A Survey of Forensic Localization and Tracking Mechanisms in Short-Range and Cellular Networks

Saif Al-Kuwari[1] and Stephen D. Wolthusen[1,2]

[1] Information Security Group, Department of Mathematics, Royal Holloway, University of London, Egham Hill, Egham TW20 0EX, United Kingdom
[2] Norwegian Information Security Laboratory, Gjøvik University College, P.O. Box 191, N-2802 Gjøvik, Norway

Abstract. Localization and tracking are critical tools in criminal and, increasingly, forensic investigations, which we show to be greatly aided by the proliferation of mobile phone and other wireless devices even if such devices are not suitable for communication and hence interception. In this paper we therefore provide a survey and taxonomy of both established and novel techniques for tracking the whereabouts of individuals and devices for different environments and platforms as well as the underlying assumptions and limitations in each case. In particular, we describe cellular, wireless, and personal area networks in infrastructure and ad-hoc environments. As individual localization and tracking methods do not always yield the required precision and accuracy, may require collaboration, or will exhibit gaps in densely built-up or highly active radio frequency environments, we additionally discuss selected approaches derived from multisensor data fusion and tracking applications for enhancing performance and assurance. This paper also briefly discusses possible attacks against a localization/tracking process and how trustworthy the measurement estimations are, an aspect that has been evidently less investigated so far.

Keywords: Radio Frequency Localization, Tracking, Localization Fusion, Sensor Networks, Cellular Networks.

1 Introduction

Given its numerous civil and military applications, localization and tracking of static or mobile objects has long been an important area of research. In this paper, we provide a survey of approaches applicable to criminal and forensic application areas based on different frequency domains and communication mechanisms. Generally, locating or tracking an object can either be object-based or network-based. While in the former case, the object localizes itself using various localization techniques, in the latter, the surrounding (reference) objects localize a target — this kind of localization can be active, where the reference objects collaborate with the target to localize/track it, or passive, where the reference

S. Goel (Ed.): ICDF2C 2009, LNICST 31, pp. 19–32, 2010.

objects clandestinely localize/track the target by observing its emissions and movement pattern. We review various localization and tracking techniques in different environments considering their applicability and limitations. These localization and tracking approaches are especially important in forensic applications and can also be used for scene reconstruction after the fact. An equally important, yet slightly overlooked, aspect of these approaches is how trustworthy they are and the kind of attacks that can possibly mislead the tracking/localization algorithms.

2 Related Work

The importance of understanding how various localization techniques are being implemented in different types of wireless networks motivated other researchers to write similar surveys. Hightower *et al.* [1,2,3] presented a series of related papers defining and introducing some of the most fundamental concepts in wireless networks localization, such as triangulation, trilateration, location proximity and scene analysis.

Pandy *et al.* [4] presented a thorough classification model for localization techniques and showed how some examples of real localization systems can fit in their model. The authors based their classification on some of the most influential factors on the accuracy of localization, like environment (indoor vs. outdoor). The authors classified localization techniques based on: area of deployment, physical layer technology, measurement parameters, type of lookup table, estimation technique, localization entity and security parameters.

In his survey, Gezici [5] discussed several popular localization algorithms in wireless networks. Gazici developed his discussion based on a two-step localization procedure. First, parameters like RSS, are estimated, and then, a geometric (triangulation/trilateration) or statistical approach is adopted to estimate the actual location of the target. Statistical estimation methods can be parametric like Bayesian and Maximum Likelihood (ML), or nonparametric like k-NN (k-Nearest-Neighbor), SVR (Support Vector Regression) and neural networks.

Srinivasan *et al.* [6] discussed security issues and requirements of the localization techniques in wireless sensor networks. Security requirements in sensor networks do not significantly differ from such requirements in other types of networks, including: authentication, integrity, availability, non-repudiation and privacy, which the author evaluated for selected localization schemes.

3 Localization in Sensor Networks

Most of the sensor networks localization techniques are generic and are being used in cellular networks too, but the inverse it is not always true. A target object can be localized in reference of other objects, with known location, in several ways. Geometrically, and in 2 dimensions, object T (target) can be localized if the distance and/or angles between T and some reference objects can be accurately measured. In particular, an object T can be localized in two steps: (i) measuring

the distances/angles between T and other reference objects with known location, then (ii) apply a geometric process to determine the location of T. In the following subsections, we first discuss the various distance/angle measurements techniques (section 3.1) and then introduce some geometric approaches to estimate the location of an object (section 3.2); statistical localization approaches are not discussed in this paper, see [7].

3.1 Parameter Measurement

In this section we discuss some of the most popular techniques for measuring the distance/angle between two or more objects, typically, a single transmitter and a single or multiple receivers.

Received Signal Strength. The distance between a transmitter and a receiver can be estimated by measuring the strength of the transmitter's signal as it is received by the receiver [8]. Ideally, and for a direct line of sight (LOS)[1] scenario, the power of the signal is approximately equals to $1/d^2$, where d is the distance between the transmitter and the receiver. However, environmental and other factors can potentially affect the Received Signal Strength (RSS) measurements making it a nonlinear measure. RSS is sometimes referred to as RSSI (Received Signal Strength Indicator/Indication) when used in cellular network context. However, in most of the literature as well as in this paper, RSS and RSSI are used interchangeably.

Time of Arrival. TOA, also known as Time of Flight (TOF), is a measure of the time a signal travels from an object (transmitter) to another (receiver). In order to correctly calculate TOA, both the transmitter and the receiver have to be synchronized either by referring to a global clock or by exchanging time synchronization information. Once the TOA is measured, the distance between the two objects can be estimated by the distance equation: $d = v.t$ where d is the distance, v is the speed of the signal and t is TOA. In free space, the speed of the signal is approximately equal to the speed of light (around 300,000 km/s). The accuracy of both RSS and TOA largely depends on environment modeling. In urban environments, the non-line of sight (NLOS) situation is very likely where obstacles (natural or human-built) block the direct path between the transmitter and the receiver; ways to mitigate the effect of NLOS exist [9]. Round Tripe Time of Arrival (RT-TOA) [10] is a variant of TOA employed in systems where full time synchronization is not provided or guaranteed. Basically, in RT-TOA an object P_1 sends a signal to object P_2 at time t_1. P_2 then replies back to object P_1 which receives the reply at time t_2. Finally, the RT-TOA is approximately $t_2 - t_1$. Usually, RT-TOA neglects delays, like processing delay, if such delays are likely to be insignificant. However, these delays can be accounted for by adding a a random variable to the estimate time.

[1] The transmission between two entities is said to be in a line of sight when it is not blocked or affected by obstacles on its way from the transmitter to the receiver.

Time Difference of Arrival. In TDOA, only reference objects have to be synchronized [11], this is in contrast to TOA measurements where synchronization is required among both the reference and target objects. TDOA measures the time difference of a signal received at different reference objects. To localize an object in 2D, at least three reference objects are required (4 objects for 3D). First, the TDOA between the target object and two reference objects form a hyperbola where the target object is located, with the two reference objects being foci[2]. A third reference object adds a second hyperbola where the intersection of the two hyperbolas is the location of the target object. TSOA (Time Sum of Arrival) is based on a similar approach where the sum of the TOA at several reference points forming ellipsoids intersecting at the target's location [12].

Angle of Arrival. In AOA, the reference objects measure the angle between the arriving signals emitted by the target object and a reference direction known as *orientation* [13]. AOA is severely affected by the NLOS conditions; under these conditions, signals received are not necessarily coming from the direction where they were originally transmitted by the target. Antenna arrays are required to measure AOA which not all standard sensor nodes are necessarily equipped with; this makes its adoption as a primary location technique in ad hoc and PAN networks slightly expensive. Another way to measure AOA is when a receiving object has more than one integrated directional antenna. In this case, the AOA is the RSS ratio between at least two of the antennas [14]; but this is still a rather expensive requirement.

3.2 Geometric Location Estimation

After measuring the distances between the reference and the target objects as discussed above, the location of the target object can be geometrically estimated by either triangulation (based on AOA measurements), trilateration (based on TOA or RSS measurements) or multi-lateration (based on TDOA measurements).

Triangulation. In triangulation [15], an object is localized based on AOA measurements from two reference objects. Figure 1 illustrates triangulation where C is triangulated in reference to A and B. Since we assume knowledge of the locations of A and B, the distance between them can be calculated by the following formula: $\overline{AB} = \sqrt{(x_b - x_a)^2 + (y_b - y_a)^2}$, where the coordinates of A and B are (x_a, y_a) and (x_b, y_b), respectively. After measuring the angles α and β, and calculating the distance from A to B, and since $\frac{\sin\alpha}{\overline{BC}} = \frac{\sin\beta}{\overline{AC}} = \frac{\sin\delta}{\overline{AB}}$, $\overline{AC} = \frac{\overline{AB}.\sin\beta}{\sin\delta}$. Since $\alpha + \beta + \delta = 180$ ($\delta = 180 - \alpha - \beta$) and $\sin\delta = \sin(180 - \delta)$, then $\sin\delta = \sin(\alpha + \beta)$. Therefore, $\overline{AC} = \frac{\overline{AB}.\sin\beta}{\sin(\alpha+\beta)}$, and $\overline{XC} = \overline{AC}.\sin\alpha$, which forms the right triangule $\widehat{AXC}$. Using Pythagorean theorem, $\overline{AX} = \sqrt{(\overline{AC})^2 - (\overline{XC})^2}$.

[2] In a hyperbola there are two foci points, F_1 and F_2. These points have the property that given any point P_i on either of the hyperbola's curves, the difference between the distance from P_i to F_1 and P_i to F_2 is constant.

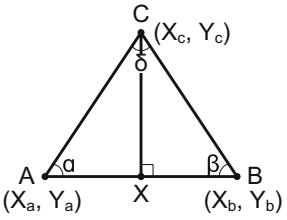

Fig. 1. Triangulation

Finally, the coordinates of C are determined in reference to the coordinates of A, where $x_c = x_a + \overline{AX}$ and $y_c = y_a + \overline{XC}$.

Trilateration. The simplest way to trilaterate a target is by solving the system of quadratic equations consisting of the circle equations of three intersecting circles representing the reference objects. These circles are formed by measuring the distances before the reference objects and the target, then these distances constitute the radii of the circles (each reference object forms one circle). Solving such system yields the intersection point of the circles and this is where the target is located [16]. However, in most cases, the three circles will not be ideally aligned to intersect in exactly one point. Instead, they will probably intersect in three pionts forming a *circular triangle* (also called curvilinear triangle) as shown in figure 2, where the target is probably located at its center. Fewell [17] presented an algorithm to calculate the common overlap area when three circles intersect; however, we are only interested in finding the three intersection points, not the actual area bounded by them. Hence, we use Fewell's algorithm up to the stage when the intersection points are calculated, then we treat them as vertices of a regular triangle and find its centroid where the target probably is. Figure 2 illustrates how trilateration is calculated, where: r_a is the radius of circle a, d_{ab} is the distance between the centers of circles a and b, and (x_{ab}, y_{ab}) is the intersection point[3] of circles a and b.

Based on [17], the three intersection points are calculated as follows: We first calculate the sines and cosines of angles θ' and θ" as shown in figure 2.

$cos\theta' = ({d_{12}}^2 + {d_{13}}^2 - {d_{23}}^2)/(2d_{12}d_{13}), \qquad sin\theta' = \sqrt{1 - cos^2\theta'}$

$cos\theta'' = -({d_{12}}^2 + {d_{23}}^2 - {d_{13}}^2)/(2d_{12}d_{23}), \qquad sin\theta'' = \sqrt{1 - cos^2\theta''}$

Next, we calculate the three intersection points (x_{12}, y_{12}), (x_{13}, y_{13}), and (x_{23}, y_{23}):

$\underline{(x_{12}, y_{12})}$: $x_{12} = \frac{{r_1}^2 - {r_2}^2 + {d_{12}}^2}{2d_{12}}, y_{12} = \frac{1}{2d_{12}}\sqrt{2{d_{12}}^2({r_1}^2 + {r_2}^2) - ({r_1}^2 - {r_2}^2)^2 - {d_{12}}^4}$

$\underline{(x_{13}, y_{13})}$: $x_{13} = x_{13}'cos\theta' - y_{13}'sin\theta', \quad y_{13} = x_{13}'sin\theta' + y_{13}'cos\theta'$

where: $x_{13}' = \frac{{r_1}^2 - {r_3}^2 + {d_{13}}^2}{2d_{13}}, \quad y_{13}' = \frac{-1}{2d_{13}}\sqrt{2d_{13}^2({r_1}^2 + {r_3}^2) - ({r_1}^2 - {r_3}^2)^2 - {d_{13}}^4}$

$\underline{(x_{23}, y_{23})}$: $x_{23} = x_{23}''cos\theta'' - y_{23}''sin\theta'' + d_{12}, \quad y_{23} = x_{23}''sin\theta'' + y_{23}''cos\theta''$

where: $x_{23}'' = \frac{{r_2}^2 - {r_3}^2 + {d_{23}}^2}{2d_{23}}, y_{23}'' = \frac{1}{2d_{23}}\sqrt{2{d_{23}}^2({r_2}^2 + {r_3}^2) - ({r_2}^2 - {r_3}^2)^2 - {d_{23}}^4}$

[3] Two circles intersect in two points, but we are only interested in the point contributing a vertex to the circular triangle formed by the intersection with a third circle.

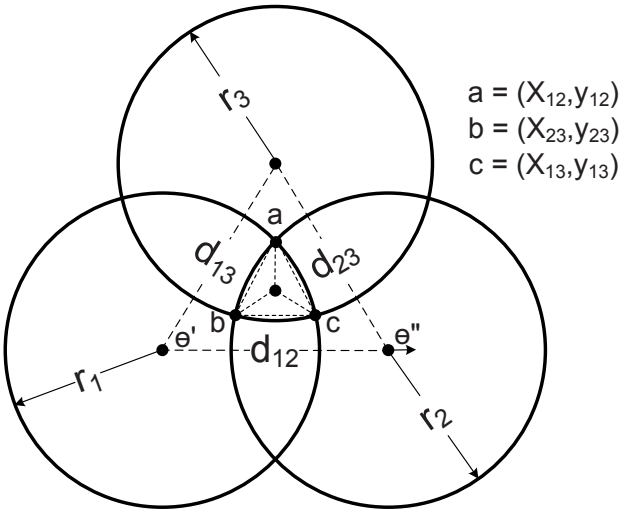

Fig. 2. Trilateration

Once the three vertices of the circular triangle is calculated, we treat it as a normal triangle and calculate its certroid which will be our estimated location of the target:

$$C = \left(\frac{x_{12} + x_{13} + x_{23}}{3}, \frac{y_{12} + y_{13} + y_{23}}{3} \right)$$

Multi-lateration and Multi-angulation. Multi-lateration [18] is similar to trilateration but is based on TDOA measurements rather than TOA or RSS. Generally, in multi-lateration, three reference objects measure the TDOA when receiving a signal from a target object which forms two hyperboloids intersecting at the target's location—TDOA from a fourth object forming a third hyperboloid is measured if localizing the target object in 3D is required.

Similarly, Multi-angulation [19] is closely related to triangulation where a target object is localized based on known angles. However, while triangulation is localizing a target object in reference of two objects, multi-angulation is a generalization approach with more reference objects. Increasing the number of reference objects is especially beneficial to enhance the accuracy of the localization process in noisy environments.

4 Localization in Cellular Networks

In 1996 the Federal Communication Commission (FCC) issued the E911 mandate aiming to further improve the 911 emergency calls when being made from mobile handsets. The mandate requires telecom operators to be able to accurately locate a mobile handset initiating a 911 call with accuracy of around 50

meters 67% of the time and within 150 meters 95% of the time for handset-based solutions, and within 100 meters 67% of the time and within 300 meters 95% of the time for network-based solutions [20]. Below we discuss a few popular localization techniques in cellular networks—Cell ID and Enhanced Cell ID are not discussed due to their severe accuracy discrepancies; see [21].

Enhanced Observed Time Difference. E-OTD [22] is based on Observed Time Difference (OTD) measurements; OTD estimates the difference in time to receive signals from two transmitting Base Stations (BS') at a single Mobile Station (MS). In E-OTD, the MS estimates its own location by calculating OTD when receiving signals from pairs of BS'. E-OTD requires at least three reference BS' (P_1, P_2, P_3) to make at least two OTD measurements (e.g. OTD_1 from P_1 and P_2, OTD_2 from P_1 and P_3, or P_2 and P_3). While E-OTD is often used in GSM networks, OTDOA (Observed Time Difference of Arrival) is generally considered the UMTS version of E-OTD developed especially to operate on UMTS networks. E-OTD was strongly believed to be the next generation location service. However, beside requiring the handsets to be slightly modified to enable E-OTD (introducing cost implications), it also failed to meet FCC E-911 location performance requirements; E-OTD/OTDOA were recently largely replaced by U-TDOA.

Uplink Time Difference of Arrival. U-TDOA [23], standardized by 3GPP (3rd Generation Partnership Project), is a localization technology to estimate the location of a MS by measuring how long it tooks signals emitted from MS to be received at several BS'. Unlike E-TOA, U-TDOA is a network-based scheme; that is, the localization process is carried out by the reference BS' which doesn't impose extra hardware or software requirements on the MS'. Moreover, U-TDOA uses multi-lateartion (see section 3.2)

Global Positioning System. GPS [24] is a location system developed by the US Department of Defense (DoD). GPS is similar to E-OTD in that it is handset-based (the target localizes itself in reference of surrounding reference objects), but its references are satellite rather than BS'. To be able to use GPS, an object has to use a special GPS receiver to correctly receive and decode signals from at least 4 out of the 24 satellites orbiting around the earth and constantly emitting these GPS signals. A GPS-enabled device calculates its its position by means of trilateration in reference to the satellites it receives GPS signals from. GPS localization and tracking proved to be useful for certain situations, but beside requiring additional hardware, it is also not suitable for indoor or underground environments where GPS signals are usually not available.

Assisted Global Positioning System. With conventional GPS system, the GPS device localizes itself independently, from receiving the GPS signals to the location estimation calculations. An A-GPS [25] system, on the other hand, consists of three components: (i) an A-GPS devices that can receive GPS signals but can not decode them, (ii) an A-GPS server equipped with a fully featured GPS receiver, and (iii) a network infrastructure which mediates between the A-GPS devices and the A-GPS server. In nutshell, the A-GPS devices localizes

itself by sending the GPS signals it receives to the A-GPS server, which in turn, estimates the location of the devices (based on the GPS signals provided) and returns it back to the device.

Differential Global Positioning System. The aim of D-GPS is to improve the accuracy of GPS localization by correcting the timing errors introduced with signals received from the satellites [26]. Usually, two receivers located within approximately the same vicinity receive the same timing errors. Hence, static reference stations with a pre-configured locations are distributed carefully to cover a large area. Once these static stations receive GPS signals, they compare the signals with their pre-configured locations to find the timing errors. Information about these errors is then propagated to the mobile stations in its vicinity so they can correct their received GPS signals accordingly.

5 Localization Fusion

Multi-sensor data fusion entails combining data from different sources and relates them to improve the accuracy [27]. In Localization algorithms, fusing more than one localization technique/measure proved efficient in terms of accuracy—for a general overview about data fusion in wireless localization, see [28]. Fusion, however, may introduce additional overhead and so increase energy consumption. Below we discuss a few examples of localization fusion algorithms in wireless networks.

5.1 Fusing Different Technologies

In [29] and [30], Aparicio *et al.* proposed an algorithm to fuse Bluetooth and WLAN measurements to locate a target in an indoor environment where Bluetooth stations and Access Points (AP's) are randomly distributed over the localization area. This technique incorporates building two maps, one based on RSS measurements from the Bluetooth stations and another based on RSS measurements from the WiFi AP's. The main idea is to specify the boundaries of the localization area by Bluetooth—which is a short range technology and would produce more accurate estimates for this purpose—and then only accept the WiFi RSS measurements reporting the target to be within this area.

5.2 Fusing Different Parameters

The most common technique in localization fusion is to fuse the measurements of different parameters, like RSS and TOA. In the following subsections we briefly introduce such fusion algorithms—algorithms proposed to fuse multiple measurements of the same parameter at different intervals (e.g. TDOA [31]) are not discussed.

Fusing Signal Strength with Time Measurements. Catovic *et al.* [32] proposed an algorithm to fuse TOA/TDOA measurements with RSS in short-range

partially synchronized Wireless Sensor Networks (WSN). The algorithm benefits from the improved time-based and RSS measurements due to the short-range nature of WSN. The proposed algorithm also accounts for WSN's heterogeneous characteristics which influences some general communication properties like communication range and routing schemes. In [33], the same authors presented an evaluation of the *Cramer-Rao Bound* (CRB) [4] for their proposed algorithms. This CRB computation was found to have been derived incorrectly and corrected by Huang *et al.* [34]. The main drawback of this scheme is the partial synchronization requirement that is not always available in WSN's. Luo *et al.* [35] proposed an algorithm based on Covariance Intersection (CI)[5] which fuses RSS and TDOA measurements. This algorithm is based on the so-called self-localization, where an object localizes itself in reference to its neighboring objects. In other work, McGuire *et al.* [36] presented a nonparametric estimation method[6] to fuse RSS and TDOA.

Fusing Direction with Time Measurements. In [37], Venkatraman *et al.* proposed two algorithms based on TOA and AOA fusion. The first algorithm, called *Hybrid TOA/AOA Algorithm* is based on trilateration where a target object is located at the common overlap area of at least three intersecting circles formed by TOA measurements from at least three reference objects. In this algorithm, AOA measurements are taken to further constrain this area and enhance the accuracy of the localization. The second Algorithm, called *Hybrid Lines of Position Algorithm*, is based on solving Lines of Position (LOP)[7] by the least square algorithm. LOP are generated by an astronomical method called *Intercept Method* that is usually used to locate an object on earth. The authors proposed enhancing this algorithm by generating LOP based on TOA and others based on AOA. Similarly, Cong *et al.* [38] proposed a two-step least square algorithm to fuse TDOA and AOA measurements in wideband CMDA cellular network. Additionally, Hsin-Yuan *et al.* [39] and Ping *et al.* [40] proposed schemes to fuse angular (AOA) and time (TOA/TDOA) measurements with neural networks.

6 Tracking in Sensor and Cellular Networks

Since, usually, there are limited resources available for sensor nodes, it is important that they maintain an efficient power-saving scheme. Consequently, most of the tracking algorithms proposed for sensor networks account for power efficiency. One approach is to minimize the number of the active tracking sensors to only those located closer to the target. This can be done by accurately localizing the target node. Kim *et al.* [41] proposed an algorithm that tracks a target

[4] CRB is the lower bound of the mean-square error of an estimate of a deterministic parameter. CRB determines the accuracy of the estimator.

[5] CI fuses two or more variables with unknown correlation.

[6] Non-parametric methods are statistical methods applied on variables with unknown probability distribution.

[7] A single LOP is a line in which a target object is situated. The intersection of multiple LOP yeilds the location of that target.

through a set of steps. Once the surrounding objects detects the presence of the target, they collaboratively localize it and predict its next movement based on its velocity, assuming that the target doesn't perform sudden or rapid movements. The nodes then notify other nodes located toward the area that the target is expected to move to.

When tracking multiple targets, the energy requirement issue becomes even more significant. Jiang *et al.* [42] proposed an algorithm to maintain efficient energy consumption in a multi-target tracking scenario. The algorithm divides the tracking area into tracking subareas where nodes are switched between sleep and awake states based on a scheduling scheme.

In law enforcement and forensic applications, it is sometimes necessary to hide the tracking process while tracking a suspect by enforcing passive localization and tracking approach [16]. Implementing such applications is slightly more challenging in sensor (ad hoc) networks than in cellular networks because where in the latter we have knowledge of some parameters like BS locations and can reconstruct the scene, we don't for the former.

Tracking a mobile handset in cellular networks (this include GSM and CDMA) has been an active area of research. However, because such tracking is based on long-range communication, the accuracy of algorithms developed for this purpose is severely hindered. Beside the conventional localization methods employed in sensor networks (RSS, TOA etc.), filtering is usually used to further enhance the estimation process accuracy. In [43], Mihaylova *et al.* presented two sequential Monte Carol techniques, namely, particle filter and Rao-Blackwellised particle filter, which are based on RSSI measurements of signals emitted by the MS. Zaidi *et al.* [44] proposed similar algorithms based on variants of Kalman filter using RSSI measurements. The techniques based on these filters are very technical and a detailed discussion of them is beyond the scope of this paper.

7 Accuracy and Trustworthiness Issues

Maintaining a consistent estimation accuracy is the main problem in most localization or tracking processes. The ideal situation of having a clear line of sight between the transmitter and the receiver is highly unrealistic especially in urban environments. In fact, localizing or tracking an object is based on a set of nonlinear parameters, such as RSS, which are affected by environmental and physical factors. As we discussed earlier, the localization or tracking algorithms are as accurate as the parameters they are based on. Radio waves are usually described by their behavior while propagating from a point to another. Modeling these radio propagation behaviors largely influences the accuracy of any localization/tracking process. Based on the environment, radio propagation models are classified as Foliage Models (propagation through foliage), Terrain Models (effect of terrain characteristics on radio propagation) and City or built-up Models. City Models were derived from empirical data collected at urban environments to investigate the characteristics of radio propagation in such environments. Young Model, Okumura Model, Hata Model and Lee Model are examples of popular city

radio propagation models [45]. These models, however, are mostly relevant for long-range propagation and hence for localization/tracking in cellular networks; for a discussion about radio propagation models in short-range environments, see [46].

Tracking requires a step further beyond radio propagation to model movement of the target(s). Such models are called mobility models and can range from probabilistic to deterministic; see [47] for an overview of mobility models in Ad Hoc networks, and [48] for mobility in cellular networks.

There is an important distinction between accuracy of an estimate and how trustworthy it is. Such distinction is especially significant in forensics and law enforcement applications where the integrity of evidence is essential. It is important to have knowledge of whether and how potential malicious adversaries can masquerade the measurements and thus the forensic evidence. In the following subsections we discuss a few possible ways a tracking process can be attacked. Such situations and scenarios make it extremely important to maintain both good error/accuracy estimate as well as high level of trustworthiness on these estimates; this can be achieved by studying both the tracking environment and the ways in which tracking can be mislead. For the best of our knowledge, this area of research has been less investigated.

Address Spoofing. If the address of the tracker (or one of the genuine trackers) was spoofed, the integrity of the whole tracking process fails. In such scenario, an attacker impersonates one of the trackers and take over the tracking process, during this time, the attacker can easily modify the tracking information. This attack, however, can be prevented by enforcing mutual authentication whereby both the agents and the trackers prove to each other that they are in fact who they claim they are.

Denial of Service (DoS). Anther way to attack a tracking process is to temporarily disable it by temporarily rendering its resources unavailable. Such attacks involves repetidely sending traffic to trackers to overwhelm them which may result in losing track of the target. This attack may be prevented by configuring the trackers to accept traffic from only specific entities.

Man-In-the-Middle (MITM). An attacker can mediate between two or more trackers pretending to be one for the other. An attacker in this case can either be passive, where it only relays traffic, or active, where it alters traffic as it passes through it. This type of attack can be prevented by encryption. Usually, the traffic is location-updates and is small enough to allow for encryption without necessarily overwhelming the tracking process.

8 Conclusion

In this paper, we surveyed various localization and tracking approaches in wireless networks. Applications of Localization/tracking can either be passive or active. In passive applications, like crime prevention, the target (suspect) is unaware of the the localization/tracking process. On the other hand, in active

applications, like E911 emergency call, the localization/tracking process is handled cooperatively by both the target and other surrounding tracking objects. We first introduced some localization techniques that are usually used in sensor networks and are the basis for more complex ones used in cellular networks. We also provided a discussion about multi-sensor data fusion where various localization parameters are fused to improved accuracy. Most of the tracking algorithms proposed for sensor networks are based on energy-efficient schemes because (usually) sensors are energy-constrained entities. Furthermore, Tracking in cellular networks are usually based on complex filters to enhance accuracy that is severely affected by the long-range nature of cellular networks. Finally, we discussed radio propagation and mobility modeling which have the greatest impact on the accuracy of localization/tracking algorithms; we further discussed the possible attacks a tracking/localization process can be vulnerable to and note that, in this area, there is less research on intrusion detection/prevention which may affect how trustworthiness these algorithms are.

References

1. Hightower, J., Borriello, G.: Location Sensing Techniques. UW CSE 01-07-01, University of Washington, Department of Computer Science and Engineering, Seattle, WA (2001)
2. Hightower, J., Borriello, G.: Location Systems for Ubiquitous Computing. Computer 34(8), 57–66 (2001)
3. Hightower, J., Borriello, G.: A Survey and Taxonomy of Location Systems for Ubiquitous Computing. Technical report, IEEE Computer (2001)
4. Pandey, S., Agrawal, P.: A Survey on Localization Techniques for Wireless Networks. Journal of the Chinese Institute of Engineers 29(7), 1125–1148 (2006)
5. Sinan, G.: A Survey on Wireless Position Estimation. Wirel. Pers. Commun. 44(3), 263–282 (2008)
6. Srinivasan, A., Wu, J.: A Survey on Secure Localization in Wireless Sensor Networks. In: Furht, B. (ed.) Encyclopedia of Wireless and Mobile communications (2008)
7. Roos, T., Myllymäki, P., Tirri, H.: A Statistical Modeling Approach to Location Estimation. IEEE Transactions on Mobile computing 1(1), 59–69 (2002)
8. Caffery, J., Stüber, G.L.: Subscriber Location in CDMA Cellular Networks. IEEE Transactions on Vehicular Technology 47(2), 406–417 (1998)
9. Chan, Y., Tsui, W., So, H.: Time-of-Arrival Based Localization Under NLOS Conditions. IEEE Transactions on Vehicular Technology 55(1), 17–24 (2006)
10. Mailaender, L.: On the Geolocation Bounds for Round-Trip Time-of-Arrival and All Non-Line-of-Sight Channels. EURASIP Journal on Advances in Signal Processing 2008(584670), 10 (2008)
11. Gustafsson, F., Gunnarsson, F.: Positioning Using Time-Difference of Arrival Measurements. In: Conference on Acoustics, Speech, and Signal Processing (ICASSP 2003), vol. 6, pp. 553–556 (2003)
12. Mizusawa, G.: Performance of Hyperbolic Position Location Techniques for Code Division Multiple Access. Master's thesis, Virginia Polytechnic Institute and State University, Blacksburg, Virginia (1996)

13. Rong, P., Sichitiu, L.: Angle of Arrival Localization for Wireless Sensor Networks. In: SECON 2006: 3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks, vol. 1, pp. 374–382 (2006)
14. Patwari, N., Ash, J.N., Kyperountas, S., Hero, A.O., Moses, R.L., Correal, N.S.: Locating the Nodes: Cooperative Localization in Wireless Sensor Networks. IEEE Signal Processing Magazine 22(4), 54–69 (2005)
15. Hjelle, O., Daehlen, M.: Triangulations and Applications. Springer, Heidelberg (2006)
16. Al-Kuwari, S., Wolthusen, S.D.: Passive Ad-Hoc Localization and Tracking in Short-Range Communication (manuscript submitted for publication) (2009)
17. Fewell, M.: Area of Common Overlap of Three Circles. Unclassified DSTON-TN-0722, Maritime Operations Division, Defence Science and Technology Organisation, Edinburgh South Australia 5111, Australia (2006)
18. Shang, Y., Shi, H., Ahmed, A.: Performance Study of Localization Methods for Ad Hoc Sensor Networks. In: IEEE Conference on Mobile Ad Hoc and Sensor Systems, pp. 184–193 (2004)
19. Ash, J., Potter, L.: Robust System Multiangulation Using Subspace Methods. In: IPSN 2007: Proceedings of the 6th international conference on Information processing in sensor networks, pp. 61–68. ACM, New York (2007)
20. Federal Communications Commission (FCC): OET Bulletin no. 71: Guidelines for Testing and Verifying the Accuracy of E911 Location Systems (2000)
21. Borenovic, N., Simic, I., Neskovic, M., Petrovic, M.: Enhanced Cell-ID + TA GSM Positioning Technique. In: EUROCON 2005: The International Conference on Computer as a Tool, vol. 2, pp. 1176–1179 (2005)
22. Kos, T., Grgic, M., Kitarovic, J.: Location Technologies for Mobile Networks. In: 6th EURASIP Conference focused on Speech and Image Systems, Signals and Image Processing, pp. 319–322 (2007)
23. Nasser, N.: Automatic Location Systems for Mobile Phones. Arab Research Institute in Sciences & Engineering (ARISER) 2(2), 53–59 (2008)
24. Raza, A., Hameed, S., Macintyre, T.: Global Positioning System - Working and its Applications. In: Innovations and Advanced Techniques in Systems, Computing Sciences and Software Engineering, Netherlands, pp. 448–453. Springer, Heidelberg (2008)
25. Djuknic, G., Richton, R.: Geolocation and Assisted GPS. Computer 34(2), 123–125 (2001)
26. Morgan-Owen, J., Johnston, T.: Differential GPS Positioing. Electronics & Communication Engineering Journal 7, 11–21 (1995)
27. Hall, D., Llinas, J.: An Introduction to Multisensor Data Fusion. Proceedings of the IEEE 85, 6–23 (1997)
28. Kleine-Ostmann, T., Bell, A.: A Data Fusion Architecture for Enhanced Position Estimation in Wireless Networks. IEEE Communications Letters 5(8), 343–345 (2001)
29. Aparicio, S., Perez, J., Bernardos, A., Casar, J.: A Fusion Method Based on Bluetooth and WLAN Technologies for indoor location. In: Proceedings of IEEE Conference on Multisensor Fusion and Integration for Intelligent Systems, pp. 487–491 (2008)
30. Aparicio, S., Tarrio, P., Perez, J., Bernardos, A., Casar, J.: An Indoor Location Method Based on a Fusion Map Using Bluetooth and WLAN Technologies. In: International Symposium on Distributed Computing and Artificial Intelligence 2008 (DCAI 2008), vol. 50, pp. 702–710 (2009)
31. Zhang, C., Liu, J., Liu, S., Li, W.: Research on Improving TDOA Location Accuracy Based on Data Fusion. In: Proceedings of the IEEE 6th Emerging Technologies: Frontiers of Mobile and Wireless Communication, vol. 2, pp. 761–764 (2004)

32. Catovic, A., Sahinoglu, Z.: Hybrid TOA/RSS and TDOA/RSS Location Estimation Schemes for Short-Range Wireless Networks. Bechtel Telecommunication Technical Journal (BTTJ) 2(2), 77–84 (2004)
33. Catovic, A., Sahinoglu, Z.: The Cramer-Rao Bounds of Hybrid TOA/RSS and TDOA/RSS Location Estimation Schemes. IEEE Communications Letters 8(10), 626–628 (2004)
34. Huang, J., Wan, Q.: Comments on The Cramer-Rao Bounds of Hybrid TOA/RSS and TDOA/RSS Location Estimation Schemes. IEEE Communications Letters 11(11), 848–849 (2007)
35. Lue, R., Chen, O., Tu, L.: Node Localization through Data Fusion in Sensor Network. In: AINA 2005: Proceedings of the 19th International Conference in Advanced Information Networking and Applications, pp. 337–342 (2005)
36. McGuire, M., Plataniotis, K., Venetsanopoulos, A.: Data Fusion of Powr and Time Measurements for Mobile Terminal Location. IEEE Transactions on Mobile Computing 4(2), 142–154 (2005)
37. Venkatraman, S., Caffery, J.: Hybrid TOA/AOA Techniques for Mobile Location in Mon-Line-Of-Sight Environments. IEEE Wireless Communication and Networking Conference 1, 274–278 (2004)
38. Cong, L., Zhuang, W.: Hybrid TDOA/AOA Mobile User Location for Wideband CDMA Cellular Systems. IEEE Transactions on Wireless Communications 1(3), 439–447 (2002)
39. Hsin-Yuan, C., Tung-Yi, C.: Hybrid TDOA/AOA Mobile User Location with Artificial Neural Networks. In: IEEE International Conference on Networking, Sensing and Control, pp. 847–852 (2008)
40. Ping, Z., Ling-yan, L., Hao-shan, S.: A Hybrid Location Algorithm Based on BP Neural Networks for Mobile Position Estimation. IJCSNS International Journal of Computer Science and Network Security 6(7A), 162–167 (2006)
41. Kim, H., Kim, E., Han, K.: An Energy Efficient Tracking Method in Wireless Sensor Networks. In: Koucheryavy, Y., Harju, J., Iversen, V.B. (eds.) NEW2AN 2006. LNCS, vol. 4003, pp. 278–286. Springer, Heidelberg (2006)
42. Jiang, B., Ravindran, B., Cho, H.: Energy Efficient Sleep Scheduling in Sensor Networks for Multiple Target Tracking. In: Nikoletseas, S.E., Chlebus, B.S., Johnson, D.B., Krishnamachari, B. (eds.) DCOSS 2008. LNCS, vol. 5067, pp. 498–509. Springer, Heidelberg (2008)
43. Mihaylova, L., Angelova, D., Honary, S., Bull, D., Canagarajah, C., Ristic, B.: Mobility Tracking in Ceullar Network Using Particle Filtering. IEEE Transactions on Wireless Communciations 6(10), 3589–3599 (2007)
44. Zaidi, Z., Mark, B.: Real-Time Mobility Tracking Algorithms for Cellular Networks Based on Kalman Filtering. IEEE Transactions on Mobile Computing 4, 195–208 (2005)
45. Seybold, J.S.: Introduction to RF Propagation. Wiley Interscience, Hoboken (2005)
46. Domazetovic, A., Greenstein, J., Mandayam, B., Seskar, I.: Propagation Models for Short-Range Wireless Channels with Predictable Path Geometries. IEEE Transactions on Communications 53(7), 1123–1126 (2005)
47. Camp, T., Boleng, J., Davies, V.: A Survey of Mobility Models for Ad Hoc Network Research. Wireless Communication and Mobile Computing (WCMC): Special issue on Mobile Ad Hock Networking 2(5), 483–502 (2002)
48. Kim, K., Choi, H.: A Mobility Model and Performance Analysis in Wireless Cellular Network with General Distribution and Multi-Cell Model. Wireless Personal Communication (2009)