A Survey on Secure Localization in Wireless Sensor Networks

Avinash Srinivasan and Jie Wu
Florida Atlantic University, Boca Raton, FL, USA

Keywords: *Adversary, attack, beacon, intruder, localization, security, wireless sensor networks.*

Definition: *Localization is the process by which an object determines its spatial coordinates in a given field.*

1 Introduction

Wireless sensor networks (WSNs) are shaping many activities in our society, as they have become the epitome of pervasive technology. WSNs have an endless array of potential applications in both military and civilian applications, including robotic land-mine detection, battlefield surveillance, target tracking, environmental monitoring, wildfire detection, and traffic regulation, to name just a few. One common feature shared by all of these critical applications is the vitality of sensor location. The core function of a WSN is to detect and report events which can be meaningfully assimilated and responded to only if the accurate location of the event is known. Also, in any WSN, the location information of nodes plays a vital role in understanding the application context. There are three visible advantages of knowing the location information of sensor nodes. First, location information is needed to identify the location of an event of interest. For instance, the location

of an intruder, the location of a fire, or the location of enemy tanks in a battlefield is of critical importance for deploying rescue and relief troops. Second, location awareness facilitates numerous application services, such as location directory services that provide doctors with the information of nearby medical equipment and personnel in a smart hospital, target-tracking applications for locating survivors in debris, or enemy tanks in a battlefield. Third, location information can assist in various system functionalities, such as geographical routing [2, 3, 6, 11, 13, 15], network coverage checking [20], and location-based information querying [26]. Hence, with these advantages and much more, it is but natural for location-aware sensor devices to become the defacto standard in WSNs in all application domains that provide location-based service.

A straightforward solution is to equip each sensor with a GPS receiver that can accurately provide the sensors with their exact location. This, however, is not a feasible solution from an economic perspective since sensors are often deployed in very large numbers and manual configuration is too cumbersome and hence not feasible. Therefore, localization in sensor networks is very challenging. Over the years, many protocols have been devised to enable the location discovery process in WSNs to be autonomous and able to function independently of GPS and other manual techniques [8, 12, 14, 19, 22, 23]. In all these literatures, the focal point of location discovery has been a set of specialty nodes known as *beacon nodes*, which have been referred to by some researchers as anchor, locator, or seed nodes. However, in this chapter we shall use the term beacon node without loss of generality. These beacon nodes know their location, either through a GPS receiver or through manual configuration, which they provide to other sensor nodes. Using this location of beacon nodes, sensor nodes compute their location using various

techniques discussed in section 3. It is, therefore, critical that malicious beacon nodes be prevented from providing false location information since sensor nodes completely rely on the information provided to them for computing their location.

There are three important metrics associated with localization: *energy efficiency*, *accuracy*, and *security*. Though the first two metrics have been researched extensively, the security metric has drawn the attention of researchers only recently, and as such has not been addressed adequately. As security is a key metric, we are motivated to survey the existing techniques focusing on secure localization. This chapter, in which we review secure localization techniques that have been featured in literature thus far, is intended to be a single point of reference for researchers interested in secure localization.

The rest of the chapter is organized as follows. In Section 2 we discuss the unique operational challenges in WSNs. In Section 3 we give an overview of the localization process and enumerate the security requirements. Section 4 presents the classification of localization techniques. In Section 5, we discuss the attacker model and present attacks that are specific to localization. In Section 6 we survey the existing secure localization models. Finally, we conclude this chapter in Section 7.

2 Operational Challenges in WSNs

WSNs, unlike their counterparts, are often deployed to operate in unattended and hostile environments rarely encountered by typical computing devices: rain, snow, humidity, and high temperature. When used for military applications like landmine detection, battlefield surveillance, or target tracking, the conditions further

deteriorate. In such unique operational environments, WSNs have to operate autonomously and consequently are faced with unique challenges. An adversary can now capture and compromise one or more sensors physically. Once captured, a node is at the mercy of the adversary. The adversary can now tamper with the sensor node by injecting malicious code, forcing the node to malfunction, extracting the cryptographic information held by the node to bypass security hurdles like authentication and verification, so on and so forth. Now, the adversary can launch attacks from within the system as an insider, and most existing systems would fail in the face of such inside attacks.

For instance, consider a beacon-based localization model. Now, since sensor nodes are not capable of determining their own location, they have no way of determining which beacon nodes are being truthful in providing accurate location information. There could be malicious beacon nodes that give false location information to sensor nodes compelling them to compute incorrect location. This situation, in which one entity has more information than the other, is referred to as *information asymmetry*. The information asymmetry in beacon-based localization models has been addressed in [36]. [36] also presents an effective way of resolving insider attacks. The attacker can also launch sybil, worm hole, or replay attacks to disrupt the localization process.

3 Overview of Localization Process

Localization is the process by which sensor nodes determine their location. In simple terms, localization is a mechanism for discovering spatial relationships between objects. The various approaches taken in literature to solve this localization prob-

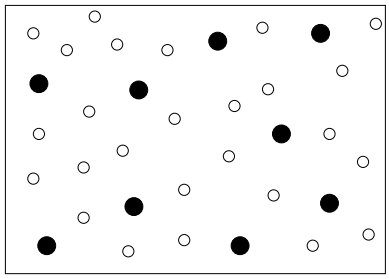
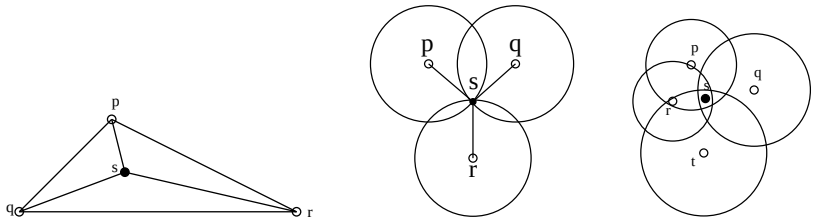


Figure 1: A network with sensor and beacon nodes. Sensor nodes are represented by hollow circles and beacon nodes are represented by shaded circles.

lem differ in the assumptions they make about their respective network and sensor capabilities. A detailed, but not exhaustive, list of assumptions made include assumptions about device hardware, signal propagation models, timing and energy requirements, composition of network viz homogeneous vs. heterogeneous, operational environment viz indoor vs. outdoor, beacon density, time synchronization, communication costs, error requirements, and node mobility [23]. In node mobility four different scenarios arise. First, both sensor and beacon nodes ate static. Second, sensor nodes are static while beacon nodes move. Third, sensor nodes move while beacon nodes are static. Fourth, both sensor and beacon nodes move.

In localization models that use GPS as the source, the localization process is straightforward. However, in a localization model that uses beacon nodes to help sensor nodes with location discovery, the beacon nodes are either manually configured with their location or equipped with a GPS receiver which they can use to determine their location. Beacon nodes then provide their location information to sensor nodes and help them in computing their location. The idea of beacon-based localization is presented in Figure 1. The localization process itself can be classified into two stages. In the first stage, a node merely estimates its distance to



(a) (b) (c)

Figure 2: (a) Triangulation (b) Trilateration (c) Multilateration

other nodes in its vicinity using one or more features of the received signal. In the second stage, a node uses all the distance estimates to compute its actual location. The method employed in stage two to compute the actual location depends on the signal feature used in stage one, and can be classified into three main groups as follows.

- Triangulation: A large number of localization algorithms fall into this class. In simple terms, the triangulation method involves gathering Angle of Arrival (AoA) measurements at the sensor node from at least three sources. Then using the AoA references, simple geometric relationships and properties are applied to compute the location of the sensor node.

- Trilateration: Trilateration is a method of determining the relative positions of objects using the geometry of triangles similar to triangulation. Unlike triangulation, which uses AoA measurements to calculate a subject's location, trilateration involves gathering a number of reference tuples of the form (x, y, d). In this tuple, d represents an estimated distance between the source providing the location reference from (x, y) and the sensor node. To accurately and uniquely determine the relative location of a point on a 2D plane

using trilateration, a minimum of 3 reference points are needed.

- Multilateration: Multilateration is the process of localization by solving for the mathematical intersection of multiple hyperbolas based on the Time Difference Of Arrival (TDoA). In multilateration, the TDoA of a signal emitted from the object to three or more receivers is computed accurately with tightly synchronized clocks. When N receivers are used, it results in $N-1$ hyperbolas, the intersection of which uniquely positions the object in a 3D space. When a large number of receivers are used, $N > 4$, then the localization problem can be posed as an optimization problem that can be solved using, among others, a least squares method.

Secure localization in sensor networks has become a major focus of research in recent years. Like any other process, localization also has security requirements, which are listed below. The breach of any of these security requirements is a harbinger of compromise in the localization process.

1. Authentication: Information for localization must be provided only by authorized sources. Therefore, before accepting location-related information, the provider has to be authenticated.

2. Integrity: The information provided by the source should be untampered before the sensor nodes can use it to discover their location.

3. Availability: All the information required by a sensor node to compute its location must be available when needed.

4. Non-Repudiation: Neither the source that provides the location information

nor the sensor nodes that receive the location information should be able deny the information exchange at a later time.

5. Privacy: Location privacy is one of the most important security requirements. The source should only help the sensor node in determining its location. Neither the source's location nor the sensor node's location should be disclosed at any point. This constraint helps to prevent malicious nodes from claiming a different legitimate location in the network.

Error in the estimated location of a sensor can be classified into two groups: intrinsic and extrinsic [35]. Intrinsic errors are most often caused by abnormalities in the sensor hardware and software, and can cause many complications when estimating node positions. On the otherhand, extrinsic errors are attributed to the physical effects on the measurement channel. This includes shadowing effects, changes in signal propagation speed, obstacles, etc. Extrinsic errors are more unpredictable and harder to handle. Measurement errors can significantly amplify the error in position estimates. Also, use of lower-precision measurement technology combined with higher uncertainty of beacon locations will augment errors in position estimates.

4 Classification of Localization Techniques

In this section, we shall classify localization techniques and discuss their merits and demerits.

1. **Direct approaches:** This is also known as *absolute localization*. The direct approach itself can be classified into two types: *Manual configuration* and

GPS-based localization. The manual configuration method is very cumbersome and expensive. It is neither practical nor scalable for large scale WSNs and in particular, does not adapt well for WSNs with node mobility. On the other hand, in the GPS-based localization method, each sensor is equipped with a GPS receiver. This method adapts well for WSNs with node mobility. However, there is a downside to this method. It is not economically feasible to equip each sensor with a GPS receiver since WSNs are deployed with hundreds of thousands of sensors. This also increases the size of each sensor, rendering them unfit for pervasive environments. Also, the GPS receivers only work well outdoors on earth and have line-of-sight requirement constraints. Such WSNs cannot be used for underwater applications like habitat monitoring, water pollution level monitoring, tsunami monitoring, etc.

2. **Indirect approaches:** The indirect approach of localization is also known as *relative localization* since nodes position themselves relative to other nodes in their vicinity. The indirect approaches of localization were introduced to overcome some of the drawbacks of the GPS-based direct localization techniques while retaining some of its advantages, like accuracy of localization. In this approach, a small subset of nodes in the network, called the *beacon nodes*, are either equipped with GPS receivers to compute their location or are manually configured with their location. These beacon nodes then send beams of signals providing their location to all sensor nodes in their vicinity that don't have a GPS receiver. Using the transmitted signal containing the location information, sensor nodes compute their location. This approach effectively reduces the overhead introduced by the GPS-based method. How-

ever, since the beacon nodes are also operating in the same hostile environment as the sensor nodes, they too are vulnerable to various threats, including physical capture by adversaries. This introduces new security threats concerning the honesty of the beacon nodes in providing location information since they could have been tampered by the adversary and misbehave by providing incorrect location information. This particular problem has been addressed well in [36] where a reputation and trust-based system is used to monitor such misbehavior.

Within the indirect approach, the localization process can be classified into the following two categories.

1. Range-based: In range-based localization, the location of a node is computed relative to other nodes in its vicinity. Range-based localization depends on the assumption that the absolute distance between a sender and a receiver can be estimated by one or more features of the communication signal from the sender to the receiver. The accuracy of such an estimation, however, is subject to the transmission medium and surrounding environment. Range-based techniques usually rely on complex hardware which is not feasible for WSNs since sensor nodes are highly resource-constrained and have to be produced at throwaway prices as they are deployed in large numbers. [12, 14, 18, 19, 21, 25, 29] are some examples of range-based localization techniques. The features of the communication signal that are frequently used in literature for range-based localization are as follows:

    - Angle of Arrival (AoA): Range information is obtained by estimating and mapping relative angles between neighbors. [19, 25] make use of

AoA for localization.

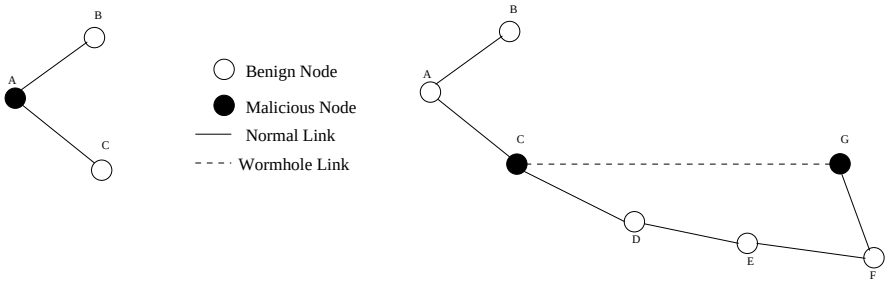
- Received Signal Strength Indicator (RSSI): Use a theoretical or empirical model to translate signal strength into distance. RADAR [10] is one of the first to make use of RSSI. RSSI has also been employed for range estimation in [7, 16, 21].
- Time of Arrival (ToA): To obtain range information using ToA, the signal propagation time from souce to destination is measured. A GPS is the most basic example that uses ToA. To use ToA for range estimation, a system needs to be synchronous, which necessitates use of expensive hardware for precise clock synchronization with the satellite. ToA is used in [1, 21] for localization.
- Time Difference of Arrival (TDoA): To obtain the range information using TDoA, an ultrasound is used to estimate the distance between the node and the source. Like ToA, TDoA necessitates the use of special hardware, rendering it too expensive for WSNs. [4, 9, 14, 18] are some localization techniques that make use of TDoA.

2. Range-free: Range-free localization never tries to estimate the absolute point-to-point distance based on received signal strength or other features of the received communication signal like time, angle, etc. This greatly simplifies the design of hardware, making range-free methods very appealing and a cost-effective alternative for localization in WSNs. Amorphous localization [5], Centroid localization [8], APIT [23], DV-Hop localization [24], SeRLoc [27], and ROCRSSI [28] are some examples of range-free localization techniques. Range-free techniques have also been employed in [17].

5 Attacker Model

Before reviewing the existing secure localization models, we feel it is necessary to analyze the attacker model to understand the attacker's capabilities. The attacker can either be an insider or an outsider. As an insider, the attacker has access to all of the cryptographic keying material held by a node. This is potentially dangerous since the attacker can now claim to be a legitimate part of the network. Authentication or verification via password and other mechanisms give way under this attacker model. On the otherhand, in the outsider attack model, the attacker is outside the network and has no information about cryptographic keys and passwords necessary for authentication. The attacker can only capture a node but cannot extract the sensitive information. This model is comparatively less detrimental, but harmful nonetheless. So, for a localization process to be secure it has to be robust in its defense against both outsider and insider attacks. Some attacks that have been discussed for nearly a decade in literature that are the most common against localization schemes are as follows:

- Replay Attack: A replay attack is the easiest and most commonly used by attackers. Specifically, when an attacker's capability is limited, i.e., the attacker cannot compromise more than 1 node, this is the most preferred attack. In a replay attack, the attacker merely jams the transmission between a sender and a receiver and later replays the same message, posing as the sender. The other way to launch a replay attack is, as shown in Figure 3(a), malicious node A retransmits to node C the message it receives from node B. A replay attack has a two-fold consequence. First, the attacker is replaying the message of another node. Second, the attacker is transmitting



(a) (b)

Figure 3: (a) Replay attack example. Node A replays to C the message it receives from B. (b) Wormhole attack example. Nodes C and G have a wormhole link.

stale information. In particular, the chances of the information being stale is higher in networks with higher node mobility. When replay attacks are launched on the localization process, a localizing node will receive an incorrect reference thereby localizing incorrectly. Unlike a wormhole attack, a single node can disrupt the network with a replay attack.

- Sybil Attack: The sybil attack requires a more sophisticated attacker compared to the replay attack. In a sybil attack, a node claims multiple identities in the network. When launched on localization, localizing nodes can receive multiple location references from a single node leading to incorrect location estimation. Like the replay attack, the sybil attack can also be launched by a single node since there is no need for collusion among nodes to launch this attack.

- Wormhole Attack: A wormhole attack is the most complicated of all the mentioned attacks. To launch a wormhole attack, the attacker has to compromise at least two nodes. In a wormhole attack, the colluding nodes in the network tunnel messages transmitted in one part of the network to their

colluding partners in other parts of the network. The effect of a wormhole attack on localization is depicted in Figure 3(b). Here, node A is sending its reference to nodes B and C. However, since there is a wormhole link between C and G, G can locally replay the location reference of A in its neighborhood, misleading node F. Consequently, F will compute its location incorrectly. Intuitively, wormhole attacks pose more serious problems in range-free localization compared to range-based localization.

6 Existing Secure Localization Systems

In this section we review the existing secure localization techniques, throwing light on their strengths and weaknesses.

6.1 SeRLoc

In [27], Lazos and Poovendran propose a novel scheme for localization of nodes in WSNs in untrusted environments called SeRLoc. SeRloc is a range-free, distributed, resource-efficient localization technique in which there is no communication requirement between nodes for location discovery. SeRLoc is robust against wormhole attacks, sybil attacks and sensor compromise. SeRLoc considers two sets of nodes: N, which is the set of sensor nodes equipped with omnidirectional antennas, and L, which is the set of locator nodes equipped with directional antennas. The sensors determine their location based on the location information transmitted by these locators. Each locator transmits different beacons at each antenna sector with each beacon containing two pieces of information: the locator coordinates and the angles of the antenna boundary lines with respect to a common

global axis. Using directional antennas improves the localization accuracy.

In SeRLoc, an attacker has to impersonate several beacon nodes to compromise the localization process. Also, since sensor nodes compute their own location without any assistance from other sensors, the adversary has no incentive to impersonate sensor nodes. Wormhole attacks are thwarted in SeRLoc due to two unique properties: sector uniqueness property and communication range violation property. In SeRLoc, to improve the localization accuracy, either more locators have to be deployed or more directional antennas have to be used. The authors also make an assumption that no jamming of the wireless medium is feasible. This is a very strong assumption for a real world setting.

6.2 Beacon Suite

In [29], Liu, Ning, and Du present a suite of techniques for detecting malicious beacon nodes that provide incorrect information to sensor nodes providing location services in critical applications. Their suite includes detection of malicious beacon signals, detection of replayed beacon signals, identification of malicious beacon nodes, avoidance of false detection, and finally the revoking of malicious beacon nodes. They use beacon nodes for two purposes: to provide location information to sensor nodes, and to perform detection on the beacon signals it hears from other beacon nodes. A beacon node does not necessarily need to wait passively to hear beacon signals. It can request location information. The beacon node performing the detection is called the *detecting node* and the beacon node being detecting is called the *target node*. They suggest that the detecting node should use a non-beacon ID when requesting location information from a target node in order to observe the true behavior of the target node.

Their revocation scheme works on the basis of two counters maintained for each beacon node, namely *alert counter* and *report counter*. The alert counter records the suspiciousness of the corresponding beacon node and the report counter records the number of alerts this node reported and was accepted by the base station. When a detecting node determines that a target node is misbehaving, it reports to the base station. Alert reports are accepted only from detecting nodes whose report counter is below a threshold and against nodes that are not yet revoked. When this criteria is met, the report counter and the alert counter of the detecting and the target node, respectively, are incremented. These two counters work on a discrete scale and the revocation mechanism is centralized. This has been improved to be more robust in [36] by employing a continuous scale and a reputation and trust-based mechanism.

6.3 Attack Resistant Location Estimation

In [30], Liu, Ning, and Du put forward two range-based robust methods to tolerate malicious attacks against beacon-based location discovery in sensor networks. The first method, attack-resistant Minimum Mean Square Estimation, filters out malicious beacon signals. This is accomplished by examining the inconsistency among location references of different beacon signals, indicated by the mean square error of estimation, and defeats malicious attacks by removing such malicious data. The second method, voting-based location estimation quantizes the deployment field into a grid of cells and has each location reference 'vote' on the cells in which the node may reside. This method tolerates malicious beacon signals by adopting an iteratively refined voting scheme. Both methods survive malicious attacks even if the attacks bypass authentication.

However, there is a downside to both of these techniques. In the proposed localization technique, an attacker cannot dislodge sensors by compromising a few range estimates. Nonetheless, this localization model fails if the attacker can compromise a simple majority of range estimates. Assume there are k nodes in a neighborhood. Now, if the attacker can compromise $\lfloor \frac{k}{2} \rfloor + 1$ beacon nodes in that neighborhood, then he can generate more malicious location references than benign ones. This will lead to failure of the minimum mean square estimation technique in the neighborhood, the effects of which can propagate throughout the network. Similar attacks are possible for the voting-based location estimation technique.

6.4 Robust Statistical Methods

In [31], Li, Trappe, Zhang, and Nath introduced the idea of being tolerant to attacks rather than trying to eliminate them by exploiting redundancies at various levels within wireless networks. They examine two classes of localization: *triangulation* and *RF-based fingerprinting*. They have presented two statistical methods for securing localization in sensor networks. Both methods are based on the simple idea of filtering out outliers in the range estimates used for location estimation used by sensors.

For the *triangulation*-based localization, they propose to use an adaptive least squares and least median squares estimator. This adaptive estimator switches to the robust mode with least mean squares estimation when attacked and enjoys the computational advantage of least squares in the absence of attacks. For the *fingerprinting*-based method, the traditional Euclidean distance metric is not secure enough. Hence, they propose a median-based nearest neighbor scheme that is robust to location attacks. In this paper, the authors have also discussed attacks that

are unique to localization in sensor networks. The statistical methods proposed in [31] are based on the assumption that benign observations at a sensor always outnumber malicious observations. This is a strong assumption in a real word setting where an attacker can launch sybil attacks or even wormhole attacks to outnumber the benign observations.

6.5 SPINE

In [32], Capkun and Hubaux devise secure positioning in sensor networks (SPINE), a range-based positioning system based on verifiable multilateration which enables secure computation and verification of the positions of mobile devices in the presence of attackers. SPINE works by bounding the distance of each sensor to at least three reference points. Verifiable multilateration relies on the property of distance bounding, that neither the attacker nor the claimant can reduce the measured distance of the claimant to the verifier, but only enlarge it. By using timers with nanosecond precision, each sensor can bound its distance to any reference point within range.

If the sensor is within a triangle formed by three reference points, it can compute its position via verifiable multilateration, which provides a robust position estimate. This is based on a strong assumption that any attacker does not collude with compromised nodes. Verifiable multilateration effectively prevents location spoofing attacks, wormhole and jamming attacks, and prevents dishonest nodes from lying about their positions. However, SPINE has some drawbacks. In order to perform verifiable multilateration, a high number of reference points is required. SPINE is a centralized approach which creates bottle-neck at the central authority or the base station. Also, it is very unlikely that an attacker will not try to collude

with other compromised nodes.

6.6 ROPE

Lazos, Poovendran, and Capkun design ROPE [33], a robust positioning system in WSNs. ROPE, a hybrid algorithm, has a two-fold benefit to the system. First, it allows sensors to determine their location without any centralized computation. Second, ROPE provides a location verification mechanism by virtue of which the location claims of sensors can be verified prior to data collection. In ROPE, the network consists of two types of nodes: sensors and locators. Each sensor shares a pairwise key with every locator. Since the number of locators is less, it does not impose a large storage overhead on the sensors.

To measure the impact of attacks on ROPE, they introduce a novel metric called Maximum Spoofing Impact. ROPE achieves a significantly lower Maximum Spoofing Impact while requiring the deployment of a significantly smaller number of reference points, compared to [32]. ROPE is second to only [32] to propose a solution for jamming attacks. ROPE is also resilient to wormhole attacks and node impersonation attacks. The robustness of ROPE has been confirmed via analysis and simulation.

6.7 Transmission Range Variation

In [34], Anjum, Pandey, and Agrawal show a novel transmission-based secure localization technique for sensor networks. They have presented a Secure Localization Algorithm (SLA). Their technique does not demand any special hardware and considers a network with two sets of nodes: the sensor nodes and the beacon nodes. Their scheme works as follows. Beacon nodes associate unique nonce to different

power levels at a given time which they transmit securely at the associated power level. As a result, each sensor node receives a set of unique nonce which it will have to transmit back to the sink via the beacon nodes. Then the location of the sensor node can be estimated securely, based on this set of nonce. This is a centralized localization technique where the sink determines the location of the sensor node.

This model has a few drawbacks. The authors have not considered the collaboration of sensor nodes which is very crucial and has to be addressed to suit the real world scenario. They have also assumed that all beacon nodes in the network and the sink are to be trusted and assumed the encryption between beacon nodes and sink to be stronger than that between sensor nodes and sink. They have shown that their model is resilient to replay attacks, spoofing attacks, modification attacks and response delay attacks. Another major drawback arises from the fact that this a centralized model with the base station as the single point of failure. This also causes a significant bottleneck at the base station.

6.8 DRBTS

DRBTS [36] is a distributed reputation and trust-based security protocol aimed at providing a method for secure localization in sensor networks. This work is an extension of [29]. In this model, incorrect location information provided by malicious beacon nodes can be excluded during localization. This is achieved by enabling beacon nodes to monitor each other and provide information so that sensor nodes can choose who to trust, based on a quorum voting approach. In order to trust a beacon node's information, a sensor must get votes for its trustworthiness from at least half of their common neighbors. Specifically, sensor nodes use a simple

majority principle to evaluate the published reputation values of all the beacon nodes in their range.

With this model, it is clearly demonstrated that sensors can accurately guess the misbehaving/non-misbehaving status of any given beacon node, given a certain assumption about the level of corruption in the system. Authors also show that their system grows in robustness as node density increases, and show through simulations the effects of different system parameters on robustness. This distributed model not only alleviates the burden on the base station to a great extent, but also minimizes the damage caused by the malicious nodes by enabling sensor nodes to make a decision on which beacon neighbors to trust, on the fly, when computing their location.

6.9 HiRLoc

Lazos and Poovendran propose another model, a high-resolution, range-independent localization technique called HiRLoc [37]. In HiRLoc, sensors passively determine their location without any interaction amongst themselves. HiRLoc also eliminates the need for increased beacon node density and specialized hardware. It is robust to security threats like wormhole attacks, sybil attacks and compromising of the network entities by virtue of two special properties: antenna orientation variation and communication range variation. In HiRLoc, Lazos and Poovendran have used cryptographic primitives to ensure the security of beacon transmissions. Here, each beacon transmission is encrypted using a global symmetric key, an idea very similar to the one used in [36].

Unlike SeRLoc, in HiRLoc, sensors receive multiple beacons from the same locator. This relaxation helps in improving the accuracy of location estimation.

There are two important observations. First, since no range measurements are required for localization, they are free from attacks aiming at altering the measurements, like jamming to increase hop count. Second, since sensors do not rely on other sensor nodes for computing their location, it is robust to sensor compromise attacks.

7 Summary

Sensor location is vital for many critical applications like battlefield surveillance, target tracking, environmental monitoring, wildfire detection, and traffic regulation. Localization has three important metrics: *energy efficiency*, *accuracy*, and *security*. Though the first two metrics have drawn the attention of researchers for nearly a decade, the security metric has been addressed only recently. In this chapter we have discussed the unique operational challenges faced by WSNs, presented a comprehensive overview of the localization process, and discussed the three localization techniques: triangulation, trilateration, and multilateration. We have also delineated the security requirements of localization, and discussed the merits and demerits of both range-based and range-free localization models that have been proposed as an effective alternative for GPS-based localization. The attacker model and attacks specific to localization have also been discussed in detail. Finally, we conclude the chapter with a survey of all secure localization techniques proposed thus far. This chapter is intended to serve as a single point of reference to researchers interested in secure localization in WSNs.

8 Acknowledgements

We would like to thank the anonymous reviewers for their valuable feedback on the contents and organization of this chapter. This work was supported in part by NSF grants, ANI 0073736, EIA 0130806, CCR 0329741, CNS 0422762, CNS 0434533, CNS 0531410, and CNS 0626240.

References

[1] B. H. Wellenhoff, H. Lichtenegger and J. Collins. Global Positions System: Theory and Practice. *Fourth Edition. Springer Verlag*, 1997.

[2] J. C. Navas and T. Imielinski. Geographic Addressing and Routing. *In Proceedings of MOBICOM '97*, Budapest, Hungary, September 26, 1997.

[3] Y.-B. Ko and N. H. Vaidya. Location-Aided Routing (LAR) in Mobile Ad Hoc Networks. *In the Proceedings of MobiCom '98*, 1998.

[4] A. Harter, A. Hopper, P. Steggles, A.Ward, and P.Webster. The anatomy of a context-aware application. *In Proceedings of the MOBICOM '99*, 1999.

[5] R. Nagpal. Organizing a Global Coordinate System from Local Information on an Amorphous Computer. *A.I. Memo1666*, MIT A.I. Laboratory, August 1999.

[6] B. Karp and H. T. Kung. Greedy Perimeter Stateless Routing. *In the Proceedings of MobiCom '00*, 2000.

[7] J. Hightower, G. Boriello, and R.Want. SpotON: An Indoor 3D Location Sensing Technology Based on RF Signal Strength. *Technical Report 2000-02-02*, University of Washington, February 2000.

[8] N. Bulusu, J. Heidemann, and D. Estrin. GPS-less low cost outdoor localization for very small devices. *In IEEE Personal Communications Magazine*, 7(5):28-34, October 2000.

[9] N. B. Priyanath, A. Chakraborty, and H. Balakrishna. The cricket location-support system. *In Mobile Computing and Networking*, 2000.

[10] P. Bahl and V. N. Padmanabhan. RADAR: An In-Building RF-Based User Location and Tracking System. *In Proceedings of the IEEE INFOCOM '00*, March 2000.

[11] M. Mauve, J. Widmer and H. Hartenstein. A Survey on Position-Based Routing in Mobile Ad Hoc Networks. *IEEE Network Magazine*, 2001.

[12] L. Doherty, K. S. Pister, and L. E. Ghaoui. Convex optimization methods for sensor node position estimation. *In Proceedings of IEEE INFOCOM '01*, 2001.

[13] Y. Yu, R. Govindan, and D. Estrin. Geographical and energy aware routing: A recursive data dissemination protocol for wireless sensor networks. *Technical Report UCLA/CSD-TR-01-0023*, UCLA, Department of Computer Science, May 2001.

[14] A. Savvides, C. Han, and M. Srivastava. Dynamic fine-grained localization in ad-hoc networks of sensors. *In Proceedings of ACM MobiCom '01, pages 166-179*, July 2001.

[15] Y. Xu, J. Heidemann and D. Estrin. Geography-Informed Energy Conservation for Ad Hoc Routing. *In Proceedings of MOBICOM '01*, Rome, Italy, July 2001.

[16] D. Niculescu and B. Nath. Ad Hoc Positioning Systems (APS). *In Proceedings of IEEE GLOBECOM '01*, November 2001.

[17] C. Savarese, J. Rabay and K. Langendoen. Robust Positioning Algorithms for Distributed Ad-Hoc Wireless Sensor Networks. *USENIX Technical Annual Conference*, Monterey, CA, June 2002.

[18] A. Savvides, H. Park, and M. Srivastava. The bits and flops of the n-hop multilateration primitive for node localization problems. *In Proceedings of ACM WSNA '02*, September 2002.

[19] A. Nasipuri and K. Li. A directionality based location discovery scheme for wireless sensor networks. *In Proceedings of ACM WSNA '02*, September 2002.

[20] T. Yan, T. He, and J. A. Stankovic. Differentiated Surveillance Service for Sensor Networks. *In Proceeding of First ACM Conference on Embedded Networked Sensor Systems (SenSys '03)*, Los Angeles, CA 2003.

[21] N. Patwari, A. O. Hero, M. Perkins, N. S. Correal, and R. J. ODea. Relative Location Estimation in Wireless Sensor Networks. *IEEE Transactions on Signal Processing*, VOL. 51, NO. 8, AUGUST 2003

[22] R. Nagpal, H. Shrobe, and J. Bachrach. Organizing a global coordinate system from local information on an ad hoc sensor network. *In the 2nd International Workshop on Information Processing in Sensor Networks (IPSN '03)*, Palo Alto, April, 2003.

[23] T. He, C. Huang, B. M. Blum, J. A. Stankovic, and T. F. Abdelzaher. Range-free localization schemes in large scale sensor networks. *In Proceedings of ACM MobiCom '03*, 2003.

[24] D. Niculescu and B. Nath. DV Based Positioning in Ad Hoc Networks. *In Journal of Telecommunication Systems*, 2003.

[25] D. Niculescu and B. Nath. Ad Hoc Positioning System (APS) using AoA. *In Proceedings of IEEE INFOCOM '03*, San Francisco, CA, USA, 2003.

[26] H. Gupta, S. R. Das, and Q. Gu. Connected Sensor Cover: Self-Organization of Sensor Networks for Efficient Query Execution. *In Proceeding of MobiHoc '03*, Annapolis, Maryland, June 2003.

[27] L. Lazos and R. Poovendran. SeRLoc: Secure range independent localization for wireless sensor networks. *In ACM workshop on Wireless security (ACM WiSe '04)*, Philadelphia, PA, October 1 2004.

[28] C. Liu and K. Wu. Sensor Localization with Ring Overlapping Based on Comparison of Received Signal Strength Indicator. *Proceedings of The 1st IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS '04)*, Fort Lauderdale, Florida, October, 2004.

[29] D. Liu, P. Ning, and W. Du. Detecting Malicious Beacon Nodes for Secure Location Discovery in Wireless Sensor Networks. *25th IEEE International Conference on Distributed Computing Systems (ICDCS '05)*, pp. 609-619, 2005.

[30] D. Liu, P. Ning, W. Du. Attack-Resistant Location Estimation in Sensor Networks. *In Proceedings of The Fourth International Conference on Information Processing in Sensor Networks (IPSN '05)*, pages 99-106, April 2005.

[31] Z. Li, W. Trappe, Y. Zhang, and B. Nath. Robust statistical methods for securing wireless localization in sensor networks. *In Proceedings of IPSN '05*, 2005.

[32] S. Capkun and J.-P. Hubaux. Secure positioning of wireless devices with application to sensor networks. *In Proceedings of IEEE INFOCOM '05*, 2005.

[33] L. Lazos, R. Poovendran, and S. Capkun. ROPE: Robust Position Estimation in Wireless Sensor Networks. *In the Proceedings of the 4th international symposium on Information processing in sensor networks, IPSN '05*, 2005.

[34] F. Anjum, S. Pandey, P. Agrawal. Secure localization in sensor networks using transmission range variation. *2nd IEEE International Conference on Mobile Adhoc and Sensor Systems, MASS '05*, pp. 195-203, November 2005.

[35] A. Savvides, W. L. Garber, R. L. Moses, and M. B. Srivastava. Analysis of Error Inducing Parameters in Multihop Sensor Node Localization. *IEEE Transactions on Mobile Computing*, VOL. 4, NO. 6, November/December 2005

[36] A. Srinivasan, J. Teitelbaum, J. Wu. DRBTS: Distributed Reputation-based Beacon Trust System. *2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing (DASC '06)*, pp. 277-283, 2006.

[37] L. Lazos and R. Poovendran. HiRLoc: High-Resolution Robust Localization for Wireless Sensor Networks. *IEEE Journal on Selected Areas in Communications*, VOL. 24, NO. 2, February 2006.