Securing Wireless Localization: Living with Bad Guys

Zang Li, Yanyong Zhang, Wade Trappe*
Wireless Information Network Laboratory (WINLAB)
Rutgers University
73 Brett Rd., Piscataway, NJ 08854

Badri Nath**
Computer Science Department
Rutgers University
110 Frelinghuysen Rd., Piscataway, NJ 08854

I. Introduction

The infrastructure provided by wireless networks promises to have a significant impact on the way computing is performed. Not only will information be available while we are on the go, but new location-aware computing paradigms along with location-sensitive security policies will emerge. Already, many techniques have emerged to provide the ability to localize a communicating device [**?**], [1]–[4].

Enforcement of location-aware security policies (e.g., this laptop should not be taken out of this building, or this file should not be opened outside of a secure room) requires trusted location information. As more of these location-dependent services get deployed, the very mechanisms that provide location information will become the target of misuse and attacks. Therefore, as we move forward with deploying wireless systems that support location services, it is prudent to integrate security into the protection of localization techniques.

The purpose of this paper is to examine the problem of secure localization from a viewpoint different from traditional network security services. In addition to the different attacks and misuse faced by wireless localization mechanisms, it is our viewpoint that these vulnerabilities can be mitigated by exploiting the redundancy present in typical wireless deployments. Rather than introducing countermeasures for every possible attack, our approach is to provide *localization-specific*, *attack-tolerant* mechanisms that shield the localization infrastructure from threats that bypass traditional security defenses. The idea is to live with bad nodes rather than eliminate all possible bad nodes.

II. Attacks Unique to Localization

Broadly speaking, there are two main categories of localization techniques: those that involve range estimation, and those that do not [1]. These different localization methods are built upon the measurement of some basic properties. In Table I, we enumerate several properties that are used by localization algorithms, along with different threats that may be employed against these properties. The threats that we describe are primarily non-cryptographic threats, though it should be recognized that some attacks may be difficult to classify exclusively as a cryptographic or non-cryptographic threat.

We now explore several of these threats. Due to space limitations, we leave the discussion of other threats for an expanded follow-up paper. We start by looking at methods that employ time of flight. The basic concept behind time of flight methods is that there is a direct relationship between the distance between two points, the propagation speed, and the duration needed for a signal to propagate between these two points. For time of flight methods, an attacker may try to bias the estimation of distance to a larger value by forcing the observed signal to come from a multipath. This may be accomplished by placing a barrier sufficiently close to the transmitter and effectively removing the line-of-sight signal. Another technique that may be used to falsely increase the distance estimate occurs in techniques employing round-trip time of flight. Here, an adversarial target that does not wish to be located by the network, receives a transmission and holds it for a short time before retransmitting. An attack that skews the distances to smaller values can be accomplished by exploiting the propagation speed of different media. For example, in CRICKET [2], the combination of an RF signal and an ultrasound signal allows for the estimation of distance since the acoustic signal travels at a slower propagation velocity. An adversary located near the target may therefore hear the RF signal and then transmit an ultrasound signal that would arrive before the original ultrasound signal can reach the receiver [5].

As another example, consider a range-based location system that uses signal strength as the basis for location. Such a system is very closely tied to the underlying physical-layer path loss model that is employed (such as a free space model where signal strength decays in inverse proportion to the square of distance). In order to attack such a system, an adversary could introduce an absorbing barrier between the transmitter and the target, changing the underlying propagation physics. As the signal propagates through the barrier, it is attenuated, and hence the target would observe a significantly lower received signal strength. Consequently, the receiver would conclude that it is further from the transmitter than it actually is.

Hop count based localization schemes [6] usually consist of two phases. In the first phase, per-hop distance is measured. In the second phase, anchor points flood beacons to individual sensor nodes, which count the number of hops between them, and these hop counts are translated into physical distances. As a result, adversaries can initiate attacks as follows: (1) manipulate the hop count measurement, and (2) manipulate the translation from hop count to physical distance. A number of tricks can be played to tweak hop count measurements, ranging from PHY-layer attacks, such as increasing/decreasing transmission power, to network layer attacks that tamper with the routing path. Since PHY-layer attacks have been discussed earlier, we now focus on discussing the possible network layer attacks, namely, jamming and wormholes [7]. By jamming a certain area between two nodes, beacons may take a longer route to reach the other end (as shown in Figure 1), which increases the measured hop count. While jamming may not always increase the hop count, for it may not block the shortest path between the two nodes, the other type of attacks, which involve wormhole links, are more harmful because they can often significantly shorten the shortest path and result in a much smaller hop count. Figure 1 illustrates such a scenario: the shortest path between anchor L and node A has 7 hops, while the illustrated wormhole brings the hop count down to 3. Similarly, these attacks can also affect the translation from hop count to physical distance. In addition, if adversaries can manage to physically remove or displace some sensor nodes, even correct hop counts are not useful for obtaining accurate location calculations.

Localization methods that use neighbor location are built upon the implicit assumption that neighbors are uniformly distributed in space around the wireless device. These localization methods, such as the Centroid method or SerLoc [4], can be attacked by altering the shape of the received radio region. For example, an attacker can shrink the effective radio region through blocking some neighbors by introducing a strong absorbing barrier around several neighbors. Another approach to shrinking the radio region is for an adversary to employ a set of strategically located jammers. Since these neighbors are not heard by the wireless device, the location estimate will be biased toward the unblocked side.

III. Live with Bad Guys: Attack-tolerant Strategies

As discussed in the previous section, wireless networks are exposed to numerous localization-specific attacks. Solutions that can combat some of these attacks have been proposed, often involving

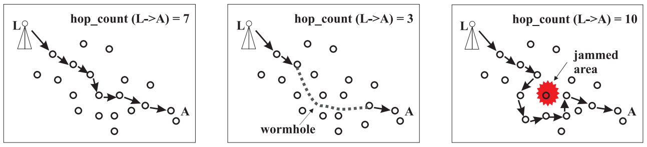

Fig. 1. (Left) Operation of localization using hop count, (Middle) Wormhole attack on hop count methods, and (Right) Jamming attack on hop count methods.

*The authors may be contacted by e-mail at zang, yyzhang, trappe@winlab.rutgers.edu

**The author may be contacted by e-mail at badri@cs.rutgers.edu

Property	Example Algorithms	Attack Threats
Time of Flight	Cricket	Remove direct path and force radio transmission to employ a multipath; Delay transmission of a response message; Exploit difference in propagation speeds (speedup attack, transmission through a different medium).
Signal Strength	RADAR, SpotON, Nibble	Remove direct path and force radio transmission to employ a multipath; Introduce different microwave or acoustic propagation loss model; Transmit at a different power than specified by protocol; Locally elevate ambient channel noise.
Angle of Arrival	APS	Remove direct path and force radio transmission to employ a multipath; Change the signal arrival angel by using reflective objects, e.g., mirrors; Alter clockwise/counter-clockwise orientation of receiver (up-down attack).
Region Inclusion	APIT, SerLoc	Enlarge neighborhood by wormholes; Manipulate the one-hop distance measurements; Alter neighborhood by jamming along certain directions.
Hop Count	DV-Hop	Shorten the routing path between two nodes through wormholes; Lengthen the routing path between two nodes by jamming; Alter the hop count by manipulating the radio range; Vary per-hop distance by physically removing/displacing nodes.
Neighbor Location	Centroid Method, SerLoc	Shrink radio region (jamming); Enlarge radio region (transmit at higher power, wormhole); Replay; Modify the message; Physically move locators; Change antenna receive pattern.

TABLE I

PROPERTIES EMPLOYED BY DIFFERENT LOCALIZATION ALGORITHMS AND ATTACKS THAT MAY BE LAUNCHED AGAINST THESE PROPERTIES.

conventional encryption techniques. In this study, we take the viewpoint that instead of coming up with solutions for each attack, we should learn how to make localization function properly even with the presence of these attacks. The main idea is to take advantage of the redundancy in both the wireless deployment and the underlying properties to help localization techniques:

1) **Multimodal Localization Strategies:** Most current localization techniques employ only a single property at a time, thereby facilitating attacks by an adversary that target a single property. It should be realized, however, that there are correlations between the different properties that might not be maintained by attacking a single property. It is possible to exploit several properties simultaneously to corroborate each other and improve the robustness of localization.
2) **Robust Statistics:** We can employ robust statistical estimation and data cleansing methods to ignore the wrong values introduced by adversaries. Many of the localization schemes have the property whereby an adversary may introduce values that significantly differ from true values, while if the adversary introduces values that are not significantly different from the true values, the effect on localization will be minimal. Therefore, robust statistical methods that are stable in the presence of outliers, or identify outliers and perform data cleansing are desirable for localization.

We now provide an example of each of these strategies.

Multimodal Techniques: Attacks on localization methods utilizing neighbor locations, such as the centroid method, generally involve modifying the neighbor list of the sensor. One way to combat these attacks is to deploy both neighbor location *and* a two-sector antenna on each sensor. The sensor knows the direction of the global axis so that it can align its antenna section border to the x-axis or y-axis. To get its coordinates, the sensor first aligns its antenna to the x-axis, as shown in Figure 2. Then every neighbor heard in the upper sector should have a larger y-coordinate than that of the sensor, while every neighbor heard in the lower sector should have a smaller y-coordinate. The sensor could estimate its own y-coordinate by simply averaging the smallest y-coordinate in the upper neighbors and the largest y-coordinate in the lower neighbors. If no neighbor is heard in a sector, say the upper sector, the sensor estimates its own y-coordinate as the largest y-coordinate in the lower neighbors. Similarly, the sensor's x-coordinate can be estimated. In this scheme, only the neighbors that are closest to the sensor in the x-coordinate or y-coordinate will affect the estimation. When wrong neighbor information is injected by an attacker, if the forged neighbor is far away from the sensor in both coordinate, it has no effect at all. If it's close in a coordinate, it won't hurt the estimation much. Similar statement holds for jamming attack (blocking could occur naturally due to border effect as well). On the other hand, if the attacker tries to harm the sensor's orientation capability, it can be easily detected since the neighbor coordinate rule will not hold when the antenna orientation is not aligned to the global axis. Therefore, the extra information provided by the sectored antenna enhances the robustness of the localization significantly.

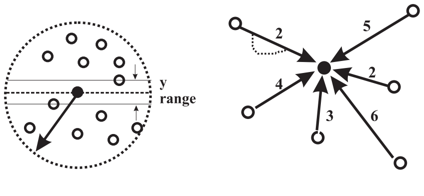

Fig. 2. Left figure depicts a scenario where use of a sectored antenna allows one to narrow y-value region. Right figure depicts a wormhole attack that introduces a false hop value in DV-hop.

Robust Statistics: Consider an attack on a hop-based scheme, such as DV-hop [6], where an adversary alters the hop count, perhaps through a wormhole attack (as depicted in Figure 2). In such an attack, only *significantly* altered hop counts will result in noticeable error in the output location. Following the flooding of beacons by anchor points, a collection of $\{(x, y, h)\}$ values results, where h represents the hop count to an anchor at (x, y). Ideally, these $\{(x, y, h)\}$ values map out a parabolic surface $h(x, y)$ whose minimum value (x_0, y_0) is the wireless device location, and solving for (x_0, y_0) is a simple least squares problem. However, in the presence of possible outliers resulting from misinformation from adversaries, solving for (x_0, y_0) should employ robust statistical estimation. A natural approach is to employ least median of squares (LMedS). LMedS, however, is a computationally intensive scheme and an efficient and statistically robust alternative would involve solving random subsets of $\{(x, y, h)\}$ values to get several candidate (x_0, y_0) values. These candidates may then be clustered and a robust centroid may be found using order statistics.

IV. CONCLUSION

As wireless networks are increasingly deployed for location-based services, these networks are becoming more vulnerable to misuses and attacks that can lead to false location calculation. Towards the goal of securing localization, this paper has made two main contributions. It first enumerates a list of novel attacks that are unique to wireless localization algorithms. Further, this paper proposes the idea of tolerating attacks, instead of eliminating them, by exploiting redundancies at various levels within wireless networks.

REFERENCES

[1] K. Langendoen and N. Reijers, "Distributed localization in wireless sensor networks: a quantitative comparison," *Comput. Networks*, vol. 43, no. 4, pp. 499–518, 2003.

[2] N. Priyantha, A. Chakraborty, and H. Balakrishnan, "The CRICKET location-support system," 2000, pp. 32–43.

[3] D. Nicelescu and B. Nath, "Ad hoc positioning (APS) using AOA," 2003, pp. 1734 – 1743.

[4] L. Lazos and R. Poovendran, "SeRLoc: Secure range-independent localization for wireless sensor networks," in *Proceedings of the 2004 ACM Workshop on Wireless Security*, 2004.

[5] S. Capkun and J.P. Hubaux, "Secure positioning in sensor networks," Technical report EPFL/IC/200444, May 2004.

[6] D. Nicelescu and B. Nath, "DV based positioning in ad hoc networks," *Telecommunication Systems*, vol. 22, no. 1-4, pp. 267–280, 2003.

[7] Y.C. Hu, A. Perrig, and D. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in *Proceedings of IEEE Infocom 2003*, 2003, pp. 1976–1986.