Secure location verification and determination

Alexander Willner
Center for Informatics
University of Goettingen
Email: mail@alexanderwillner.de

October 29, 2004

Abstract

This document considers two different approaches dealing with secure location claims. The first protocol is called ECHO [1] and handles with the secure verification of a location via ultra-sound. The second procedure increases the robustness of location determination protocols like RADAR [2]. Those are using standard IEEE 802.11 equipment. The document gives an introduction, overview, analysis and potential directions of both protocols. It focuses mainly on the security advantages or flaws.

Keywords: ECHO, IEEE 802.11, location based services, mobile systems, RADAR, secure location determination, secure location verification, wireless

1 Motivation

In mobile computing, location becomes an important factor for commercial success and security. The more confident a system can locate the position of a user or a mobile device in physical, symbolic, absolute or relative context the more application areas can be developed. Based upon the mobile device location appropriate services can be offered or refused. Determination or verification of user locations in wireless networked environments meets the requirements of many new applications. The keyword LBS[1] stands for a huge palette of new mobile services in the commercial area. These services can be found with many diverse characteristics in likewise different environments based on varying technologies.

For example a German cellular phone company charges different fees for phone calls based on the location of the mobile phone. Furthermore the mobile device can be

[1] location based services

Figure 1: Cell-ID :: example

located through a web interface (see figure 1 for example) by using the same technology: Cell-ID [3]; an other possibility to locate a mobile device is using WAP [4]. Although simple delivery tracking (e.g. DELIS-track) or city informations (e.g. MobileGIS-LS [5]) are existing LBS examples.

In order to secure locate mobile devices different protocols (e.g. [6]) were developed or existing protocols were enhanced. This is necessary since some critical applications are based on this security. This document is based on two related ACM papers [1, 7]. These are describing two different approaches which are used in the field of location-aware computing: active location *verification* and passive location *determination*.

Besides the concerned techniques other technologies and related papers are playing an important role in this field but cannot be discussed in detail: like infrared based tracking [8, 9, 10], magnetic tracking [11], Global Positioning System (GPS) [12], physical proximity [13] or computer vision systems [14, 15].

2 Location verification

2.1 Introduction

For the mobile node, location verification is an active process. It is induced by the client and verifies a stated position. Example of use: a company provides special

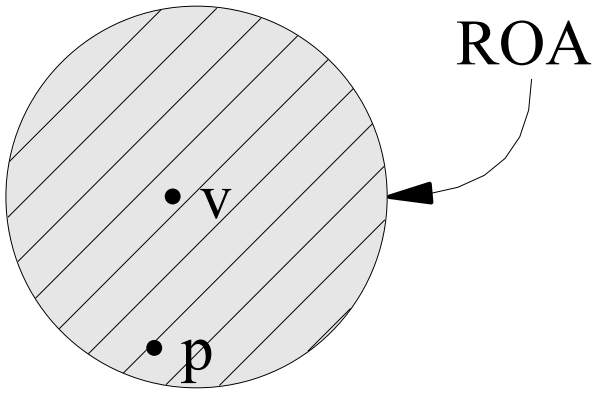

Figure 2: ECHO :: design.

informations to their customers for free if they enter a football stadium. If the clients are outside of the building, they have to pay for the service an extra fee. This chapter is describing the ECHO protocol based on a paper [1] from the University of Berkeley. The client / prover (p) has to prove its location (l) to the verifier node (v) within a region of acceptance (ROA) - (see figure 2). In other words: The football fan (p) has to prove his location (l) is inside the football stadium (ROA) to a special device (v) somewhere inside this stadium.

The work on this protocol was primarily initiated in the context of nodes in sensor networks. This caused little constraints to the used hardware. Small cheap nodes with a minimum of computation power and a variety of environmental sensors eliminate methods like public-key encryption and authentication for example. Also no prearranged setup should be required.

To meet all this requirements the problem had been simplified. With the use of *special hardware* only an *in-region verification* has to be arranged instead of a more complex verification of an exact point.

2.2 Design

The ECHO protocol is based on a more than 60 mill. years old system bats are using for orientation. The concept is to utilize speed properties of both radio frequency (RF) and sound (ultra-sound). The speed of sound waves is approx. 330 m/s and the speed of light is approx. 300.000.00 m/s).

To start the procedure the prover (p) sends a request to the verifier (v) via radio frequency. Afterwards the verifier sends an arbitrary value (N) back to the prover (p) also via radio frequency and starts a timer. Immediately after receiving the value the prover (p) sends it back to the verifier (v) via ultra-sound (see figure 3). Since the slow speed of ultra-sound the verifier (v) then can calculates the distance to the prover (p)

COMMUNICATION PHASE:

1. $p \xrightarrow{\text{radio}}$ broadcast : (ℓ, Δ_p).
   The prover broadcasts its claimed location ℓ and processing delay Δ_p.
2. $t_s \leftarrow$ **time** ().
   $v \xrightarrow{\text{radio}} p : N$.
   A single verifier v starts its timer and responds with a random nonce
   We require $\ell \in \mathsf{ROA}(v, \Delta_p)$ and $\Delta_p \geq \frac{n}{b_o} + \frac{n}{b_i}$.
   If no such verifier exists or Δ_p is invalid, **abort**.
3. $p \xrightarrow{\text{sound}} v : N$.
   $t_f \leftarrow$ **time** ().
   The prover echoes the nonce over ultrasound.
   The verifier records the finish time.

VERIFIER COMPUTATION PHASE:

4. **if** sent nonce differs from received nonce
   return false
5. **if** $t_f - t_s > \frac{d(v,\ell)}{c} + \frac{d(v,\ell)}{s} + \Delta_p$
   return false
6. Otherwise, **return true**

Figure 3: ECHO :: formal description

after receiving the arbitrary value by using the timer and the known speed of sound. The longer it takes for the verifier to receive the sent value the bigger is the distance to the prover (see figure 2). In other words: If the football fan is outside the stadium the ultra-sound waves from his device to the verification node inside the stadium take too long.

1. $p \xrightarrow{radio} v : l$
2. $v \xrightarrow{radio} p : N$
3. $p \xrightarrow{sound} v : N$

v accepts if $l \in R$ and elapsed time $\leq d(v, l) * (c^{-1} + s^{-1})$

Due the use of special hardware and simplification of the problem this procedure is a very simple and secure solution. Its security is based on physical laws which cannot be falsified. But the following subsection will elaborate three problems which come along with this design.

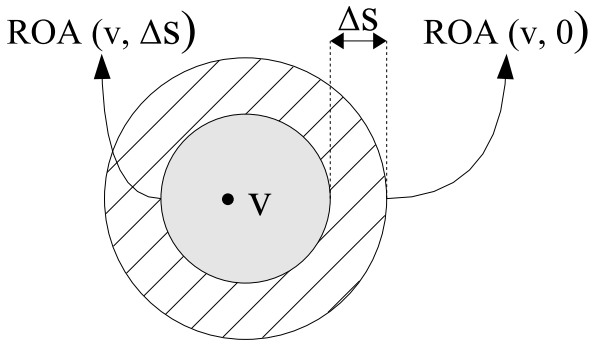

Figure 4: ECHO :: processing delay

2.3 Protocol security

2.3.1 Processing delay

In ideal case the prover can response immediately after receiving the value. In practice the prover needs a processing delay of at least Δs seconds. As we can remember the verifier node calculates the distance by checking the response time. The longer the prover needs to send the value back the bigger is the distance the verifier is calculating. A delayed answer is reducing the checkable region of acceptance (ROA) depending on the client response time (see figure 4). In other words: Assuming the football fan owns a device which needs a long time to receive and send the informations. Than, depending on his device, he has to be located very close to the verifier node to be able to prove that he is actually in the stadium.

Since physical laws it is not possible to answer faster than in $\Delta s = 0$ seconds. From this follows that it is not possible to fake a position closer to the verifier node by manipulating the processing delay.

2.3.2 Packet transmission time

Depending on the length of the arbitrary value (N) it takes some time to broadcast and receive all bits. This period is also reducing the checkable ROA. An attacker could exploit the transmission delay to launch an attack, he could simply guess the first (or last) few bits of the nonce and send them preemptively. Suppose the verifier stops its timer upon receiving the first bits. The attacker could start sending a few randomly guessed bits. Due to that, the verifier calculates a too small distance.

To avoid any possible attacks the verifier starts timing before sending first bit and stops after receiving the last bit. This maximizes the transmission time and is reducing the valid ROA again.

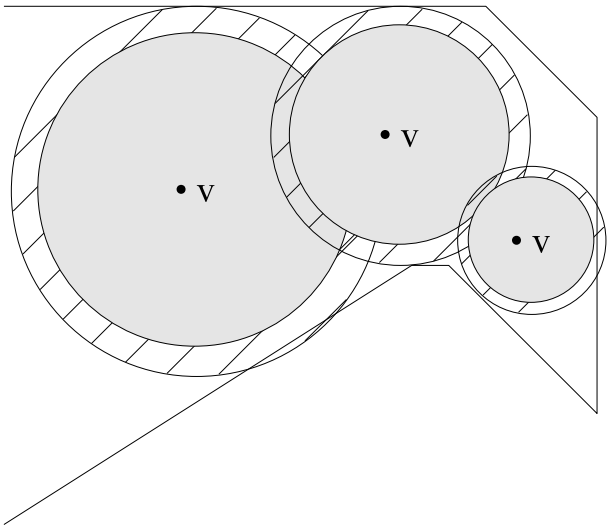

Figure 5: ECHO :: non-circular regions

2.3.3 Non-circular regions

Since the we assume that our communication equipment is unidirectional and signals travel at the same time the ROA must be a circle. But in general the area which has to be covered is a square or a polygon but not a circle. It could happen that the circular ROA overlaps a different shaped area and an attacker could be in the ROA without being in the covered area.

The use of multiple verifier nodes with different ranges of coverage can avoid this problem see (figure 5). It is not possible to get a squared ROA but 5 manually placed nodes can maximize the coverage of a square to 93.3%.

2.4 Summary

In this section an in-region verification technique and possible problems were introduced. The ECHO protocol is a provable secure and lightweight protocol. Its security rests on physical properties of sound and RF signals and does not require any cryptography, time synchronization or any prior agreements. Therefore it is suitable for low-cost devices such as those in sensor networks.

For 80-90% of legitimate location claims it can guarantee in-region verification and it is based on specific hardware.

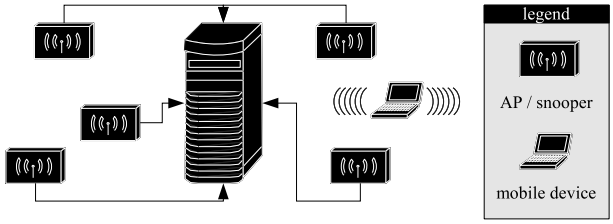

Figure 6: RADAR :: design

3 Location determination

3.1 Introduction

Verification determination is a passive process for the client; it is a server-side process to locate the position of a mobile device. This chapter considers a system, very similar to the RADAR protocol [2, 16], introduced by a paper [7] of the University of Houston.

RADAR is using the existing RF[2] infrastructure to achieve localization. It uses the signal strength to construct a radio map of a defined region[3]. With the use of the constructed map and the received signal strength of a mobile node the system can calculate the position. This solution is easy in deployment, scalable, cheap (no special hardware) and low in maintenance.

The original RADAR protocol is using typical IEEE 802.11 compatible equipment to locate devices without their permission. Other papers [17, 18, 19] are trying to enhance the accuracy of WLAN location determination. But a malicious node for example does not want to be located at the right position and could modify its hardware or variate its transmission power. This is the focus of the concerned paper.

3.2 Design

The first system to use signal strength from standard WLAN cards to detect locations was RADAR. Correlating sensor readings from different known positions are used to build a radio map of a region. This is called the *off-line* phase. As shown in figure 6 different sensors are connected to a central server. They are called *snoopers* and are responsible for observing the signal strengths. Instead of only receiving packets from associated stations snoopers are receiving all traffic on any given channel if requested.

During the *on-line* phase sensor measurements are used by the central server to calculate the position relative to the known positions. This is usually done by using a Markov localization algorithm [20, 21, 22].

[2]radio frequency
[3]see ROA

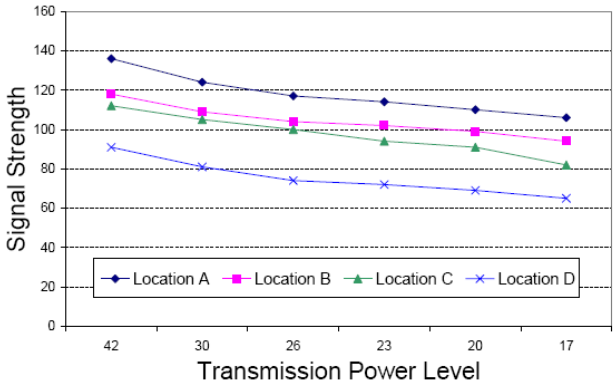

Figure 7: RADAR :: Lower transmission power cause linear decreases of all observed signal strength

3.3 Security enhancements

Model errors, multi-path-problems[4] or signal strength modifications can articulately reduce the accuracy of location determination systems. Such errors can also be exploited by malicious users to hide their position. To avoid this problems the localization algorithm was modified.

The *histogram method* was developed in prior work [17] of the same authors. It is a Bayesian algorithm which uses directly the signal strength histogram obtained from training to calculate each position. This method assumes that the trained signal strength histogram accords to the observed signal strength in the on-line phase. If the client is using a different WLAN implementation or jitter its transmission power this assumption is not true.

Lower transmission power cause linear decreases of all observed signal strength (see figure 7). This observation helps to design a filter to increase the robustness of location determination. The *difference method* is using these differences observed signal strength instead of the raw signals. It is a weighting heuristic loosely based on Bayesian inference. The training data gets post-processed after the off-line phase to be the signal strength difference between every pair of snoopers. The central server computes the differences of all data between every pait of snoopers for localization determination. The generated statistic from all packets during each inference window is defined as the observation.

[4]reflection, scattering or diffraction caused by layout, construction material, electrical links, object or people

3.4 Summary

The introduced indoor server-side location system can handle unmodeled variations in hardware and transmission power. After an off-line phase devices can be located in an defined region with standard IEEE 802.11 WLAN equipment. Both systems could be improved in their exactness. They fail to locate devices outside the trained area.

Unlike the histogram method fluctuating signal strength or modified hardware have much less effect to the difference methods accuracy. The histogram method is very sensitive to other aspects than the training model. In particular in the case of locating a malicious device the method is insufficient robust.

4 Conclusion and outlook

Despite the different fields of appliance both systems are capable to gain user services and specific informations based on his/her physical position. Both issues are able to work within a specific (trained) local range. Different possible attacks and security problems were mentioned and solved.

The ECHO system uses specialised hardware to solve an in-region localization. A more precise region verification could be done by using the intersections. Right now the different verification nodes do not communicate with each other. This would potentiate a triangulation to narrow a more exact position of the client down. Also pre-shared keys could be used to verify that a particular prover is inside a region.

The introduced indoor server-side location system can be used with standard IEEE 802.11 equipment. The localization methods could be enhanced for a better accuracy. Even assumptions based on simple probabilistic model of human movement could be used to improve the systems precision. Attacker with non-standard antennas (e.g. parabolic) and malicious devices outside the trained area still can trick the system. The possibility to track a users movement without his/her permission also raises interesting privacy issues.

To complete the picture of related literature I want to point out some chosen papers in the bibliography at the end of the paper, since those were not particularly mentioned in the chapters above.

- Cellular-Based Systems: [23, 24] and see above.
- Ultrasonic-Based: [25, 26, 27, 28, 29]
- RF Propagation Models: [30]
- Ad-hoc RF-Based Systems: [31, 32, 33, 34]
- Infrastructure RF-Based Systems: [35, 36, 37, 38]

References

[1] Naveen Sastry, Umesh Shankar, and David Wagner, "Secure verification of location claims," *University of California, Barkley*, 2003.

[2] Paramvir Bahl and Venkata N. Padmanabhan, "Radar: An in-building rf based user location and tracking system," *Proceedings of IEEE INFOCOM*, 2000.

[3] Nico Deblauwe, Leo Van Biesen, "A cellular localisation technology: Multi cell-id," *Vrije Universiteit Brussel*, 1999.

[4] Ch. Wong, M.C. Lee, and R. Chan, "Gsm-based mobile positioning using wap," *Chinese University of Hong Kong.*

[5] Dr. Uwe Jasnoch, Dr. Dirk Balfanz, Ralf Schfer, Heiko Blechschmied, and Dirk Burmeister, "Mobile location-based services for darmstadt," *Fraunhofer institute for graphical data processing*, 2002.

[6] Konidala M. Divyan, Robert H. Deng, Jianying Zhou, and Kwangjo Kim, "A secure and privacy enhanced location-based service transaction protocol in ubiquitous computing environment," *The 2004 Symposium on Cryptography and Information Security Sendai, Japan*, 2004.

[7] Ping Tao, Algis Rudys, Andrew Ladd, and Dan Wallach, "Wireless lan location-sensing for security applications," *Rice University, Houston*, 2003.

[8] H. Ma and J. A. Paradiso, "The findit flashlight: Responsive tagging based on optically triggered microprocessor wakeup," *UbiComp, Gothenburg, Sweden*, 2002.

[9] R. Azuma, "Tracking requirements for augmented reality," *Communications of the ACM, Vol. 36, No. 7.*, 1995.

[10] Roy Want, Andy Hopper, Veronica Falco, and Jonathan Gibbons, "The active badge location system," *ACM Transactions on Information Systems, Vol. 10, No. 1, pp 91-102.*, 1992.

[11] E. Prigge and J. How, "Signal architecture for a distributed magnetic local-positioning system," *The first IEEE international conference on sensors, Orlando, Florida*, 2002.

[12] P. Enge, and P. Misra, "Special issue on gps: The global positioning system," *Proc. of the IEEE*, 1999.

[13] Robert J. Orr and Gregory D. Abowd, "The smart floor: A mechanism for natural user identification and tracking," *Proceedings of the 2000 Conference on Human Factors in Computing Systems, The Hague, Netherlands*, 2000.

[14] Krumm J, Harris S, Meyers B, Brumitt B, Hale M and Shafer S., "Multi-camera multi-person tracking for Easy Living," *Proc. 3rd IEEE Intl Workshop Visual Surveillance, IEEE Press, Piscataway*, 2000.

[15] Earl Joseph Charlson, Huber L. Graham, and Xinhua Zhuang, "Video Camera Method for Moving-Vehicle Location," *IEEE Transactions on Vehicular Technology*, 1998.

[16] P. Bahl and V. N. Padmanabhan, "Enhancements to the radar user location and tracking system," *Technical Report, Microsoft Research*, 2000.

[17] A. M. Ladd, K. E. Bekris, A. Rudys, G. Marceau, L. E.Kavraki, and D. S. Wallach, "Robotics-based location sensing using wireless Ethernet," *Proceedings of The Eighth ACM International Conference on Mobile Computing and Networking(MOBICOM), Atlanta, GA*, 2002.

[18] M. Youssef and A. Agrawala, "Small-scale compensation for WLAN location determination systems," *Proceedings of IEEE Networking and Communications Conference, New Orleans, LA*, 2002.

[19] M. Youssef, A. Agrawala, and A. U. Shankar, "WLAN location determination via clustering and probability distributions," *Proceedings of IEEE Conference on Pervasive Computing and Communications, Fort Worth, TX*, 2003.

[20] Wolfram Burgard, Dieter Fox, Daniel Hennig, and Timo Schmidt, "Estimating the absolute position of a mobile robot using position probability grids," *Proceedings of the Thirteenth National Conference on Artificial Intelligence*, 1996.

[21] Reid Simmons and Sven Koenig, "Probabilistic robot navigation in partially observable environments," *Proceedings International Joint Conference on Artificial Intelligence*, 1995.

[22] Leslie Pack Kaelbling, Anthony R. Cassandra, and James A. Kurien, "Acting under uncertainty: Discrete bayesian models for mobile-robot navigation," *Proceedings of the IEEE/RSJ International Conference on Intelligent Robots and Systems*, 1996.

[23] T. Liu, P. Bahl and I. Chlamtac, "Mobility Modeling, Location Tracking, and Trajectory Prediction in Cellular Networks," *IEEE Journal on Special Areas in Communications, Special Issue on Wireless Access Broadband Networks*, 1998.

[24] Sirin Tekinay, "Special issue on Wireless Geolocation System and Services," *IEEE Communications Magazine*, 1998.

[25] Nissanka B. Priyantha, Allen Miu, Hari Balakrishnan, and Seth Teller, "The Cricket Compass for Context-Aware Mobile Applications," *Proc. 7th ACM MobiCom, Rome, Italy*, 2001.

[26] Nissanka B. Priyantha, Anit Chakraborty, Hari Balakrishnan, "The Cricket Location-Support system," *Proc. 6th ACM MobiCom, Boston, MA*, 2000.

[27] Andy Harter and Andy Hopper, "A Distributed Location System for the Active Office," *IEEE Network, Vol. 8, No. 1*, 1994.

[28] A. Harter, A. Hopper, P. Steggles, A. Ward, and P. Webster, "The anatomy of a context-aware application," *Proceedings 5th ACM MobiCom Conf.*, 1999.

[29] Andy Ward, Alan Jones, Andy Hopper, "A New Location Technique for the Active Office," *IEEE Personal Communications, Vol. 4, No. 5*, 1997.

[30] H. Hashemi, "The indoor radio propagation channel," *The indoor radio propagation channel*, 1993.

[31] Dragos Niculescu, Badri Nath, "Ad Hoc Positioning System (APS) Using AoA," *INFOCOM*, 2003.

[32] Slobodan N. Simic' and Shankar Sastry, "A Distributed Algorithm For Localization In Random Wireless Networks," *Department of Electrical Engineering and Computer Sciences, University of California Berkeley*, 2001.

[33] S. Capkun, M. Hamdi, J. P. Hubaux, "GPS-Free Positioning in Mobile Ad-Hoc Networks," *Proceedings of HICSS, Hawaii*, 2001.

[34] Nirupama Bulusu, John Heidemann, Deborah Estrin, "GPS-less Low Cost Outdoor Localization For Very Small Devices," *Technical report 00-729, Computer science department, University of Southern California*, 2000.

[35] Moustafa Youssef and Ashok Agrawala, "On the Optimality of WLAN Location Determination Systems," *Communication Networks and Distributed Systems Modeling and Simulation Conference, San Diego, California.*, 2004.

[36] S. Ganu, A.S.Krishnakumar, P.Krishnan, "Infrastructure-based Location Estimation in WLAN Networks," *IEEE Wireless Communications and Networking Conference*, 2004.

[37] Thomas Christ, Philip Godwin, "A Prison Guard Duress Alarm Location System," *Proc. IEEE International Carnahan Conference on Security Technology*, 1993.

[38] Roberto Battiti, Thang Lee Nhat, Alessandro Villani, "Location-aware computing: a neural network model for determining location in wireless LANs," *Technical Report DIT-02-0083*, 2002.