A Fast Active Location Detection Schema for Adversary Nodes in Wireless Networks

Siyu Zhan[1, a], Ying Wu[2, b] , Yu Xiang[1,c] and Guoming Lu[1, d]

[1]School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China;

[2] Chengdu Software Industry Development Center, Chengdu 610042, China.

[a]zhansy@uestc.edu.cn, [b]wuying1212@foxmail.com, [c]jcxiang@uestc.edu.cn, [d]lugm@uestc.edu.cn

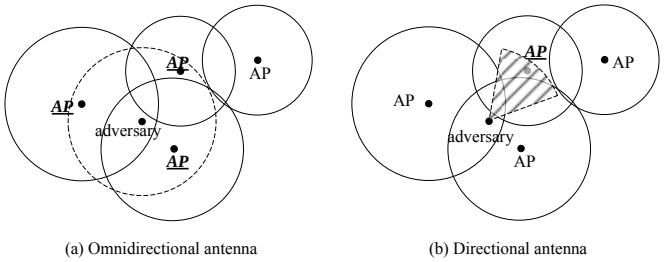
Keywords: Localization; Security; Wireless Network.

Abstract. The growing interest in location based service and wireless security necessitates the development of an effective scheme which can actively locate the attackers. In this paper, a novel localization scheme is proposed, called F-ALD, which can actively locate attackers without depending on any signal features. Compare to our previous research, the F-ALD adjusted the optimal model by calculating the expectation of aggregated reward rather than the aggregated reward. The performance evaluation shows the time cost of F-ALD reduced by 50% while there is almost no effect on the error rate. Furthermore, the F-ALD does not need any special hardware support and it can be stored in the wireless network nodes. Also, the F-ALD scheme can be supported by IEEE 802.11 and many other wireless network standards.

1. Introduction

The increasing connectivity of the Internet, the pervasive deployment of wireless networks, and the wide availability of network attack tools on the Web are providing a fertile environment for adversaries to launch network attacks against remote critical infrastructures with relative ease and anonymity. Such increasingly vulnerable and interconnected critical infrastructures include telecommunications, banking and finance, energy, transportation, and essential government services. Such attacks have motivated the development of attack countermeasures and surveillance systems to protect critical systems. Location identification is one of these defense systems, which can identify the physical location of the attack source and eliminate its threat. In addition, some location based services, such as environment monitoring, target tracking, remote system controlling, and location based authorization service[1], also need the location identification system.

However, most existing secure localization systems have focused on preventing or eliminating the effects of attackers to ensure legitimate nodes' correct location computation[2], which are named as passive localization systems in this paper. Few passive localization systems can prevent an attacker from falsifying its location when the attacker is equipped with advanced radio technologies, such as software defined radios (SDRs) and smart antennas. This is because traditional localization systems rely on passive observation of the emitted radio signals from the adversary's device and the result depends on the accuracy of the assumptions about the channel propagation model, the transmission parameters and/or the antenna pattern. With the help of advanced radio technologies, an adversary can easily change its radio parameters or beam direction, which causes a large difference between true location of the attacker and the computed result. As shown in Fig. 1, an attacker with omni-directional antenna can be seen by three neighboring nodes, while with directional antenna there is only one node can see it, which will bring a lot of troubles to traditional localization method.



(a) Omnidirectional antenna (b) Directional antenna

Fig. 1. Position estimation distortion of localization caused by beamforming

The challenge of passive localization systems is an adversary can easily change its radio features to hide itself from localization systems. To address this challenge, we proposed an active localization mechanism called F-ALD, which is an active scheme to locate the adversary based on range-free localization strategy so that it does not need any signal features to estimate the location of the adversary. In order to get the location of the adversary quickly and reduce the probability of attacker being alerted, the process of F-ALD is modeled as a finite horizon discrete Markov decision process (MDP). Compare to our previous research, the F-ALD calculated the expectation of aggregated reward to reduce the time cost 50%. Furthermore, the F-ALD does not need the support of wireless equipment which is needed in our previous research and the F-ALD has no requirement on the computation of wireless networks nodes which can be used even in WSNs (wireless sensor networks), in which the nodes always have limited computational capabilities.

The rest of the paper is organized as follows. Section II describes the related work. Section III presents the F-ALD disassociation mechanism. Its improved disassociation MDP process is in Section IV. The simulation results and implement are shown in Section V. Finally, Section VI concludes the whole paper.

2. Related Work

2.1 Challenges for range-free systems

Range-free localization systems[3] aim at estimating a possible region of a target node by collecting information about the node's connectivity with other nodes. The key to this kind of systems is that a node must connect with more than one other node. The correct mapping from connectivity information to location estimation relies on the assumption that the target node uses an omni-directional antenna and does not vary its transmission parameters. These assumptions are easily violated if an adversary adapts its transmission power and steers its beam to a certain direction with directional antennas.

2.2 Challenges for range-base systems

There are a lot of range-based systems, i.e. TOA, TOF, TDOA etc. Most of these systems share a common feature: they use absolute estimates of the nodes' mutual distances or angles to locate a wireless node. The difference of these systems is the signal features used to derive these absolute estimates. Received signal strength indicator (RSSI) [4] relies on estimated signal power strength. Time of arrival (TOA) and time difference of arrival (TDOA)[5] measure the time cost between receiver and sender. Angle of arrival (AOA)[6] involve gathering the angle of arrival measurements at the node from at least three sources. Like what it can do in range-free systems, an adversary can fool range-based localization systems by distorting angle of arrival through beamforming, power adaptation and transmission delay variation. For example, the adversary is able to steer its beam to only one node so that there is not enough distance information to locate the adversary. The adversary is also able to find a strong reflector, e.g., a wall, and steer its beam to the reflector with directional antenna. In this case, the angle of arrival is different from its direction. And it can also decrease its emission power while concentrating its emission power within a smaller angle, then RSSI would be useless in such case. As to TOA and TDOA, an intelligent attacker can intentionally delay transmit signals to bring difficulties for time measurement.

In this paper, we propose a novel scheme to solve the localization problem for such an attacker equipped with SDRs or smart antennas. It overcomes the shortcoming of these passive localization systems and is robust against the attacks from these malicious users.

3. Overview of F-ALD

In this section, we present an active scheme, F-ALD, which lures the adversary to dynamically change its connecting nodes, forces the adversary to involuntarily reveal the true features of its signal, and then identifies its location. Our discussion is based on range-free systems. In range-based systems, it could be very simple for an attacker to change the radio power or direction to hide its location.

3.1 Localization Process

F-ALD's process exploits the following assumptions. First, the attacker must connect to a neighboring wireless network node to launch network attacks. We call these nodes as the attacker's CN (connecting node). In practical systems, the CN is the access point in WLAN and is a normal neighboring node which directly receives and forwards the attack's data in WSN. We call a CN as the home CN of the attacker in initial state. Second, in order to get reliable connection with its home CN, even though the attacker may use smart antenna or SDR to narrow its beam angle, the angle is still reasonably large so that in an environment with a high density of nodes, the emitted signals of the attacker can still be received by multiple nodes.

Under these assumptions, the F-ALD processes are as followed:

1) F-ALD conservatively estimates that the attacker could be in any point in a disk within the home CN as the centroid and the estimated distance as the radius.

2) Since the initial location estimation region may be too large for localization purpose, to narrow it down, F-ALD then exploits the adversary's desire for communications to lure or force the adversary to change its home CN. This is done by luring the attacker to establish mutual connections with another CN and disconnect from its current home CN.

3) When the attacker connects to the new home CN, F-ALD obtains a new estimation disk and narrows the location estimation area down to the intersection of the original estimation area and the new estimation disk.

F-ALD repeatedly makes the attacker to switch home CNs until the targeted localization accuracy is reached or it is impossible to further narrow down the location estimation due to running out of neighboring nodes of the adversary. When F-ALD ends its active localization effort, the attacker's real location area is revealed to be in the final location estimation region.

4. Optimal Localization Model

To effectively locate an attacker, F-ALD must compute the best activation sequence of the attacker's neighbouring nodes by considering the following three factors. First, we need to locate the attacker as fast as possible. Second, there is a risk that the attacker is alerted and moves to a new location if the attacker is forced to connect to a new CN but cannot see any node. Hence, we associate with such an alert state with an alert "cost" factor C_{alert} to capture the penalty caused by the F-ALD's termination of its current localization process. Finally, the estimation region of the attacker's location is narrowed down. Hence, we define the "reward" in each step as the reduction of the attacker's location estimation area compared to the estimation in the previous step.

Considering these three factors, the best activation sequence of a step should maximize the aggregated reward while minimizing the aggregated step cost and alert cost. To calculate this best trade-off point between reward and cost, F-ALD models the best activation sequence as a Markov decision process (MDPs).

4.1. Definition of MDP

The MDP model for F-ALD's node activation process is defined as a tuple $(S,A,A(s),P_a(s,s'),r_a(s))$ where S is the state space, S is the action space, A(s) is the action space for state $s \in S$, $P_a(s,s')$ is the

transition probability of a given action a ∈ A(s) from state s to state s', $r_a(s)$ is the expected immediate reward received after taking an action a ∈ A(s) at state s.

Each state s_x in S refers to the set of CNs the attacker has connected to, where the subscript $x=x_1x_2...x_k$ represents that the attacker has connected to x_1,x_2,..., and x_k. The estimation of the attacker's location region at state s_x, denoted as Area(s_x), is the intersection of the estimation disks of all CNs in x. The only exception in the state space notation is the state that corresponds to the situations where the attacker is alerted. These states are represented by s_{alert}.

4.2. Calculation of MDP

Given the cost and reward associated with each step of the operation, the goal of F-ALD's active-CN-selection operation is to maximize the aggregation of expected rewards minus costs by using an optimal sequence of activated CNs. The optimal sequence can be computed as follows.

Given any state s_x, F-ALD determines the optimal set of activated CNs, denoted by $\pi(s_x)$, as follows:

$$\pi(s_x) := \arg\max_a \left[r_a(s_x) + \gamma \sum_{y=x+z, z\in a} P_a(s_x, s_y) V_{s_x}(s_y) \right] \quad (1)$$

, where $V_{s_x}(s_y)$ represents the maximum expected aggregated reward from state s_x to state s_y. $V_{s_x}(s_y)$ is defined as:

$$V_{s_x}(s_y) := r_{\pi(s_x)}(s_y) + \gamma \sum_{z=y+n, n\in\pi(s_y)} P_{\pi(s_y)}(s_y, s_x) V_{s_y}(s_z) \quad (2)$$

, where $0 < \gamma \le 1$ is the discounting factor for the future reward and captures the fact that the future reward is less important due to the chance that the attacker may move in the future.

To find the optimal CN activation process based on (1) and (2), there are two remaining problems, finding the transition probability between two states and defining the reward function.

1) Transition probability calculation: Given states s_x , s_y and an action a, if the transition from s_x to s_y is possible, ALD calculates the transition probability based on the two assumptions. (a) At state s_x, it is assumed that the probability density of the adversary's location is uniform over the estimated region of state s_x. (b) We assume the selection of the attacker is completely random so that each active CN in this subset has an equal opportunity to be chosen. In other words, if the attacker is inside the intersection area of an active CNs in the subset, the attacker selects any one of them as its home CN with probability 1/n.

With these assumptions, the expectation transition probability from state s_x to s_y under action n is:

$$P_a(s_x, s_y) = \sum_{k=1}^{n} \sum_{r_v\in a_k, i\in v} \frac{Area(s_x \cap r_v)}{Area(s_x)k} \quad (3)$$

, where Area(s_x) is the area of the state s_x and r_v is the region defined by the intersection of the coverage regions of nodes in *v*.

2) Reward function calculation: The reward function for an action a at state s is defined as a function of the decreased difficulty for locating the attacker within the region. Note that for a particular state, the larger is the estimated region of the attacker, the harder to locate the attacker within this region. Hence, the reward for transition from state sx to state sy can be represented by

$$r(s_x, s_y) = Area(s_x) - Area(s_y) - C \quad (4)$$

, where C is the constant cost for alert the attacker. Hence, the reward function in the MDP definition (1) becomes

$$r_a(s_x) = \sum_{y=x+z, z\in a} P_a(s_x, s_y) r(s_x, s_y) \quad (5)$$

3) *Expectation area calculation*: In our previous research, we use the Packet Test Estimate (PTE) step to narrow the expectation area. Somehow, the PTE needs some support of some wireless

equipment and it also needs the wireless network nodes can calculate the MDP process, which are two nontrivial problems need to solve.

Instead of calculate the transition probability, the expected transition probability is calculated in this paper. We modified the (3) to :

$$E\left(P_a\left(s_x, s_y\right)\right) = \sum_{k=1}^{n} \sum_{r_v \in a_k, i \in v} \frac{E\left(Area\left(s_x \cap r_v\right)\right)}{Area\left(s_x\right)k} \tag{6}$$

To calculate the $E\left(Area(s_x \cap r_v)\right)$ is very difficult as well as to calculate the relatively new radius because the shape of a node's signal coverage is not regular, so that we have to find a compromise solution. In our experiments, we studied many shapes to find out that the new radius approximately equals to $\frac{3}{4}R$.

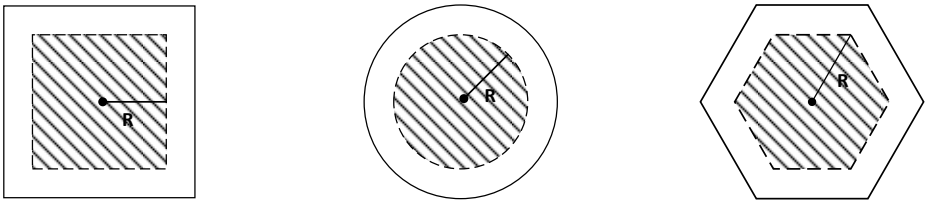


Fig. 2 the expected area calculation based on different shapes

Then, we can improve the (2) to :

$$V_{s_x}\left(s_y\right) :\cong E\left(V_{s_x}\left(s_y\right)\right) = r_{\pi(s_x)}\left(s_y\right) + \gamma \sum_{z=y+n, n \in \pi\left(s_y\right)} E\left(P_{\pi(s_y)}\left(s_y, s_x\right)\right) V_{s_y}\left(s_z\right) \tag{8}$$

5. Evaluation and Implementation

We evaluate the performance of the F-ALD in a grid topology where the nodes density in the topology is represented by the ratio r/d, where r is the radius of the coverage region of a node and d is the minimum distance between two nodes, which are as same as our previous research.

In our first simulation, we study the relationship between the network nodes density and the performance of the F-ALD as well as compare it with our previous research. As shown in Fig. 3, the error rate difference between the F-ALD and ALD is very small. The error rate of the F-ALD is just a little worse than the ALD, however the F-ALD does not need the support of wireless equipment.

In our second simulation, we study the step cost (time cost) of the F-ALD. We compare the step cost of the F-ALD with the ALD. As shown in Fig. 4, the step cost of the F-ALD is just a half of the ALD. We successfully reduce the step cost by 50% even though we do not have any support of wireless equipment like the ALD.

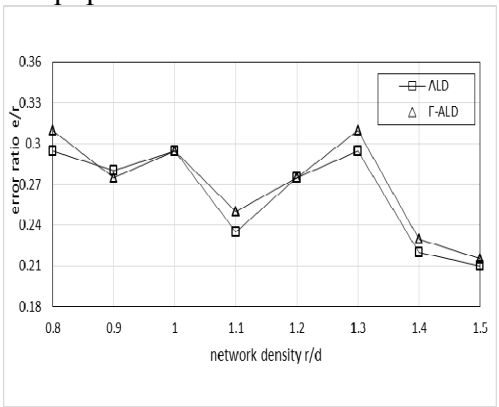


Fig. 3 the performance of the F-ALD

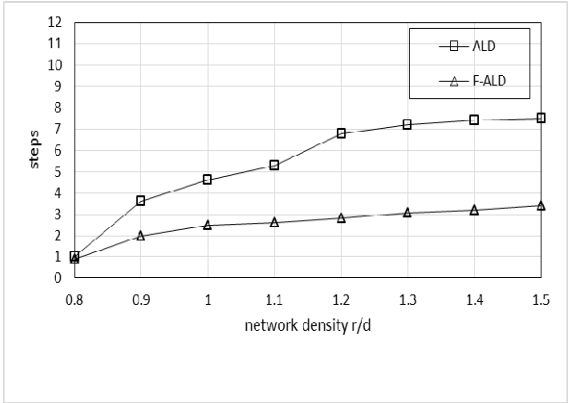


Fig. 4 the step cost of the F-ALD

6. Summary

We have presented a range-free localization scheme, called F-ALD. Different with existing secure localization schemes, it is an active scheme and will not be affected by the attacker's falsifying its position by advanced radio technologies such as SDR and smart antennas. Its process is modeled as a finite horizon discrete Markov decision process and an optimal approximation algorithm is used to solve this MDP process. Our simulation results show that the F-ALD can effectively reduce the step cost by 50% and similar error rate compared to our previous research even though the F-ALD does not need any support of wireless equipment.

Acknowledgments

This work is supported by the National Natural Science Foundation of China No. 61202444, No. 61202084, No. 61501096 and Chengdu Research Institute of UESTC No. RWS-CYHKF-02-20150005.

References

[1]. Subhankar Dhar, Upkar Varshney. Challenges and business models for mobile location-based services and advertising. Communications of the ACM. Vol. 54 (2011) No. 5, p. 121-128.

[2]. Jennifer Yick , Biswanath Mukherjee , Dipak Ghosal. Wireless sensor network survey. Computer Networks. Elsevier. Vol. 52 (2008), No. 12, p. 2292–2330.

[3]. Tian He, Chengdu Huang, Brian M. Blum, et al. Range-free localization and its impact on large scale sensor networks. ACM Transactions on Embedded Computing Systems (TECS) TECS Homepage archive. Vol. 4 (2005) No.4, p. 877-906.

[4]. Giovanni Zanca, Francesco Zorzi, Andrea Zanella, et al. Experimental comparison of RSSI-based localization algorithms for indoor wireless sensor networks. REALWSN '08 Proceedings of the workshop on Real-world wireless sensor networks. New York, NY, USA, 2008, p. 1-5.

[5]. N. B. Priyantha, A.C., H. Balakrishnan. The cricket location-support system. in Proc. of the Sixth Annual ACM International Conference on Mobile Computing and Networking (MOBICOM), Boston, Massachusetts, USA. Oct. 2001.

[6]. D. Niculescu, B.N. *Ad hoc positioning system (APS) using AOA*. in *Proc. of INFOCOM 2003, vol. 3, San Francisco, CA,USA*. Mar. 2003, p. 1734 - 1743