on Wireless security (WiSe)*, San Diego, 2003.

[10] K. Liu, N. Abu-Ghazaleh, and K. Kang, "Location verification and trust management for resilient geographic routing," in *Journal of Parallel and Distributed Computing (JPDC)*, February 2007.

[11] Y. Wei, Z. Yu, and Y. Guan, "Location verification algorithms for wireless sensor networks," in *Proceedings of IEEE ICDCS*, Toronto, June 2007.

[12] Y. Zhang, W. Liu, Y. Fang, and D. Wu, "Secure localization and authentication in ultra-wideband sensor networks," in *IEEE Journal On Selected Areas In Communications, Vol. 24, No. 4*, April 2006.

[13] L. Lazos and R. Poovendran, "Hirloc: high-resolution robust localization for wireless sensor networks," in *IEEE Journal On Selected Areas In Communications, Vol. 24, No. 2*, 2006.

[14] L. Lazos and R. Poovendran, "Rope: Robust position estimation in wireless sensor networks," in *Proceedings of International symposium on Information processing in sensor networks (IPSN)*, 2005.

[15] L. Lazos and R. Poovendran, "Serloc: Robust localization for wireless sensor networks," in *ACM Transactions on Sensor Networks , VOL. 1, NO. 1*, August 2005.

[16] Y. Zeng, S. Zhang, S. Guo, and X. Li, "Secure hop-count based localization in wireless sensor networks," in *In Proceedings of International Conference on Computational Intelligence and Security (CIS)*, 2007.

[17] Chris Karlof and David 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.

[18] B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor networks," in *Proceedings of IEEE Symposium on Security and Privacy*, Oakland, May 2005.

[19] Z. Yang, E. Ekici, and D. Xuan, "A localization-based anti-sensor network system," in *Proceedings of IEEE Conference on Computer Communications (INFOCOM) Mini Conference*, Anchorage, May 2007.

[20] J. N. Al-Karaki and A. E. Kamal, "Routing techniques in wireless sensor networks: a survey," *IEEE Wireless Communications*, vol. 11, no. 6, pp. 6–28, 2004.

[21] V. Rai and R.N. Mahapatra, "Lifetime Modeling of a Sensor Network," *Design, Automation, and Test in Europe: Proceedings of the conference on Design, Automation and Test in Europe-*, vol. 1, pp. 202–203, 2005.

[22] N.B Priyantha, A. Miu, H. Balakrishnan, and S. Teller, "The cricket compass for context-aware mobile applications," in *Proceedings of ACM International Conference on Mobile Computing and Networking (MobiCom)*, July 2001.

[23] Donald E. Knuth, *The art of computer programming, volume 2 (3rd ed.): seminumerical algorithms*, Addison-Wesley Longman Publishing Co., Inc., 1997.

[24] G. Zhou, T. He, S. Krishnamurthy, and J.A. Stankovic, "Models and solutions for radio irregularity in wireless sensor networks," *ACM Transactions on Sensor Networks (TOSN)*, vol. 2, no. 2, pp. 221–262, 2006.