Analysis of Location Spoofing Identification in Cellular Networks

Yuxin Wei[1] and Dawei Liu[2](✉)

[1] Air Force Engineering University, Xi'an, China
weij0831@126.com
[2] Xi'An JiaoTong-Liverpool University, Suzhou, China
dawei.liu@xjtlu.edu.cn

Abstract. Location spoofing is considered as a serious threat to positioning and location based services in wireless networks. Existing identification methods for location spoofing have focused primarily on wireless sensor networks. These methods may not be applicable in cellular networks due to the following two limitations: (i) relying on accurate distance measurement; (ii) incapable of dealing with bad propagation conditions. To address these two issues, we carry out an analysis of location spoofing based on angle-of-arrival (AOA) and time-difference-of-arrival (TDOA) measurement models, two commonly used signal measurement models in cellular networks, in bad propagation conditions with large measurement errors. Our analysis shows that AOA model is more robust to location spoofing in noisy conditions.

1 Introduction

Location spoofing has attracted much attention during the past ten years because of the development of wireless networking technologies. It refers to an attack carried out by malicious network users for the purpose of misleading a positioning systems. To address this problem, many location identification methods have been developed for wireless sensor networks. The basic idea is to verify the location of a target user with respective to its location. Sastry *et al.* [1] proposed an ECHO protocol for verifying the location claim of a network node based on a challenge-response mechanism. In [2,3], a network node must verify its respective distances to at least three detecting points in order to securely estimate its position. Signals forged in this way will always lead to a consistent localization. Wang [4] pointed out there existed a perfect location spoofing that traditional location spoofing identification methods were unable to deal with. A possible solution is to make use of multiple sensor nodes that can identify with each other [5]. Zhang [6] introduced a mobility-assisted secure positioning scheme and extended the application to Ultra-Wideband (UWB) sensor networks. These identification methods are primarily designed for wireless sensor network (WSN) applications. When applied to cellular networks, these methods would not work properly because of the following two limitations:

S. Boumerdassi et al. (Eds.): MSPN 2015, LNCS 9395, pp. 18–27, 2015.
DOI: 10.1007/978-3-319-25744-0_2

- *Relying on accurate distance measurement.* Existing methods commonly make use of a distance-based identification which requires accurate distance measurement between pairs of sensor nodes. Measuring the distance accurately could be difficult in cellular networks; therefore, identification would become inaccurate.
- *Incapable of dealing with large measurement error.* WSN usually covers a small area. The environmental noises and the signal measurement errors caused could be stable. In contrast, a cellular network can be deployed in a wide and complex area. The signal measurement errors caused by environmental noises could vary significantly over time and place. It is not clear whether existing identification methods can be applied in the error-prone conditions.

In this paper, we address the above mentioned two problems. We first carry out an analysis of location spoofing based the angle-of-arrival (AOA) and time-difference-of-arrival (TDOA) based measurement models which are commonly used in cellular networks. Then we propose a cooperative method to identify location spoofing in bad channel conditions. Our security analysis shows that the AOA model could offer better security and lower hardware requirement when facing location spoofing. The remainder of the paper is organized as follows. Section 2 discusses wireless positioning in AOA and TDOA models. Section 3 presents the cooperative secure positioning method. Section 4 analyzes the security of the two models. Section 5 concludes this paper and gives some directions for further research.

2 AOA and TDOA Models

In this section we present an analysis of location spoofing in AOA and TDOA based models. We propose two methods to identify location spoofing in these two models separately.

A general cellular network is considered. It consists of a mobile station (MS) at X and a group of base stations $(BS_1, \dots, BS_n)$ at $(X_1, X_2, \dots, X_n)$. In this section, we assume the magnitude of environmental noise is small. The influence of a large environmental noises will be discussed in the next section.

2.1 AOA Model

AOA measurement model has been widely applied in existing cellular networks [7]. BS equipped with antenna array allows the measurement of arriving angle of radio signals. Let θ_i be the arriving angle of a radio signal sent from the MS and measured by BS_i. The location $X(x, y)$ of the MS can be estimated via the following equation:

$$\theta_i = atan(\frac{y_i - y}{x_i - x}) \qquad (1)$$

in which $X_i(x_i, y_i)$ is the location coordinates of BS_i which can be obtained beforehand. Clearly, Eq. (1) represents a line connecting the MS and BS_i. We refer to

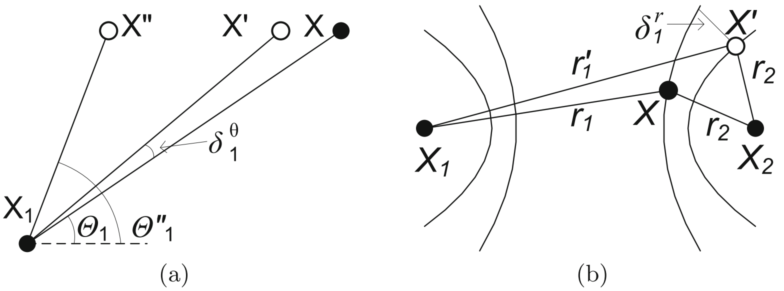

Fig. 1. Inconsistency caused by environmental noises and malicious MS. (a) In AOA model, angle measurement is biased to θ_1' and θ_1'' due to environmental noises and malicious attack respectively. (b) In TDOA model, hyperbola estimation is biased due to distance measurement error in r_1 (biased from r_1 to r_1') caused by environmental noises and/or malicious attack.

this line as a positioning line. If the radio signal sent from the MS can be measured by two or more BSs, X should be a variable satisfying Eq. (1) for all the BSs, or geometrically, be the crossing point of all the positioning lines.

By manipulating its radio signal, a malicious MS can mislead the angle measurement at BS_1 from θ_1 to a significantly biased value θ_1''. Figure 1(a) shows an example. A location estimation that makes use of BS_1 as well as other two beacons in which the angles are measured accurately would very likely to be inconsistent such that there does not exist an X satisfying Eq. (1) with all three BSs. This can be understood geometrically in terms of multiple positioning lines crossing in a region instead of a point. The degree of inconsistency could be closely related to the range of error caused by location spoofing. Liu et al. [8] proposed to measure the degree of inconsistency with the mean square error and use it to identify a location spoofing.

The presence of a malicious MS may not necessarily lead to an inconsistent location estimation [4]. A smart MS could manipulate its radio signal carefully so that all the positioning lines would cross at a point $X'' \neq X$. This means t he location estimation would be consistent; and the MS would not be identified as malicious. This type of location spoofing could be more deceptive compared with the one mentioned above. To deal with this problem, Capkun [9] proposed an identification method that made use of a hidden BS with the location unknown to any MS. According to Eq. (1), it is impossible to determine the positioning line if the BS location $X_i(x_i, y_i)$ is unknown. A malicious MS would be unable to estimate the location of the positioning lines and therefore unable to keep the consistency in location estimation. In the following discussion, we will assume the existence of at least one hidden BS. Therefore, any location spoofing would be associated with inconsistent location estimation. It is worth to mention that, literature [9], as an important contribution to location spoofing in cellular network, has not managed to address the two problems we mentioned in Sect. 1.

Environmental noises can be another cause of inconsistent location estimation. Cellular networks deployed in urban regions may have inaccurate angle measurements at every BS. Similar to the errors caused by a malicious MS, the measurement error caused by the environmental noises could lead to inconsistent location estimation. However, the range of the error is typically small when caused by the environmental noises, such as δ_1^θ shown in Fig. 1(a). This can be explained as follows: if a malicious MS wants to cause a large error in the positioning, it would have to bring a bias larger than the ones caused by environmental noises; otherwise, it would not have any significant impact on positioning result. In order words, there is not need to identify a malicious MS if its influence is in the same level of environmental noise

Based on the above analysis, we propose a location spoofing identification method as follows: (i) estimating X with Eq. (1); (ii) computing the mean square angle error (MSAE) based on the positioning result X; (iii) checking if the MSAE is within the range of the measurement error caused by environmental noises which can be measured beforehand. The MSAE is defined below:

Definition 1. Given the positioning result $X(x, y)$, of an MS and the arriving angles $(\theta_1, \ldots, \theta_n)$ measured at $(BS_1, \ldots, BS_n)$, the square angle error (SAE) of BS$_i$ is defined as

$$\delta_i^\theta = (\theta_i - atan(\frac{y_i - y}{x_i - x}))^2 \tag{2}$$

and MSAE of all BSs is defined as $\varDelta^\theta = \sum_{i=1}^{n} \frac{\delta_i^\theta}{n}$

In the above method, the MSAE is used as a measure for the degree of inconsistency. The underlying principle is: if the angle measurement is largely biased, the positioning result X would always be accompanied with a large MSAE; since the environmental noises could never cause such a large MSAE, the MS would be identified as malicious. In contrast, if the bias is small, it would be possible to find an X associated with a small MSAE. As mentioned above, a small MSAE is likely to be caused by the environmental noises or a malicious MS that does not have any significant influence on the positioning result. A similar application of MSAE has been discussed in detail in TOA based location spoofing identification in wireless sensor networks [8].

2.2 TDOA Model

TDOA is another measurement model that has been widely applied for location estimation in cellular networks. In this model, the radio signal's propagation distance is measured between the MS and BS_i with $r_i = (t_i - t) \times c$, where t is the time at which the radio signal is sent out from the MS, t_i is the time the radio signal arriving at BS_i, and c is the transmission speed of the radio signal. r_i is referred to as a pseudorange. This is because the clocks at MS and BS_i may not be synchronized. Let ϵ_i be the error caused by the synchronization bias in r_i, the location $X(x, y)$ of the MS can be related to the location $X_i(x_i, y_i)$ of BS_i as following:

$$r_i = \sqrt{(x_i - x)^2 + (y_i - y)^2} + \epsilon_i \tag{3}$$

Unlike the MS, BSs are usually synchronized with each other, meaning ϵ_i would be the same for different i. By subtracting r_1 from r_i, we can obtain the following nonlinear equation

$$\begin{aligned} r_i - r_1 = &\sqrt{(x_i - x)^2 + (y_i - y)^2} \\ &-\sqrt{(x_1 - x)^2 + (y_1 - y)^2} \end{aligned} \tag{4}$$

which relates X to X_i and X_1. Geometrically, Eq. (4) represents a hyperbola consisting of all the possible locations of the MS. If the radio signal of the MS can be measured by 3 or more BSs at the same time, X would be the crossing point of the correspoding hyperbolas determined by pairs of BSs.

The problem of inconsistent location estimation could arise in TODA measurement model if a malicious MS is involved or environmental noises are considered. In the pseudorange measurement, a malicious MS may falsify the time t whereas environmental noises can affect the measurement of t_i, both of which can result in a distorted r_i in Eq. (4). An example is shown in Fig. 1(b). A location estimation carried out by multiple BSs involving such an r_i would very likely to be inconsistent, i.e., there does not exist an X satisfying all set of equations in the form of (4). As we have explained in Sect. 2.1, the degree of inconsistency caused by environmental noises could be assumed small, whereas a large inconsistency should be caused by a malicious MS.

Based on the above analysis, we propose to identify a malicious MS with a three-step method similar to the one proposed in Sect. 2.1. In particular, we modify the parameter in step (ii) from MSAE to the mean square distance error (MSDE), and use it as a measure of consistency in locationing. The MSDE is defined as below:

Definition 2. Given an MS with the TDOA measurements $(r_2 - r_1, r_3 - r_1, \ldots, r_n - r_1)$, the square distance error (SDE) of BS$_i$ is

$$\delta_i^r = (r_i - r_1 - (l_i - l_1))^2 \tag{5}$$

where $l_i = \sqrt{(x_i - x)^2 + (y_i - y)^2}$, and the MSDE of all BSs can be obtained by $\Delta^r = \sum_{i=2}^{n} \frac{\delta_i^r}{n}$

For a benign MS, the ranges of SDE Δ_i^r and MSDE Δ^r would be small which can be measured in advance. If a malicious MS forges the time t or causes a largely biased distance measurement, Δ^r would increase significantly. Generally, the problem of secure location in both the AOA and the TDOA models can be summarized as follows: Determine whether the measured Δ (Δ^θ for the AOA model and S^r for the TDOA model) is below the threshold Δ_0 (Δ_0^θ or Δ_0^r) measured beforehand.

3 Cooperative Secure Positioning

In this section, we present a cooperative method to support secure positioning in non-line-of-sight (NLOS) propagation conditions. NLOS is known as the primary

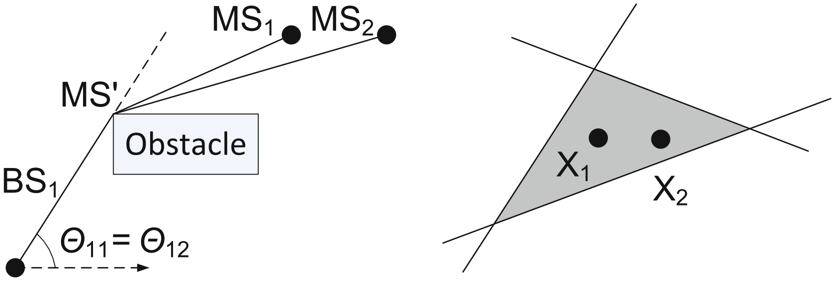

Fig. 2. AOA positioning of two MSs nearby under NLSO propagation conditions. (a) Inaccurate angle measurement; (b) Inconsistent positioning

cause of large positioning errors [10]. It is caused by obstacles blocking the direct propagation path of radio signal. Refer to Fig. 2(a) for an example and let MS_1 be benign. The radio signal's arriving angle measured at BS_1 is θ_{11}. This will lead to a biased position estimation in the form of Eq. (1). If there are two other BSs BS_2 and BS_3 that can measure the radio signal's arriving angle accurately. The positioning of MS_1 carried out by BS_1, BS_2, and BS_3 would be inconsistent as the corresponding positioning lines would cross in an area rather than a point, such the situation shown in Fig. 2(b). The same problem could happen to MS_2. Moreover, because of the obstacle, the radio signals sent from MS_1 and MS_2 could have the same arriving angle to BS_1 as if they were sent from an MS' located at a corner of the block.

In the case of a large obstacle located between MS_1 and BS_1, the degree of the inconsistency in the positioning of MS_1, measured with $\varDelta_1$, would become large. Consequently, the validity of the three-step secure positioning methods proposed in Sect. 2 would be questionable: if we set a small threshold $\varDelta_0$ as before, the benign MS_1 would be identified as malicious; if we adjust the threshold $\varDelta_0$ to a large value, a malicious MS could be identified as benign.

```
record $\varDelta(\varDelta_1, \ldots, \varDelta_m)$ for each MS
$for$ each $\varDelta_i$
    $if$ there is a $\varDelta_{j \neq i}$ satisfying $|\varDelta_i - \varDelta_j| < \varDelta_0$
        identify $MS_i$ as benign
    $else$
        identify $MS_i$ as malicious
```

To address this problem, let us consider again the MS_2 in Fig. 2(a). Since the inconsistency in the positioning of MS_2 and MS_1 is caused by the same obstacle, the degree of inconsistency, measured with $\varDelta_2$, could be similar to $\varDelta_1$, and the similarity can be measured based on the relative position of MS_1 and MS_2. Specifically, the arriving angle measured at BS_1 is the same for MS_1 and MS_2, and the difference between $\varDelta_1$ and $\varDelta_2$ is determined by the other two BSs, BS_2

and BS_3. In the above, we assumed accurate measurement at BS_2 and BS_3. This means the difference is determined by the relative position of MS_1 and MS_2. In particular, if the distance between MS_1 and MS_2 is within the range of the positioning error caused by channel noise in good channel conditions, the value of $|\mathit{\Delta}_1 - \mathit{\Delta}_2|$ would be smaller than the threshold $\mathit{\Delta}_0$ measured in good channel conditions. Based on this, we propose an identification method as above.

It is easy to see that, in the TDOA positioning model, the above-proposed method can be applied directly for the identification of location spoofing, and the analysis of the threshold will hold well. It is worth mentioning that we assumed in the above analysis that majority of the MSs are benign. This assumption would be valid for most cellular networks. For some WSNs, such as those deployed in hostile environments, this assumption may not be valid, consequently, the out method may not be able to work properly.

4 Security Analysis

4.1 AOA Model

In the AOA positioning model, the measurement of arriving angle θ does not need the coordination from the MS. As a result, an attacker will not be able to mislead the BS about θ by manipulating its radio signal. In contrast, an inaccurate measurement of θ can be caused by NLOS propagation. In this situation, the method proposed in Sect. 3 can be used for secure positioning.

In the presence of multiple attackers, one attacker, say A, can compromise the measurement of θ at one or several BSs by coordinating with another attacker in the follower manner: A does not communicate directly with the BSs around, instead, it sends and receives radio signal to another attack A' which acts as an agent for communication. In this situation, BSs may not be able to measure θ of A accurately. In order to mislead the positioning carried out by BS_1 and BS_2, A has to be cautious about its radio signal strength and its position regard to the BSs. Specifically, a too strong signal of A would be detected by the BSs and lead to the inconsistency between θ_1 and θ'_1. In order to avoid the inconsistency, A has to control its transmitting power carefully or use directional antennas. In practice, controlling the transmitting power without being detected is difficult since BSs do not release their positions in AOA positioning. Moreover, it A is inside the convex hull of the BSs [11], it would be impossible for A to carry out such an attack.

Another problem for the proposed the cooperative secure positioning comes with the presence of multiple attackers. Recall that we identify an attacker by testing its inconsistency $\mathit{\Delta}$ with other MSs. If an pair of MSs can be found with a similar $\mathit{\Delta}$, both of them could be identified as benign. This identification method may not be robust against multiple attackers. Consider Fig. 2 for an example, and let A and A' be two close attackers. By coordinating with each other, A and A' could cause inconsistencies similar to each other, consequently, both of them would be identified as benign. A solution is to modify the step 3 of the method proposed in Sect. 3 as follows: "if majority of $\mathit{\Delta}$ satisfying $|\mathit{\Delta}_i - \mathit{\Delta}| < \mathit{\Delta}_0$". As long as the majority of MSs are benign, which is a reasonable assumption for cellular networks, all the attackers can be identified even if they had the same Δ.

4.2 TDOA Model

Distance-based positioning requires coordination between each BS and MS. An attacker A may compromise BSs by manipulating its radio signal. For example, A may report a false local time t to a BS, resulting in an error in the measurement of r. Consequently, the positioning based on Eq. (3) would be inaccurate. However, this type of attack will not affect the TDOA positioning. Recall that the biases δ_1 and δ_i are removed by subtracting r_1 from r_i. After this, the Eq. (4) will not contain the variable t. As long as the same signal (with the same t) is observed by BS_i and BS_1, a manipulated t would not have any influence on TDOA positioning.

On the other hand, the attacker may affect the TDOA positioning by reporting to BS_i and BS_1, respectively, two different t, and the positioning using Eq. (4) would be inaccurate. Figure 1(b) illustrates an example, where r_2 is accurate and r_1' is altered because t sent to MS_2 is different from the one sent to MS_1. This attack can be carried out by one or multiple attackers. In order to convince all the BSs that they are observing the same signal, A needs to avoid different signals with different t being observed by the same BSs. Based the analysis in Sect. 4.1, this requires the position information all BSs.

In the TDOA model, positioning could be carried out in the uplink and downlink. In the uplink positioning, such information is not released, therefore, the positioning system would be secure against the attack. In the donwlink positioning, such information is released to every MS, consequently, an attacker outside the convex hull region of the BSs can compromise the positioning by manipulating its radio signal.

Remark. Based on the analysis above, the angle-based model outperforms the TDOA distance-based model in: (i) It require less BSs for a secure positioning. (ii) It does not suffer from some attacks. The detail comparison can be found in Table 1.

Table 1. Comparison of two positioning models.

	AOA model	TDOA model
Number of BSs	≥ 2	≥ 3
Physical measurement	Uplink	Uplink & downlink
Reveal BS coordinates	No	Yes*
Number of attacker	≥ 2	≥ 1
Coordination required	Yes	No
Attacker's position	Restricted	Anywhere

*BS coordinates are broadcast in downlink positioning

5 Conclusions

Existing location spoofing identification methods are mostly inadequate for cellular networks. One major reason is that they rely on accurate distance for positioning, which is difficult to achieve in cellular networks. Another reason is that they cannot work properly in non-line-or-sight (NLOS) propagation conditions. In this paper, we present an identification method based on the angle-of-arrival (AOA) model and the time-difference-of-arrival (TDOA) model, which have been applied widely in cellular networks. This method can identify a malicious mobile station (MS) when the positioning error caused by environmental noises is small. We also propose a cooperative secure positioning method to deal with the problem of NLOS propagation conditions which can cause a large positioning error. The underlying principle is that a malicious MS can be identified by analyzing the inconsistency in the positioning of the MSs located nearby. Our security analysis shows that compared with the TDOA model, AOA model could be more robust, as it requires only 2 BSs for a secure positioning. Our future work includes the combination of the AOA and TDOA models, and the applicability of the proposed identification method when an MS is lack of large number of neighbors.

Acknowledgement. This work was supported in part by the Natural Science Foundation of Jiangsu Province under Grant BK20140404, by the Jiangsu University Natural Science Research Programme under Grant 13KJB510035, and by the Suzhou Science and Technology Development Plan under Grant SYG201405.

References

1. Sastry, N., Shankar, U., Wagner, D.: Secure verification of location claims. In: Proceedings of ACM workshop on Wireless Security, pp. 1–10 (2003)
2. Capkun, S., Hubaux, J.: Secure positioning of wireless devices with application to sensor networks. Proc. IEEE INFOCOM **3**, 1917–1928 (2005)
3. Anjum, F., Pandey, S., Agrawal, P.: Secure localization in sensor networks using transmission range variation. In: Proceedings of IEEE MASS, pp. 195–203 (2005)
4. Wang, T., Yang, Y.: Analysis on perfect location spoofing attacks using beamforming. In: Proceedings of IEEE INFOCOM, pp. 2778–2786 (2013)
5. Liu, D.: Identifying malicious attacks to wireless localization in bad channel conditions. In: Proceedings of IEEE International Workshop on Mission-Oriented Wireless Sensor Networking (MiSeNet), pp. 636–641 (2014)
6. Zhang, Y., Liu, W., Fang, Y., Wu, D.: Secure localization and authentication in ultra-wideband sensor networks. IEEE J. Sel. Areas Commun. **24**(4), 829–835 (2006)
7. Cong, L., Zhuang, W.: Hybrid TDOA/AOA mobile user location for wideband CDMA cellularsystems. IEEE Trans. Wirel. Commun. **1**(3), 439–447 (2002)
8. Liu, D., Ning, P., Du, W.: Attack-resistant location estimation in sensor networks. In: Proceedings of ACM/IEEE IPSN 2005, pp, 99–106 (2005)
9. Capkun, S., Rasmussen, K., Cagalj, M., Srivastava, M.: Secure location verification with hidden and mobile base stations. IEEE Trans. Mob. Comput. **7**(4), 470–483 (2008)

10. Sayed, A., Tarighat, A., Khajehnouri, N.: Network-based wireless location: challenges faced in developing techniques for accurate wireless location information. IEEE Sig. Process. Mag. **22**(4), 24–40 (2005)
11. Liu, D., Lee, M.C., Pun, C.M., Liu, H.: Analysis of wireless localization in nonline-of-sight conditions. IEEE Trans. Veh. Technol. **62**(4), 1484–1492 (2013)