ProVer: A Secure System for the Provision of Verified Location Information

Michelle Graham and David Gray

School of Computing, Dublin City University, Dublin, Republic of Ireland
{mgraham,dgray}@computing.dcu.ie

Abstract. With location becoming one of the few key pieces of context regarding a user and services springing up to take advantage of this, location verification is an increasingly important system aspect, allowing these services to trust in a device's supplied location. We propose to remove the burden of providing this feature from Location Based Services (LBS) through the introduction of ProVer, a system to provide verified location information regarding any mobile user employing a wireless device. ProVer does not rely on a pre-existing infrastructure to verify a device's location but instead employs evidence from neighbouring devices to confirm a specific device's presence, allowing almost unlimited reach in the system's coverage. ProVer also ensures a device's personal information, such as identity and location, remain private and secure, allowing devices to participate in the system with confidence.

1 Introduction

In recent years, there has been a definite shift towards mobile computing, with more and more services moving to a mobile setting. For this reason, the issue of context has become a key factor, with location being a crucial part of the context of any situation. Many services have since been introduced into the public domain capitalising on a user's location [1], and these Location Based Services (LBS) continue to grow in popularity, with the market seeing no sign of reaching saturation point. One area of LBS development involves the employment of more reliable location information than simple GPS coordinates or user provided data. For example, those services which employ location as a form of access control require their users to prove themselves to be within a specific area in order to access the content requested [2]. This form of "verified" location information is costly, requiring those LBS employing it to somehow verify the current location of a user, usually through the use of some sort of infrastructure. The need to possess such a capability reduces the number of different possible LBS through discouraging the development of those services employing verified location information.

To address this issue, we have developed ProVer, a system for the Provision of Verified location information. ProVer can provide secure, verified location information, which can then be employed by any LBS. This approach removes the need for LBS to possess the location verification capability themselves, abstracting this process away from their system and allowing them to focus on employing

S. Ystad et al. (Eds.): MobiCASE 2009, LNICST 35, pp. 366–373, 2010.

the location information within their services. ProVer does not rely on a pre-existing infrastructure, but instead employs other devices in the vicinity of the requesting device, thus allowing the system's coverage to extend far beyond any infrastructure-bound approach.

In this paper, we introduce ProVer as a method of abstracting the task of location verification away from LBS. This work outlines the complete ProVer system, including both a protocol for the protection of evidence gathering and a trust-based approach to verification once evidence has been supplied by the claiming device. In Section 2, we discuss other work on location verification. In Section 3, we outline the functionality of the system and its approach to location verification. In Section 4, we list a small selection of possible applications for ProVer and the benefit of employing an intermediary approach to location verification. Finally, in Section 5 we conclude the paper.

2 Related Work

With the ongoing increase in popularity of mobile computing and networking, a great deal of focus has been placed on the development of positioning and localization systems to capitalise on a device's location as user context information. These systems have traditionally been based upon an existing infrastructure [3,4,5] of trusted receiver devices, allowing location to be calculated relative to these based upon a variety of techniques, such as the measurement of radio frequency (RF) signal strength [6] and time difference of arrival [7]. These techniques have since been adapted to the area of location verification, with a heavy bias towards infrastructure dependence. In [8], Waters and Felten presented the Proximity Proving protocol, a protocol to securely verify a device's location based upon RF time of arrival (ToA). In this protocol, a device proved its location to a trusted entity in its vicinity, whose verdict could then be passed to a central Verifier. However, the timed segment of the Proximity Proving protocol is not tied to the identity of the device making a location claim, leaving it vulnerable to a collusion attack. Sastry et al [9] proposed a similar approach in the Echo protocol, employing both Ultrasound (US) and RF in its ToA calculations. However, due to the employment of US on the response leg of the exchange, this approach is vulnerable to wormhole attacks. In [10], Vora and Nesterenko proposed the use of sensors not only as location verifiers within a particular acceptance zone, but also as rejectors. This approach is heavily reliant upon infrastructure, requiring sensors within the area to function as verifiers in addition to those forming a perimeter around the acceptance zone. Capkun and Hubaux have presented several approaches to verification [11,12], though their focus is primarily on infrastructure or trusted-entity based systems. However, Capkun and Hubaux have also proposed an ad hoc adaptation of their verifiable multilateration technique [13], allowing for its employment in non-infrastructure dependent systems.

3 System Outline and Security

The ProVer system is comprised of three distinct phases; the initialisation stage, where a device requests to have its location verified, the evidence gathering stage and the verification stage, where a final verdict is reached. In the initialisation stage, a device wishing to have a location verified (Claimant) sends a request to the central entity (Verifier). The Verifier processes this request and supplies the Claimant with a list of devices in its vicinity (Proof Providers). The Claimant then begins the evidence gathering stage (section 3.2), communicating with each of the supplied Proof Providers to gather its evidence. When this process has been completed, the Claimant forwards the resulting evidence to the Verifier for use in the verification stage (section 3.3). For clarity's sake, ProVer's exchange sequence is depicted in 1. In order to participate within ProVer, either as a Claimant or a Proof Provider, a device is assumed to possess wireless ad-hoc communication capabilities, a set of asymmetric encryption keys as well as sufficient power to compute encryptions, digital signatures and decryptions in a timely manner. It is also assumed that participants possess a number of pseudonyms for use as identities, although a single core identity may also be used.

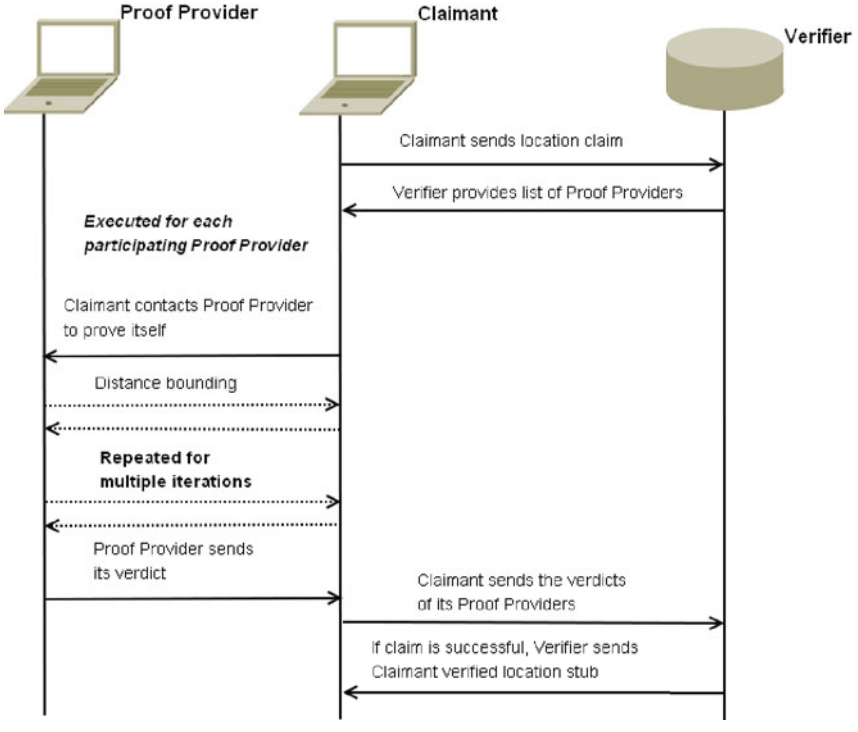

Fig. 1. ProVer exchange overview

3.1 Initiating a ProVer Session

When a device wishes to provide a verified location to a Location Based Service, it contacts the ProVer system, requesting to have its location verified. Upon receiving an initialisation request from a Claimant, the Verifier sends a message to the area seeking devices in the Claimant's vicinity to volunteer as Proof Providers. This is achieved through the employment of geographic routing [14], where a message is routed to an area rather than a specific address. Through transmitting the request in this manner, the Claimant is removed from the volunteer gathering process, protecting it from manipulation. Geographic routing also ensures that those devices which respond are in the correct area, i.e. that area mentioned in the Claimant's location claim. Those devices which respond to this volunteer request are then placed in a volunteer pool for this claim, from which the Verifier selects the final Proof Providers for use within the evidence gathering process. This selection can be done based on a number of criteria, such as those with the highest trustworthiness value or most suitable location, or it may simply be random. With the selection of Proof Providers from the volunteer pool completed, the Verifier then composes a message containing the identities of each and forwards this to the Claimant. The Claimant can then proceed to the evidence gathering stage of the verification process.

3.2 Protecting the Evidence Gathering Process

Once the Claimant receives its list of Proof Providers from the Verifier, it contacts each device and attempts to prove its presence in the area. This is achieved through the use of distance bounding [15], where a series of challenge-response exchanges are timed in order to confirm that the device responding to the challenges is within a reasonable distance. If the Claimant can respond to the Proof Provider's challenges with the correct, digitally signed response within an acceptable time limit, it is deemed to be within communication range of the Proof Provider and therefore in the vicinity, thus proving its presence. We employ a binary metric [16] in this process to confirm the absence of a proxy attack, in order to ensure that the Proof Provider be deceived into believing that the Claimant is in the area when it is not. Each Proof Provider, upon completion of the distance bounding portion of the process, compiles an evidence message and transmits this to the Claimant for forwarding to the Verifier. This message is digitally signed by the Proof Provider and composed of the Claimant's identity, a timestamp, the Proof Provider's current location and finally, a verdict regarding the Claimant's presence in the area. The Proof Provider's verdict is a binary number, with "1" indicating a positive decision and "0" a negative.

The ProVer system employs an extended version of the Secure Location Verification Proof Gathering Protocol (SLVPGP) [17], thus offering a choice between three levels of security due to its tiered design. This protocol has been designed to protect the evidence gathering process from external attackers, as well as preventing its manipulation by malicious entities, both internal and external. Through the employment of digital signatures on the messages preceeding and

following distance bounding, the integrity of information is preserved, while encryption prevents the leakage of sensitive personal information regarding participants. ProVer extends the SLVPGP through the inclusion of a final step in which the Verifier provides a verified location stub to the Claimant. This location stub is digitally signed by the Verifier and therefore cannot be undetectably tampered with. It contains the identity of the Claimant, in addition to a timestamp and the verified location, thus tying the particular verification to a specific time. In versions two and three of the SLVPGP, this signed location stub is also encrypted with the Claimant's public key, protecting its contents from eavesdroppers.

3.3 Computing the Veracity of a Claim

Upon completion of the evidence gathering stage, the Verifier receives the total collected evidence from the Claimant, for use in the calculation of its verdict. Before calculating the value of each piece of evidence, the Verifier first confirms that the evidence provided is legitimate. With each proof cleared for inclusion, the Verifier then assigns the evidence contained within the message a weight. As in the calculation of the maximum possible trust value for the claim, this weight is calculated based on the trustworthiness of the Proof Provider from which the evidence was obtained. Within the ProVer system, trustworthiness is calculated using a probability expectation formula, with a device's behaviour history within the system used as inputs for the function according to the formula

$$E(P) = \frac{\alpha}{\alpha+\beta}$$

with α representing the positive events in the behaviour history and β representing the negative events. This approach is drawn from Josang and Ismail's beta reputation system [18]. More recent events within a device's behaviour history are given more weight, through the employment of a fading factor, drawn from Buchegger and Le Boudec's reputation engine [19]. We modify their fading factor to permanently decrease the importance of older events based on the passing of time, through their removal from the behaviour history record. This modification prevents a device from retaining its trustworthiness value despite the passing of time, simply due to lack of activity. While Buchegger and Le Boudec also provide an approach to time-based fading in addition to activity-based, they enact time-based fading over the entire history of the device, which we feel too harsh an approach. The parameters employed within this calculation, α and β, are drawn from the device's behaviour history, in which that device's positive and negative behaviour is recorded for a particular role. If a device is deemed to have behaved positively in an exchange, i.e. it is honest and its verdict is in agreement with the overall verdict for that claim, it receives a positive entry in the behaviour history. If it is deemed to have behaved dishonestly, i.e. its verdict disagrees with the overall outcome of the claim, then it receives a negative entry. However, if the claim receives an "unsure" verdict, the behaviour histories of the devices involved are not updated as no judgement can be made of their behaviour.

With the trustworthiness of each Proof Provider known, its value is multiplied by the value of the evidence it provided (either a "1" or "0") to produce the

weighted evidence value. These values are then summed together, along with the trustworthiness value of the Claimant, to provide a total trust value for the claim. This value is placed on the possibility scale and the claim's final verdict is extracted. The possibility scale is composed of the maximum possible trust value for the claim (calculated by multiplying the trustworthiness values of all Proof Providers supplied to the Claimant by a positive verdict value and adding this to the Claimant's weighted trustworthiness value) and is broken up based on two thresholds, 40% and 70%. The employment of thresholds in this situation and not fixed values allows the verification process to be flexible, customising itself to the unique parameters of each claim. The first segment of the scale runs from 0% - 40%, with claims falling between these thresholds receiving a "not possible" verdict. The second segment runs from 40% to 70%, with claims falling between these thresholds receiving an "unsure" verdict. The final segment runs from 70% to 100%, with claims falling between these thresholds receiving a "possible" verdict and a signed verified location stub for use with other LBS. Once the overall verdict has been reached and the Claimant informed, the Verifier updates the behaviour histories of the devices involved.

3.4 Security of the ProVer System

As mentioned previously, the ProVer system is an extension of the SLVPGP, a protocol designed to protect the gathering of proof for location verification. In [17], the authors present a number of protocol versions, each more secure than the last. For each extension of the SLVPGP, a final verification provision stub has been designed, in keeping with the level of security provided by that extension. This approach reduces the increase in overhead costs due to data transmission and computation to a level similar to that already incurred by that extension.

The SLVPGP has been fully model checked using Casper [20] and FDR [21], confirming its security for the environment described. The ProVer extension does not impact this level of security, due to its conformity to the design standards present for each version of the protocol. Therefore, due to this fact and that the system design (the Verifier's powers and structure) does not change in adapting itself to perform as ProVer, ProVer is a secure method of verifying a location, and based upon the version employed, does not leak secure information regarding any of the participants. However, due to the method of communication and evidence gathering employed (RF transmissions received by all devices within range), information regarding the location of a device is leaked to others within its vicinity. An examination of this information leakage and its impact is available in [22].

4 Applications

As discussed briefly in section 1, we envision many possible applications for ProVer in the mobile user market. With the ever-increasing market dominance of smartphones, mobile networking capabilities are now commonly used, with new Location Based Services released regularly to capitalise on this growth.

The introduction of ProVer to the market not only allows the development of more highly functioning LBS, relying on verified information without the need for individual positioning facilities, but also allows currently available LBS to expand their services to a new level.

The linking of location and time information within the ProVer proof stub has potential for use within promotional offers, such as in-store promotions offered to customers on the premises during a specific period. A second advantage of tying location and time in this manner is the provision of access control conditional upon being at a specific location at a specific time. If the location stub was not tied to a time, it would have no expiration and thus could be used infinitely many times.

The generic nature of the location information provided by ProVer allows for its inclusion in a multitude of systems and services. A location stub is comprised of a digitally signed message containing a timestamp and a device's identity and location (in GPS format). As the location information provided is in a standardised form and not a proprietary format, it can be employed within any LBS. Rather than relying upon device based localization techniques (such as cell ids), the generic location information supplied by ProVer would allow for a device's location information to be built up without reliance on infrastructure or costly network queries.

5 Conclusion and Future Work

In this paper, we present ProVer, a system for the Provision of Verified location information. We envision ProVer as a third party location verifier, whose verified proofs can be supplied to Location Based Services (LBS) rather than those services needing to verify or compute locations themselves. This effectively abstracts the need for location verification functionality away from LBS themselves, reducing the complexity of introducing new LBS to the marketplace. ProVer does not rely on a pre-existing infrastructure for location verification, but instead employs neighbouring regular devices as evidence sources, infinitely extending the system's reach while drastically reducing its cost.

In future work, we intend to conduct a complete simulation of the ProVer system, including distance bounding, mobility in nodes and verification of claims. In addition to this, we intend to investigate the impact of heavy traffic on the effectiveness of distance bounding. Currently, our assessment of distance bounding and the binary metric has been based on results generated within a relatively empty network. We wish to confirm that these results hold true for a network with increased levels of network traffic.

References

1. LBSZone (2009), `http://www.lbszone.com`
2. Ardagna, C.A., Cremonini, M., Damiani, E., di Vimercati, S.D.C., Samarati, P.: Supporting location-based conditions in access control policies. In: ASIACCS 2006: Proceedings of the 2006 ACM Symposium on Information, computer and communications security, pp. 212–222 (2006)

3. Want, R., Hopper, A., Falcao, V., Gibbons, J.: The active badge location system. ACM Trans. Inf. Syst. 10(1), 91–102 (1992)
4. Ward, A., Jones, A.: A new location technique for the active office. Personal Communications of the IEEE 4(5), 42–47 (1997)
5. Correal, N.S., Kyperountas, S., Shi, Q., Welborn, M.: An uwb relative location system. In: IEEE Conference on Ultra Wideband Systems and Technologies, pp. 394–397 (2003)
6. Bahl, P., Padmanabhan, V.N.: Radar: An in-building rf-based user location and tracking system. In: INFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies, pp. 775–784 (2000)
7. Priyantha, N.B., Chakraborty, A., Balakrishnan, H.: The cricket location-support system. In: MobiCom 2000: Proceedings of the 6th annual international conference on Mobile computing and networking, pp. 32–43. ACM, New York (2000)
8. Waters, B., Felten, E.: Secure, private proofs of location. Technical report, Princeton University (January 2003)
9. Sastry, N., Wagner, D.: Secure verification of location claims. In: WiSe 2003: Proceedings of the 2nd ACM workshop on Wireless security, pp. 1–10 (2003)
10. Vora, A., Nesterenko, M.: Secure location verification using radio broadcast. IEEE Transactions on Dependable and Secure Computing 3, 377–385 (2006)
11. Capkun, S., Cagalj, M., Srivastava, M.: Secure localization with hidden and mobile base stations. In: Proceedings of the 25th IEEE Conference on Computer Communications (INFOCOM 2006), pp. 1–10 (2006)
12. Čapkun, S., Rasmussen, K., Čagalj, M., Srivastava, M.: Secure location verification with hidden and mobile base stations, IEEE Educational Activities Department, vol. 7, pp. 470–483 (2008)
13. Capkun, S., Hubaux, J.P.: Securing position and distance verification in wireless networks. Technical report, EFPL (2004)
14. Mauve, M., Widmer, A., Hartenstein, H.: A survey on position-based routing in mobile ad hoc networks. IEEE Network 15(6), 30–39 (2001)
15. Brands, S., Chaum, D.: Distance-bounding protocols (extended abstract). In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 344–359. Springer, Heidelberg (1994)
16. Graham, M., Gray, D.: Can you see me? the use of a binary visibility metric in distance bounding. In: Liu, B., Bestavros, A., Du, D.-Z., Wang, J. (eds.) Wireless Algorithms, Systems, and Applications. LNCS, vol. 5682, pp. 378–387. Springer, Heidelberg (2009)
17. Graham, M., Gray, D.: Protecting privacy and securing the gathering of location proofs - the secure location verification proof gathering protocol. In: Proceedings of the 1st International ICST Conference on Security and Privacy in Mobile Information and Communication Systems (MobiSec 2009) (June 2009)
18. Josang, A., Ismail, R.: The beta reputation system. In: e-Reality: Constructing the Economy (June 2002)
19. Buchegger, S., Boudec, J.Y.L.: A robust reputation system for mobile ad-hoc networks. Technical report (2003)
20. Lowe, G.: Casper: A compiler for the analysis of security protocols. In: IEEE Computer Security Foundations Workshop, p. 18 (1997)
21. Roscoe, A.W.: Modelling and verifying key-exchange protocols using csp and fdr. In: Computer Security Foundations Workshop, p. 98 (1995)
22. Rasmussen, K.B., Čapkun, S.: Location privacy of distance bounding protocols. In: CCS 2008: Proceedings of the 15th ACM conference on Computer and communications security, pp. 149–160. ACM Press, New York (2008)