# NORM: A Decentralized Location Verification Mechanism for Wireless Sensor Networks

Yingying Chen[†], Jie Yang[†], Xiuyuan Zheng[†] and Venkataraman Swaminathan[*]
[†]Dept. of Electrical and Computer Engineering
Stevens Institute of Technology, Hoboken, NJ 07030
[*]Acoustics and Networked Sensors Division
US Army, RDECOM-ARDEC, Picatinny, NJ 07806

## ABSTRACT

The location of wireless devices and sensor nodes is a critical input for many location-aware applications. Particularly, important tasks in tactical fields, such as monitoring the status of soldiers and tracking the equipments, all rely on the location information. However, adversaries may falsify the location information and undermine the activities supported by location. In this work, we propose NORM, a decentralized location verification mechanism for wireless sensor networks. To perform location verification, three schemes are developed in NORM, namely Neighbor Examination scheme, Neighbor Verification scheme, and Neighbor Localization scheme. Our simulation results provide strong evidence that NORM is not only effective in detecting abnormal locations caused by both naive adversaries as well as sophisticated adversaries, but also robust when a high percentage of sensor nodes are compromised.

## 1 INTRODUCTION

The rapid advancement in wireless technologies and sensor devices is leading to a future where wireless sensors will become pervasively deployed. This makes location of wireless devices or sensor nodes a powerful information source as it is a unique characteristic of each device. Thus, location can become a critical input for many location-aware applications. Particularly, in tactical fields, important tasks, such as monitoring the status of soldiers, tracking the equipments, robotic navigation, and detecting enemy activities, all rely on the location information. There have been a plethora of schemes developed recently to localize sensor nodes [Langendoen and Reijers 2003; Bahl and Padmanabhan 2000; Niculescu and Nath 2001; Kleisouris et al. 2008; He et al. 2003]. However, the performance of the localization algorithms degrades significantly when the sensors are deployed in hostile environments or are attacked by adversaries [Chen et al. 2006].

Although there has been some work in secure localization [Li et al. 2005; Liu et al. 2005; Lazos and Poovendran 2004], they only targeted to enhance the robustness of localization, and adversaries may falsify the location information by compromising sensor nodes or intercepting the location information when it is reported. Compromised location information is a serious threat because of their impact on critical tactical applications, and it is thus desirable to conduct location verification before it is used by location-based tasks.

In this work, we propose a method called Neighbor ObseRvation Mechanism (NORM), for position verification of wireless devices and sensor nodes. NORM is a software component deployed in each sensor node, and can assist sensor information processing and position verification in autonomous systems. We investigate NORM under two adversarial models, a naive adversary and a sophisticated adversary model. We further develop three schemes, namely, Neighbor Examination (NE) scheme, Neighbor Verification (NV) scheme, and Neighbor Localization (NL) scheme, to detect the abnormal location caused by both adversarial models.

Comparing with prior position verification techniques [Capkun and Hubaux 2005; Du et al. 2005], which required specialized hardware, network deployment knowledge, or a central verification center, the main advantage of NORM is that it utilizes the existing wireless network infrastructure without deployment knowledge. Moreover, NORM performs position verification of a sensor node in a fully distributed way depending on the spatial consistency relationship inherited between a sensor node and its neighbors. Our simulation results demonstrated the effectiveness of NORM in detecting abnormal locations and the robustness of NORM under the severity of attacks in terms of the percentage of compromised sensor nodes in the network.

This work is supported in part by the US Army, Picatinny, under Contract No. W15QKN-05-D-0011.

# Report Documentation Page

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE | 2. REPORT TYPE | 3. DATES COVERED |
|---|---|---|
| **01 DEC 2008** | **N/A** | **-** |

| 4. TITLE AND SUBTITLE | 5a. CONTRACT NUMBER |
|---|---|
| **NORM: A Decentralized Location Verification Mechanism for Wireless Sensor Networks** | 5b. GRANT NUMBER |
| | 5c. PROGRAM ELEMENT NUMBER |
| 6. AUTHOR(S) | 5d. PROJECT NUMBER |
| | 5e. TASK NUMBER |
| | 5f. WORK UNIT NUMBER |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Department of Electrical and Computer Engineering Stevens Institute of Technology Hoboken, New Jersey 07030** | 8. PERFORMING ORGANIZATION REPORT NUMBER |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSOR/MONITOR'S ACRONYM(S) |
| | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) |

12. DISTRIBUTION/AVAILABILITY STATEMENT
**Approved for public release, distribution unlimited**

13. SUPPLEMENTARY NOTES
**See also ADM002187. Proceedings of the Army Science Conference (26th) Held in Orlando, Florida on 1-4 December 2008, The original document contains color images.**

14. ABSTRACT

15. SUBJECT TERMS

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | | |
| **unclassified** | **unclassified** | **unclassified** | **UU** | **7** | |

We show that different position verification schemes can be applied to different scenarios based on application requirements.

The remainder of the paper is organized as follows. Section 2 discusses previous research in localization and position verification. We provide an overview of our problem and present the adversarial models in Section 3. We then present NORM in Section 4 and develop three position verification schemes. To evaluate the effectiveness and the robustness of NORM, our simulation results are provided in Section 5. Finally, we conclude our work in Section 6.

## 2 RELATED WORK

Recent research efforts have resulted in a number of localization algorithms [Langendoen and Reijers 2003]. They can be categorized as range-based and range-free. Range-based algorithms [Bahl and Padmanabhan 2000; Kleisouris et al. 2008] involve distance calculation to landmarks with known positions using the measurement of various physical properties, whereas range-free algorithms [Niculescu and Nath 2001; He et al. 2003] use coarser metrics to place bounds on node positions. Further, the performance of the localization algorithms can be corrupted by attacks. [Li et al. 2005] provides a broad survey of potential physical attacks to localization schemes. Moreover, secure localization mechanisms are developed to enhance the robustness of localization schemes [Li et al. 2005; Liu et al. 2005; Lazos and Poovendran 2004]. Covert base stations whose positions are not known to the attacker are employed in [Capkun and Hubaux 2006] to perform secure positioning.

[Sastry et al. 2003] was the first to propose secure verification of location claims by measuring the signal propagation time. It provided a foundation for securely using location in wireless information systems. [Capkun and Hubaux 2005; Lazos et al. 2005] proposed Verifiable Multilateration technique to verify a sensor's location. This method required specialized hardware to perform nanosecond processing and precise ranging. [Du et al. 2005] performed position verification based on consistency check of the observed neighbors and the network deployment knowledge. It assumes a highly dense network where the positions of the node follow a Gaussian distribution, which is contrary to the structure of many deployed systems where much lower densities are typical. The work that is the closest to ours is [Y. Wei and Z. Yu and Y. Guan 2007], where the information of neighboring nodes is used to perform verification. However, a central verification server is needed to conduct location verification. Our work is different in that NORM is a fully distributed position verification mechanism without using specialized hardware and network deployment knowledge.

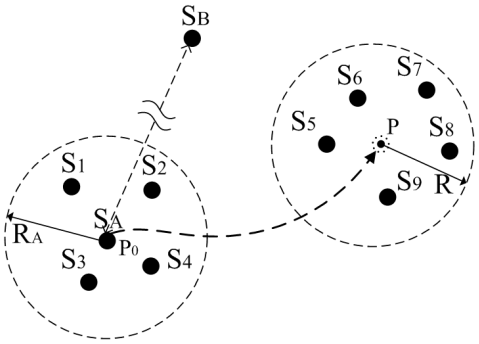


Figure 1: Illustration of two adversarial models: a naive adversary and a sophisticated adversary model.

## 3 PROBLEM OVERVIEW

In this section, we provide a high-level overview of our problem. We then present the two adversarial models that affect the location verification process.

### 3.1 Overview

In tactical fields, sensors are usually deployed to perform monitoring and tracking. For information processing or data fusion, a sensor may need to request data from another sensor. In addition to the traditional identity-based authentication, the increasingly ubiquitous trends of the wireless sensor networks are enabling the information access based on the client sensor being in the right place at the right time [Chen et al. 2006]. Thus, to facilitate location-aware computing paradigms, the access control of the information can be extended from solely identity-based authentication and built upon position verification of the client sensor.

However, adversaries (or enemies) may report incorrect location information to claim that they are in the authorized region in order to access the restricted data in a sensor node. The traditional approach for position verification is to use a centralized server that contains all the location information and can thus verify the position of the client sensor. This kind of approach inherently introduces an issue related to the location privacy. And consequently, sensor nodes may be tracked by the central server. In addition, due to environmental constraints, the deployment of a central verification server is not always possible, especially in tactical fields. As opposed to the traditional centralized location verification methods, we propose NORM, which is a decentralized mechanism to perform position verification based on the observation from the neighboring nodes of the client sensor. Thus, in NORM, when a sensor node reports its location, it also needs to send its neighbor list, which will be used to help verifying the reported location.

### 3.2 Adversary Model

In this work, we consider two adversarial models, a naive adversary and a sophisticated adversary model. In both models, the adversary claims the position of the compromised sensor at $P$, while its true position is at $P_0$. As shown in Figure 1, the compromised sensor node $S_A$'s true location is at $P_0$, but the adversary claims its position is at $P$.

For a naive adversary, it either sends an arbitrary neighbor list or reports neighbors of the compromised sensor node consistent with their reported location $P$. Whereas for a sophisticated adversary, it reports the true neighbors around the compromised sensor's true position $P_0$ to trick the system. For instance, in Figure 1, the naive adversary at the sensor node $S_A$ reports $P$ as the position of $S_A$ and sends sensor nodes $\{S_5, S_6, S_7, S_8, S_9\}$ around location $P$ as neighboring nodes of $S_A$, whereas the sophisticated adversary sends the true neighbors of $S_A$, $\{S_1, S_2, S_3, S_4\}$, around location $P_0$.

If a sensor node is compromised, it will not respond to any verification requests for confirming the observation of other nodes. Further, we define an *Anomaly Distance (AD)* as the distance between the reported location and the true location (i.e. $AD = \|P - P_0\|$). We want to design position verification schemes that can detect the abnormal location when AD exceeds certain distances.

## 4 NORM: NEIGHBOR OBSERVATION MECHANISM

In this section, we present our Neighbor ObseRvation Mechanism (NORM) for position verification of wireless devices and sensor nodes. NORM is a software component deployed in each sensor node. Comparing to prior position verification techniques, [Capkun and Hubaux 2005; Du et al. 2005], the main advantage of NORM is that it does not require special hardware, deployment knowledge, or a central verification center. NORM performs position verification of a sensor node in a fully distributed way, depending on the spatial consistency relationship inherited between a sensor node and its neighbors. We next describe three detecting schemes we developed in NORM. For illustration purpose, we use the example when a sensor node $S_B$ needs to verify the reported location of the sensor node $S_A$.

### 4.1 Defeating Naive Adversaries

**Neighbor Examination (NE) Scheme:** The NE scheme performs position verification based on the direct response from neighbors of the node under verification, i.e., $S_A$. The sensor node $S_B$ issues a special verification request to each neighbor, $S_i$, with $i = 1, 2, ...N$ ($N$ is the total number of neighbors), reported in the neighbor list of the client sensor $S_A$, and asks whether it has $S_A$ in its neighbor list. When the sensor $S_i$ receives the request, if $S_i$ has $S_A$ in its neighbor list, $S_i$ confirms and reports its current position $P_i$ back. If $S_i$ is compromised by the adversary, based on our adversary model, $S_i$ will keep silent and does not respond. We then define the neighbor examination probability $P_{ex}$ as

$$P_{ex} = \frac{\sum_{i=1}^{K} S_i}{N}, \tag{1}$$

where $K$ is the total number of neighbors that responds to the request from $S_B$. If $P_{ex} > \alpha$ where $\alpha$ is the confidence level, $S_B$ determines that $S_A$ passes the neighbor examination. A naive adversary, who sends an arbitrary neighbor list or reports neighbors around location $P$ when lying about the location of the compromised sensor node, will thus result in $P_{ex} < \alpha$ and fail the neighbor examination scheme.

### 4.2 Defeating Sophisticated Adversaries

A sophisticated adversary may claim that the compromised sensor node is at location $P$, but report the neighboring nodes around sensor's true location $P_0$. The NE scheme cannot detect the abnormal locations reported by sophisticated adversaries. The Neighbor Verification and the Neighbor Localization schemes are thus developed to detect abnormal locations reported by sophisticated adversaries that send the neighboring information around the true location of the node under verification to trick the system.

**Neighbor Verification (NV) Scheme:** Like in the NE scheme, $S_B$ first issues a special verification request to each neighbor, $S_i$ with $i = 1, 2, ...N$, reported in the neighbor list of the client sensor $S_A$, and asks whether it has $S_A$ in its neighbor list. When the sensor $S_i$ receives the request, if $S_i$ has $S_A$ in its neighbor list, $S_i$ confirms and reports its current position $P_i$ back. Based on the reported positions of the responded neighbors, $S_B$ then needs to conduct further neighbor verification. Given that the neighboring nodes of $S_A$ must be within the communication range $R_A$ of $S_A$, the distance between the estimated locations of $S_A$ and its neighbor $||P_A - P_i||$ should be within $R_A$ for an honest sensor node. $S_B$ could complete the position verification of $S_A$ if $||P_A - P_i|| < R_A$ for all $i = 1...K$.

However, since there are localization errors from the location estimation process [Bahl and Padmanabhan 2000; Elnahrawy et al. 2004], we define

$$||P_A - P_i|| < R_A + r, \tag{2}$$

where $r$ is a random variable introduced by localization errors. We may assume localization errors are Gaussian. Under this assumption, $r$ also follows a Gaussian distribution with mean $\mu$ and variance $\sigma$. Thus the probability that $P_A$

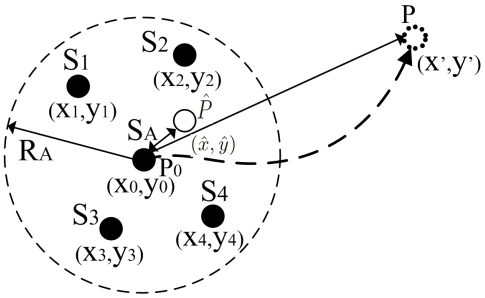


Figure 2: Illustration of the Neighbor Localization (NL) scheme.

and $P_i$ are neighbors is given by

$$\begin{aligned} Pr(P_i) &= Pr(r > (||P_A - P_i|| - R_A)) \\ &= 1 - F(||P_A - P_i|| - R_A), \end{aligned} \quad (3)$$

with $F(r)$ as the Cumulative Distribution Function of $r$,

$$F(r) = \frac{1}{\sqrt{2\pi\sigma^2}} \int_{-\infty}^{r} \exp(-\frac{(u-\mu)^2}{2\sigma^2}) \ du. \quad (4)$$

Further, we define the neighbor verification probability $P_{ve}$, which is the joint probability that all $P_i$, $i = 1...K$, are the neighbors of $P_A$ as:

$$P_{ve} = \prod_{i=1}^{K} Pr(P_i). \quad (5)$$

We then set a confidence level $\beta$ such that if $P_{ve} > \beta$, we declare that $S_A$ passes the Neighbor Verification scheme. Otherwise, the reported location information of $S_A$ is declared as compromised.

**Neighbor Localization (NL) Scheme:** The NL scheme utilizes the location of $S_A$'s neighboring nodes to estimate the position of $S_A$ and further to verify the reported position of $S_A$. The estimated position $\hat{P}$ of $S_A$ is expressed as:

$$\hat{P} = \frac{1}{K} \sum_{i=1}^{K} (X_i, Y_i), \quad (6)$$

where $K$ is the total number of responded neighbors to $S_B$, $(X_i, Y_i)$ is the position of the $ith$ neighbor. Under the normal situation, the distance between the sensor node $S_A$'s true location $P_0$ and the estimated location $\hat{P}$ from NL scheme should be small. However, if $S_A$ is compromised, the distance between the reported location $P$ of $S_A$ and $\hat{P}$ should be large.

As illustrated in Figure 2, the distance between $P_0$ and $\hat{P}$ is much smaller than the distance between $P$ and $\hat{P}$. Therefore, we define a *Maximum Tolerable Distance (MTD)* as the threshold of declaring the abnormal location in NL scheme. In particular, let $D = \|P - \hat{P}\|$. If $D > MTD$, NL scheme declares the location reported by $S_A$ is compromised.

## 5 SIMULATION RESULTS

In this section, we first present our evaluation metrics. We then introduce the simulation methodology. We next present our simulation results.

### 5.1 Evaluation Metrics

In order to evaluate the performance of NORM, we use the following metrics:

**Detection Rate:** The detection rate is defined as the percentage of actual abnormal location that are determined to be abnormal:

$$DR = \frac{N_{tp}}{N_p}, \quad (7)$$

where $N_{tp}$ is the number of abnormal locations, i.e., true positive, detected by NORM and $N_p$ is the total number of abnormal locations, i.e., positive.

**False Positive Rate:** The false positive rate is defined as the percentage of normal location that are falsely determined to be abnormal location:

$$FPR = \frac{N_{fp}}{N_n}, \quad (8)$$

where $N_{fp}$ is the number of normal locations falsely determined to be abnormal locations, i.e., false positive, and $N_n$ is the total number of normal locations.

**Receiver Operating Characteristic (ROC) curve:** To evaluate NORM we want to study the false positive rate and detection rate together. The ROC curve is a plot of the detection accuracy of the abnormal location against the false positive detection. It can be obtained by varying the detection thresholds. The ROC curve provides a direct means to measure the trade off between false-positive and correct detections.

### 5.2 Simulation Methodology

In our simulation setup, we deploy $200$ to $500$ sensors randomly in a $350m \times 350m$ square field. The communication range of the sensor node is modeled to follow a Gaussian distribution with mean at $30m$ and standard deviation as $2m$. Under this setup each sensor node can observe average number of neighbors ranging from $4$ to $11$. Further, we simulate the localization error of a sensor node by modeling the localization errors of the $X$ and $Y$ coordinates to follow a Gaussian distribution with zero mean and standard deviation of $3m$. This corresponds to the localization error with a median of $3m$ and can range from $0$ to $11m$, which is inline with previous experimental findings [Elnahrawy et al. 2004].

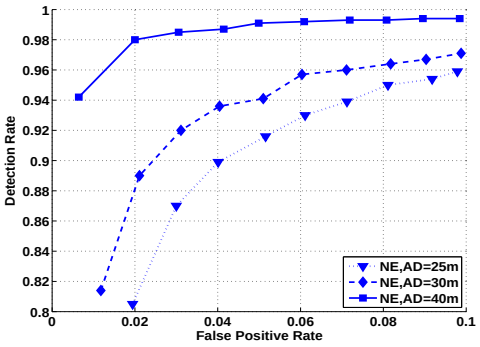


Figure 3: Naive Adversaries: Receiver Operating Characteristic (ROC) curve for impact of anomaly distance.

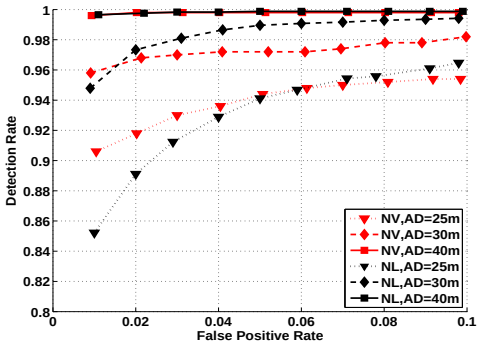


Figure 4: Sophisticated Adversaries: Receiver Operating Characteristic (ROC) curve for impact of Anomaly Distance.

We then randomly choose sensor nodes that are compromised by adversaries. The default percentage of compromised sensor nodes is set to 0.1. Based on our adversary model, a compromised sensor node will keep silent when receiving special verification requests. To evaluate the effectiveness of NORM, we vary Anomaly Distance (AD), percentage of compromised sensor nodes, network density and localization error in our simulation study.

### 5.3 Evaluation Results

**Impact of Anomaly Distance (AD):** Figure 3 presents the ROC curve under various Anomaly Distance when the Neighbor Examination (NE) scheme is used to detect abnormal locations caused by naive adversaries. We observed that NE scheme can achieve detection rates over 95% when the FPR is less than 10%. For the case of $AD = 25m$, which is less than the average communication range (i.e., $30m$) of sensor nodes, the detection rate is above 90% when the FPR reaches 5%. Further, the detection rate achieves 99% when the false positive rate is 5% for the case of $AD = 40m$. Moreover, we found that the larger the AD is, the higher the detection rate can achieve. Specifically, by examining the condition of $FPR = 0.05$ the detection rate increases from 91% to over 99% when AD increases from $25m$ to $40m$.

Figure 4 presents the ROC curves under various Anomaly Distance when NV and NL schemes are used respectively to detect the abnormal locations caused by sophisticated adversaries. Both NV as well as NL schemes present similar detection performance to NE scheme when AD ranges from $25m$ to $40m$: the detection rate increases with the increasing of the Anomaly Distance. In particular, the detection rates are above 92% when the FPR is 5% for both NV and NL schemes under the case of $AD = 25m$. The detection rates are close to 100% when the FPR is 5% for both NV and NL schemes under the case of $AD = 40m$. This indicates our position verification schemes are

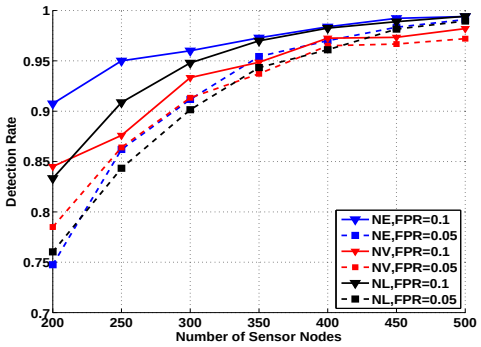


Figure 5: Impact of network density.

effective in detecting abnormal locations caused by both naive as well as sophisticated adversaries. We further observed that NV scheme outperforms NL scheme when FPR is below 5%, whereas NL scheme outperforms NV scheme when FPR is above 5%. Therefore, we can choose proper detection schemes according to the application tolerance to the false positive rate.

**Impact of Network Density:** By varying the number of sensor nodes from 200 to 500 in our simulated networks, we evaluated how the network density impact the performance of NORM. In this setup, each sensor node can observe in average 4 neighbors for the deployment of 200 sensors and 11 neighbors for the deployment of 500 sensors in the network respectively. Figure 5 presents the detection rate versus number of sensor nodes under all three schemes. We observed that the detection rate increases with the increasing of network density. In particular, when the number of sensors increases from 200 to 500, the detection rate increases from 85% to 98% for NV scheme, from 90% to 99% for NE scheme and from 83% to 98% for NL scheme respectively, under the condition of FPR less than 10%. Further, we found that NV scheme outperforms NL scheme when the number of sensors is small (e.g. 200),

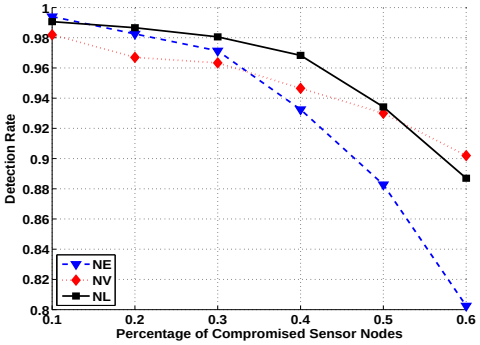


Figure 6: Impact of Percentage of Compromised Sensor Nodes in Network.

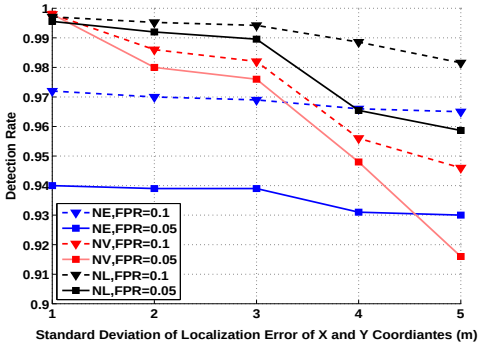


Figure 7: Impact of Localization Error of Sensor Nodes.

whereas the NL scheme outperforms NV scheme when the number of sensors is large (e.g. $500$). Since NL scheme relies on positions of neighbors to estimate the location of a sensor node, the denser the network, the more accurate the position estimation can become and thus the higher detection rate NL scheme can achieve. Hence, based on different network density, we can choose different schemes to perform position verification.

**Impact of Percentage of Compromised Sensor Nodes:** We vary the percentage of compromised sensor nodes in the network to evaluate the robustness of NORM when large number of nodes are compromised in the network. Figure 6 presents the relationship between the detection rate and the percentage of compromised sensor nodes. The false positive rate is set at 10% and the Anomaly Distance equals to $30m$.

As shown in Figure 6, the detection rates of the three schemes drop gradually from above 98% to 80% as the percentage of compromised nodes increases from 10% to 60%. A key observation of this experiment is that the performance of NORM is still over 80% even when the percentage of compromised nodes is extensively large (i.e. 60%), which indicates that NORM is robust in detecting abnormal locations under the situation when large number of nodes are compromised.

**Impact of Localization Error of Sensor Nodes:** We further examine how the localization error can impact the performance of NORM. In this experiment, we vary the standard deviation of the localization error of the X and Y coordinates of a sensor node from $1m$ to $5m$. We note that $1m$ standard deviation corresponds to a mean localization error of $1.3m$, whereas $5m$ standard deviation corresponds to a mean localization error of $6.3m$. The Anomaly Distance is maintained at $30m$ and the false positive rate is set to 5% and 10% respectively.

Figure 7 presents the detection rates of all three schemes versus the standard deviation. We observed that overall the detection rates are decreasing when the localization error is increasing for all three schemes. And the detection rates of NL and NV schemes can approach 100% no matter the FPR is 5% or 10% when the mean localization error is around $1.3m$ with a corresponding standard deviation of $1m$. Interestingly, we found that NE scheme is not as sensitive as NV and NL schemes to the localization error. Specifically, the decreasing of the detection rate of NE schemes is about 1%, whereas it is 4% for NL scheme and 8.5% for NV scheme when the mean localization error ranges from $1.3m$ to $6.3m$. This is because NE scheme does not use the positions of sensor nodes (i.e. neighboring nodes) directly, and thus the performance of NE scheme is more stable under various localization errors than other schemes that rely on the positions of sensor nodes.

## 6 CONCLUSION

In this work, we proposed a Neighbor ObseRvation Mechanism (NORM) to perform position verification in wireless sensor networks, especially for tactical environments. Three schemes, Neighbor Examination scheme, Neighbor Verification scheme, and Neighbor Localization scheme, are developed in NORM to detect abnormal locations caused by both naive as well as sophisticated adversaries. NORM conducts position verification in a fully distributed way depending on the spatial consistency relationship inherited between a sensor node and its neighbors. The main advantage of NORM is that it does not require special hardware, network deployment knowledge, or a central verification server. Simulation results demonstrated that NORM is effective in detecting abnormal locations and is robust when a high percentage of sensor nodes are compromised. Further, we found that our three position verification schemes can be applied to different network scenarios based on application requirements.

## REFERENCES


Bahl, P. and Padmanabhan, V. N. 2000. RADAR: An in-building RF-based user location and tracking system. In *Proceedings of the IEEE International Conference on Computer Communications (INFOCOM)*. 775–784.

Capkun, S. and Hubaux, J. 2006. Securing localization with hidden and mobile base stations. In *Proceedings of the IEEE International Conference on Computer Communications (INFOCOM)*.

Capkun, S. and Hubaux, J. P. 2005. Secure positioning of wireless devices with application to sensor networks. In *Proceedings of the IEEE International Conference on Computer Communications (INFOCOM)*. 1917–1928.

Chen, S., Zhang, Y., and Trappe, W. 2006. Inverting sensor networks and actuating the environment for spatio-temporal access control. In *Proceedings of the Forth ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN)*. 1–12.

Chen, Y., Kleisouris, K., Li, X., Trappe, W., and Martin, R. P. 2006. The robustness of localization algorithms to signal strength attacks: a comparative study. In *Proceedings of the International Conference on Distributed Computing in Sensor Systems (DCOSS)*. 546–563.

Du, W., Fang, L., and Ning, P. 2005. Lad: Localization anomaly detection for wireless sensor networks. In *Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium (IPDPS 05)*.

Elnahrawy, E., Li, X., and Martin, R. P. 2004. The limits of localization using signal strength: A comparative study. In *Proceedings of the First IEEE International Conference on Sensor and Ad hoc Communcations and Networks (SECON 2004)*. 406–414.

He, T., Huang, C., Blum, B., Stankovic, J. A., and Abdelzaher, T. 2003. Range-free localization schemes in large scale sensor networks. In *Proceedings of the Ninth Annual ACM International Conference on Mobile Computing and Networking (MobiCom'03)*.

Kleisouris, K., Chen, Y., Yang, J., and Martin, R. P. 2008. The impact of using multiple antennas on wireless localization. In *Proceedings of the Fifth Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON*.

Langendoen, K. and Reijers, N. 2003. Distributed localization in wireless sensor networks: a quantitative comparison. *Comput. Networks 43*, 4, 499–518.

Lazos, L. and Poovendran, R. 2004. SeRLoc: Secure range-independent localization for wireless sensor networks. In *Proceedings of the 2004 ACM Workshop on Wireless Security*. 21–30.

Lazos, L., Poovendran, R., and Capkun, S. 2005. Rope: robust position estimation in wireless sensor networks. In *Proceedings of the Fourth International Symposium on Information Processing in Sensor Networks (IPSN 2005)*. 324–331.

Li, Z., Trappe, W., Zhang, Y., and Nath, B. 2005. Robust Statistical Methods for Securing Wireless Localization in Sensor Networks. In *The Fourth International Conference on Information Processing in Sensor Networks (IPSN)*. 91–98.

Liu, D., Ning, P., and Du, W. 2005. Attack-resistant location estimation in sensor networks. In *Proceedings of the Fourth International Symposium on Information Processing in Sensor Networks (IPSN 2005)*. 99–106.

Niculescu, D. and Nath, B. 2001. Ad hoc positioning system (APS). In *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM)*. 2926–2931.

Sastry, N., Shankar, U., and Wagner, D. 2003. Secure verification of location claims. In *Proceedings of the ACM workshop on wireless security*. 1–10.

Y. Wei and Z. Yu and Y. Guan. 2007. Location verification algorithms for wireless sensor networls. In *Proceedings of the 27th IEEE International Conference on Distributed Computing Systems (ICDCS)*.