International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 4 | ISSN : 2456-3307

Woral : A Witness Oriented Secure Location Attribution Framework for Cellular Phone Devices

Yenumala. Sankara Rao*[1], Maddula Venkata Siva Nagalakshmi[2]
*[1]Associate Professor, Department of MCA , St. Mary's Group Of Institutions, Guntur, Andhra Pradesh, India
[2]PG Student ,Department of MCA , St. Mary's Group Of Institutions, Guntur, Andhra Pradesh, India

ABSTRACT

This document provides some minimal guidelines (and requirements) for writing a research paper. Issues related to the contents, originality, contributions, organization, bibliographic information, and writing style are briefly covered. Evaluation criteria and due dates for the research paper are also prLocation based services allow mobile device users to access various services based on the users' current physical location information. Path-critical applications, such as supply chain verification, require a chronological ordering of location proofs. It is a significant challenge in distributed and user-centric architectures for users to prove their presence and the path of travel in a privacy-protected and secure manner. So far, proposed schemes for secure location proofs are mostly subject to tampering, not resistant to collusion attacks, do not offer preservation of the provenance, and are not flexible enough for users to prove their provenance of location proofs. In this paper, we present WORAL, a complete ready-to-deploy framework for generating and validating witness oriented asserted location provenance records. The WORAL framework is based on the Asserted Location Proof protocol [1] and the OTIT model [2] for generating secure location provenance on the mobile devices. WORAL allows user-centric, collusion resistant, tamper-evident, privacy protected, verifiable, and provenance preserving location proofs for mobile devices. The paper presents the schematic development, feasibility of usage, comparative advantage over similar protocols, and implementation of WORAL for Android device users including a Google Glass based client for enhanced usability.

Keywords: Location Assertion; Location Proof; Location Provenance; Location Security; Witness Endorsement; WORAL

I. INTRODUCTION

Cell phones have improved the utilization of location based services (LBS) utilizing the land locations of the gadgets [3]. LBS utilize area labels, for example, in informal communities, shopping coupons, movement alarms, and travel logs. Nevertheless, LBS subject to area proofs gathered by the client have even more fascinating elements and applications. An evaluator can later confirm the claim of quality as for the client's character, the area being referred to, and the time when the client was available at that area. Be that as it may, deceitful area revealing have suggestions going from insignificant cases, for example, warming in social-diversions [4], to national security issues [5].

Self-detailed area nearness utilizing Global Positioning System (GPS) facilitates, cell triangulation in cell phones, and IP address following are generally vulnerable to controlled and false area claims [6]. Constant following of clients by specialist co-ops including outsider applications abuses the clients' protection, permits traceable personalities, and makes the clients exposed against entrusted specialist organizations [7]. The specialist co-ops may likewise offer the area information of their clients exploiting the small text in the administration assertions [8]. Carriage and uncertain executions disturb the circumstance much further. Provenance of data is essential for following the genuineness of the information back to its source [9, 10]. The provenance of area is a critical necessity in path critical situations. A legitimate claim of travel way should be confirmed as far as the area provenance. The inventory network and the moderate areas, which the item goes through [11], might exceptionally advocate the trustworthiness of an item. Provenance for area is a ceaseless procedure and is required to be protected as the client goes around gathering area proofs. Dissimilar to general information things, the grouping in which the areas are made a trip should be safeguarded in sequential request inside the provenance chain. Accordingly, area provenance depicts a more noteworthy test than that for general information things [2].

There have been various recommendations for permitting client started area verification era [3, 12–15]. A confinement specialist covering the range uses some protected distance bounding component to guarantee the client's essence when the client demands for area verification [16–18]. However, existing instruments neglect agreement assaults and additionally the provenance of the area proofs. Related works hitherto host not considered third-gathering underwriting and the chronological requesting for secure area proofs together, which makes the plans defenceless against intrigue attacks and altering the request of the confirmations [3, 6, 7, 12–25].The after represents the reasonableness of a protected and asserted area provenance framework. Bob is a designer at a development organization. The company expects Bob to go to the development locales and create a day-by-day report of the venture status. Unfortunately, Bob is accused of carelessness towards his occupation when the company endured a noteworthy misfortune because of a mishap. The inspection report that Bob exhibited was disposed of for being a false record as the organization guaranteed that Bob did not visit the development site and the mishap was a consequence of his carelessness. In a substitute situation, Bob collects area provenance records as he visits each of the construction sites, which are declared by the site engineers a witness. Along these lines, Bob would then be able to demonstrate his regular visits and the request of visit to each of the locales based on the secure area provenance records. In this paper, we display the Witness Oriented Asserted Location provenance (WORAL) system. The framework is asked on the Asserted Location Proof (ALP) convention [1] and consolidates the OTIT show for secure area provenance [2]. The WORAL structure is an entire suite of creation prepared applications, including an electronic specialist organization, a desktop-based area expert server, an Android-based client application, a Google Glass-based customer, and a desktop-based evaluator.

Commitments: The commitments in the paper are as per the following:

1) We have presented a novel answer for getting user centric, witness embraced, provenance safeguarding, and secure area proofs for cell phones without the requirement of having an incorporated model.

2) We have displayed the WORAL structure usage; a total prepared to-send suite of utilizations, supporting Android based gadgets to gather and fare area proofs, including wearable fringe devices, such as Google Glass. We built up the safe convention for WORAL in light of our prior work on secure area proofs and increased the convention utilizing secure area provenance safeguarding [1, 2].

3) We have likewise exhibited a talk and a near investigation of comparative conventions and a practicability examination in light of the appropriate application ranges.

Whatever remains of the paper is sorted out as takes after. We introduce the conceivable utilizations of area confirmation instruments in Section 2. We talk about related works and their impediments in Section 3. Segment 4 presents the key phrasings and the framework and risk models. The WORAL system architecture, in view of ALP [1] and upgraded with the OTIT display [2] is introduced in Section 5. A similar and outline investigation is incorporated into Section 6. The execution of the prepared to-convey WORAL system and its segments are depicted in Section 7. Progressing research for future improvement and the conclusions are introduced in Section 8 and Section 9 individually.

II. APPLICATIONS

Statement arranged area provenance plans could be adequately utilized as a part of an assortment of genuine situations. Our answer underscores the gadget's quality, and can be a profoundly pertinent innovation for gear dealing with organizations. At present, most top of the line gadgets accompany organizing highlights and implicit memory. Thus, these costly gadgets could without much of a stretch be observed for nearness at their specific areas. The idea of area provenance and witnesses can likewise be connected to different areas, for example, in safeguarding the trustworthiness of inventory network data for various items and administrations [11].

An intriguing application can be made at associations who have voyaging clientele or workers. Explorers can gather the attested area provenance things on their cell phones. Afterward, they can use the evidences to rearrange consequent procedures, for example, travel cost cases and schedule administration, in a protected and solid design.

The entire component of declared sealing could be used in a turned around witness arranged application. Rather than a client showing the verifications as confirmation of essence, witnesses can display legally approved records as a proof of particular clients going by a specific area. Taking the case of protection operators, development site assessors, and alleviation specialists, the nearness of these individuals are

We have been introduced sure more worried in their separate fields of activity. Observers at the specific destinations can give their supports as confirmation of visit for the operators on the field.

Expanding the idea of areas and affirmed evidence of quality, informal organizations and such group-situated stages have open doors for actualizing such plans also. A protected evidence of quality with provenance safeguarding can be utilized to frame impromptu informal communities and group systems. In this way, a protected, computerized, and non-nosy area confirmation era plot fits flawlessly as the fundamental component for every single such Lb.

III. RELATED PAINTINGS

Arrange et al. presented a piece on location-based totally get right of entry to manipulate (lbac) [26], wherein, the requester, the get admission to manipulate engine, and the vicinity provider permits assessment of lbac policies for getting access to assets and services, in line with the area of the user with respect to a specific place different processes use asynchronous dimension of spherical journey instances between the person devices and get admission to points [16, 42].alas, region reporting mechanisms the use of signal attenuation can easily be manipulated by using an attacker, suffer from channel noise, and has barriers with line-of-sight. dunne et al. proposed a three-celebration structure for place based services making use of an operator-orientated trusted birthday party [34]. such centralized architectures impose a bottleneck and complexity because of the centralized mode of operation. secure and unforgivable area proofs become mentioned through waters et al. [15].

Gonzalez-tablas et al. evolved the notion of route-stamps [24] for developing a hash-chain of place proofs. manweiler et al. [25] proposed the smile protocol, in which mutual strangers can establish shared understanding and later prove that they have got met before. However, none of those works outlines the necessities for comfortable area provenance and/or is depending on specialized hardware features.

IV. MODELING THE WORAL FRAMEWORK

In this section, we gift the terminologies and the fashions for developing the oral framework for provenance keeping relaxed region proofs. On this context, we define protection as ensuring the integrity and privateers of the vicinity provenance records that has been generated at a specific location for a user.

4.1 terminologies

Terminologies in the description of our fashions and for designing the woral architecture the carrier provider sp is the depended on entity providing the secure place provenance service to mobile users, primarily based on decentralized and certified area authorities and established auditors. a person u is an entity who visits a region and uses a mobile tool to request and save place provenance information. A website s is a bodily area with a valid cope with within a finite location below the insurance of one location authority. A vicinity authority la is a stationary entity, certified by means of the sp, recognized the use of a unique identifier, and is answerable for offering place provenance information for a particular site. A witness w is a spacious-temporally collocated cellular person who has volunteered to claim a location provenance report for the presence of some other cell tool user on the given region. A witness listing we gives the listing of all registered witnesses beneath the insurance of the region authority at a given time. A crypto-identification cid is a cryptographic identification for the user (who is additionally a witness), utilized in all stages of the protocol, ensuring privacy of the entities collaborating within the method. A vicinity evidence lap is a token of proof received with the aid of a person when touring a specific web site and an asserted proof ape is an area evidence lap asserted by means of a legitimate witness the use of his crypto-identification.

4.2 Witnesses and Assertions

We utilize the equal concept to create place proofs have the evidence asserted by using a co-located witness. in this context, a witness is a spatio-temporally co-positioned entity with the user and the location authority. A witness will assert proofs most effective whilst inclined to accomplish that and may de-check in as a witness at any time. In a commercially deployed situation, the motivation of the witness may be primarily based on awarded ‘factors’ depending on legitimate assertions. The ‘factors’ could upload to the trust value of a witness and can be redeemed for club advantages from the provider issuer. The witness to prove co-vicinity with the person will also use the assertions.

4.3. Three Hazard Model

The risk model for woral is based on the formerly described entities and is described as follows:

The area records inside the asserted region proof corresponds to a particular identification of a person and an adversary must not be able to create a vicinity proof for a place that the consumer has now not visited. The time at which the unique person visited the given website online and collected the asserted vicinity proof ought to no longer be modifiable by using an attacker to create an evidence for a different (nearby) time from the real time of visit.

The identification and location privacy of customers and witnesses are protected and an attacker may not create a dossier of customers travelling a given area and analyse the place history and identities of other users.

The chronological ordering of the proofs ought to be preserved and an attacker must not be capable of alter the order of proofs in the provenance information.

The privateers of records inside a proof is uncovered in line with the preference of the user and an attacker or auditor need to no longer be able to view any personal statistics now not intended to be uncovered with the aid of the user. a person intending to reveal a subset of the area provenance information need to not be revealing greater than what's required for the favoured section of the chain.

A malicious consumer should not be capable of cover a temporary off-song motion from the claimed vicinity provenance.

A malicious user may also need to overload the auditor withal high computational requirement for the at ease place provenance verification process. Subsequent, we describe the attacker skills for our chance model primarily based at the contexts, assumptions, capability, and viable intents for every of the entities.

Device Model

We assume that cell gadgets carried by way of customers are able to communicating with other devices and lass over wife networks. The gadgets have local storage for storing the provenance gadgets. The consumer has complete get admission to the garage and computation of the device, can run a utility at the tool, and may delete, modify, or insert any content material inside the records stored on the device. The consumer, Los Angeles, and witness can access each other’s public key from the sp. the l. A. is a set server with higher computation and storage capability than a mobile device. A location runs a wife network, and the la is immediately linked to the community. Any person interested to acquire an asserted place provenance document obtains the cope with of the Los Angeles from the web site via network proclaims. In addition, a person can gain the deal with of the place authority, and check in as an involved witness. The area authority periodically updates the to be had witness listing. While required, the region authority chooses a witness from the listing at random and sends a request to the chosen witness to assert a vicinity evidence.

Communications between l. A. and mobile customers are finished over top. All messages are signed the usage of the private key of respective entities and proven the use of the public key.

Signature of an entity e for a message m is refereed as se (m). An entity can obtain the general public key of another entity from the sp. all communications with the spa occur thru the public community using relaxation [51] and https.

The different steps and levels of the protocol had been designed, such that, to ensure the vicinity evidence is proof against collusion assaults and the provenance of the place proofs is preserved. consequently, we designed woral based at the secure vicinity proof series scheme supplied in [1] and is enhanced the usage of cozy location provenance schemes offered in [2]. inside the following subsections, we gift the exceptional additives and paintings flows of the framework.

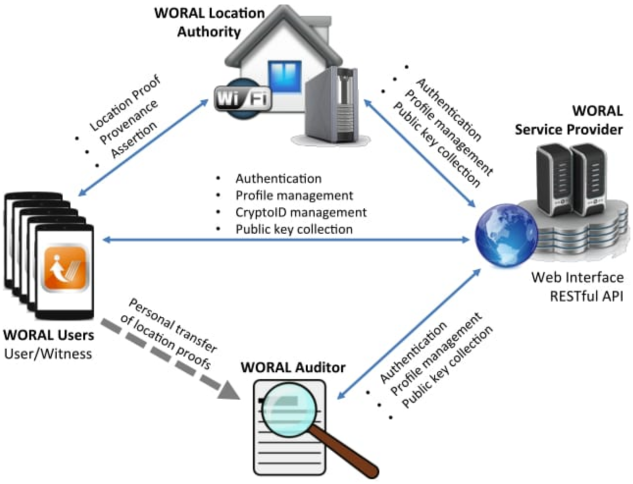

Figure 1: assessment of woral paintings go with the flow may be created and stored for the crypto-id at the mobile device. the person/witness desires to upload the public key similar to the sp, in an effort to be diagnosed via the crypto-identification. later, a request for the public key of consumer/witness for a selected crypto-id will be served by using the sp.

Location Authority Discovery

The client and witness require the IP deliver of the LA to build up a TCP association with the LA. They likewise require the remarkable area ID to get to open key of the LA. The IP and identifier are made accessible to the client and witness through the LA revelation convention utilizing communicates messages. When a client or witness needs the LA's data, it broadcasts a UDP bundle to a particular port asking for the data of LA. The LA dependably tunes in for new UDPbroadcast bundles. In the event that the parcel matches with some certain criteria (for our situation, ask for LA's data), the LA sends a UDP bundle as a reaction that contains its location ID. In the wake of accepting the reaction sent by the Lathe, client/witness can extricate the character and IP address of the LA from the got UDP bundle.

V. Witness Registration

The LA needs to keep up a rundown of accessible co-found WORAL portable clients who are intrigued to fill in as witnesses. The enrolment procedure is appeared in Figure 2. AWORAL versatile client express his readiness to fill in as an observer by sending a witness enrolment message WReg

to the LA and is characterized as:

WReg =< CIDW; tW; SW(CIDW; tW) > (1)

where CIDW is the Crypto-ID of the witness and tW, is the timestamp from the witness' cell phone.

In the wake of getting WReg from the witness, the LA includes the witness data (CIDW and witness' IP address) to the accessible witness list (WL) and sends an affirmation message RegAck to the witness.

RegAck =< R; tL; SL(R; tL) > (2)

Here, R 2 [YES, NO], and tL is the timestamp of LA.

The arrangement of cooperation among the elements for making an affirmed area confirmation with provenance protection is delineated in Figure 3 and depicted as takes after:

a) Location confirmation ask for: The client gets the identity of the LA and sends an area verification ask for PReq to theLA, as appeared in Expression 3.

pReq =< CIDU; tU; PS; LProvcur; SL(CIDU; tU; PS; LProvcur) >(3)

Here, in Expression 3, CIDU is the Crypto-ID of the client U spoke to by people in general key [3], or by anonym zed identifiers [14], tU is the timestamp from the client's cell phone, PS is the provenance conspire chose by the client, and LProvcur is the present leader of the area provenance chain. Recovering the present leader of the provenance chain does not rely upon the chose provenance plot.

b) Location confirmation era: The LA produces the area confirmation LP as appeared in Expression 4 and sends

the LP to the client.
LP =< CIDU; L; tL; LProvnew;
SL(CIDU; L; tL; LProvnew) >
WORAL Users

The WORAL Android client application is utilized for both requesting area proofs and to assert other users ‘location proofs as a witness. The home screen after the user logs in is represented in Figure 8a. The home screen allows the client to choose a crypto-ID for the present area proof request or produce new crypto-ID keys, and refresh/modify the settings. The settings screen for the client application is appeared in

Figure binds the settings mode enables the client to choose the background witness benefit highlights, and in addition the external communication include for wearable fringe gadgets. The settings are consequently matched up with the administration provider. The rundown of at present gathered confirmations can be seen as shown in Figure 8c. In addition, the client can selectively or largely fare or erase the verifications. The exported proofs have the coveted level of granularity of data

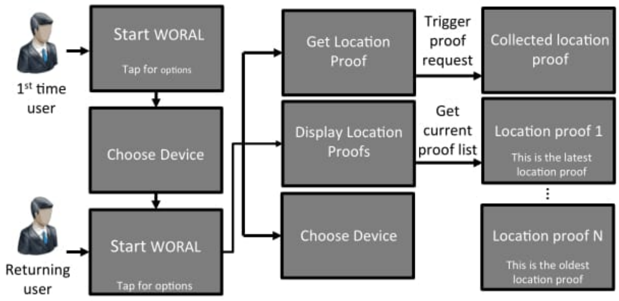

Figure 2 : Plug-n-Play Location Authorities utilizing Raspberry Pi-s

(a) Home Screen (b) Settings
(c) Proof List (d) Export Proofs

Fig2 Android User Application as chose by the clients and is appeared in Figure. The exported proofs are spared as a content record on the portable device, which would then be able to be sent by and by to the examiner by the user (e.g. email, record exchange). We have tried our application onLG Nexus 4, Samsung Galaxy Nexus, Samsung Galaxy S4,Motorola XT875, HTC 1X, HTC Evo 4G, and MotorolaMoto G telephones with Android adaptation 2.3 and higher.

WORAL Wearable Device Extension

Wearable fringe gadgets, for example, the Google Glass3,are omnipresent gadgets with systems administration capacity. Suchdevices permit consistent cooperation and protection of displayfor the clients. We broadened our WORAL structure byimplementing a Google Glass based interface for theWORAL Android client application. The wearable gadget augmentation

VI. CONCLUSION

In this paper, we present WORAL, a prepared to-convey structure for secure, witness-arranged, and provenance safeguarding area proofs. WORAL permits creating secure and alter obvious area provenance things from a given area specialist, which have been declared by a spatio-transiently co-found witness. WORAL depends on the Asserted Location Proof convention [1], and is upgraded with provenance safeguarding in view of the OTIT display [2]. The WORAL system highlights an electronic specialist organization, desktop-based area expert server, an Android-based client application including a Google Glass customer for the portable application, and a reviewer application for provenance approval.

VII. REFERENCES

[1]. R. Khan, S. Zawood, M. Haque, and R. Hasan, "Who, When, and Where? Location Proof Assertion for Mobile Devices," in Proc. of DBSec. IFIP, July 2014.

[2]. R. Khan, S. Zawood, M. Haque, and R. Hasan, "OTIT: Towards secure provenance modeling for location proofs," in Proc. of ASIACCS. ACM, 2014.

[3]. S. Saroiu and A. Wolman, "Enabling new mobile applications with location proofs," in Proc. of HotMobile, 2009, pp. 1–6.

[4]. J. VanGrove, "Foursquare cracks down on cheaters." Online at http://mashable.com/2010/04/07/foursquare-cheaters/, April 2010.

[5]. I. Maduako, "Wanna hack a drone? possible with geo-location spoofing!" Online at http://geoawesomeness.com/?p=893, July 2012.

[6]. N. O. Tippenhauer, K. B. Rasmussen, C. Popper, and S. Capkun, "iPhone and iPod location spoofing: Attacks on public WLAN-based positioning systems," SysSec Tech. Rep., ETH Zurich, April, 2008.

[7]. A. J. Blumberg and P. Eckersley, "On locational privacy, and how to avoid losing it forever," Online at https://www.eff.org/wp/locational-privacy, August 2009.

[8]. J. McDermott, "Foursquare selling its location data through ad targeting firm turn," Online at http://adage.com/article/digital/foursquare-selling-data-ad-targeting-firm-turn/243398/, July 2013.

[9]. Y. L. Simmhan, B. Plale, and D. Gannon, "A survey of data provenance in e-science," SIGMOD Rec., vol. 34, no. 3, pp. 31–36, September 2005.

[10]. R. Hasan, R. Sion, and M. Winslett, "The case of the fake Picasso:Preventing history forgery with secure provenance," in Proc. of FAST.USENIX Association, 2009, pp. 1–12.

[11]. R. Khan, M. Haque, and R. Hasan, "A secure location proof generation scheme for supply chain integrity preservation," in Proc. of HST. MA, USA: IEEE, 2013, pp. 446–450. IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTING 13

[12]. B. Davis, H. Chen, and M. Franklin, "Privacy-preserving alibisystems," in Proc. of ASIACCS. ACM, 2012, pp. 34–35.

[13]. P. Gilbert, L. P. Cox, J. Jung, and D. Wetherall, "Toward trustworthy mobile sensing," in Proc. of HotMobile. ACM, 2010, pp. 31–36.

[14]. W. Luo and U. Hengartner, "Proving your location without giving up your privacy," in Proc. of HotMobile, 2010, pp. 7–12.

[15]. B. R. Waters and E. W. Felten, "Secure, private proofs of location," Technical report TR-667-03, Princeton University, January 2003.

[16]. S. Brands and D. Chaum, "Distance-bounding protocols," in Proc. of EUROCRYPT. Springer-Verlag New York, Inc., 1994, pp. 344–359.

[17]. J. T. Chiang, J. J. Haas, and Y.-C. Hu, "Secure and precise location verification using distance bounding and simultaneous multilateration," in Proc. of WiSec. ACM, 2009, pp. 181–192.

[18]. K. B. Rasmussen and S. Cˇ apkun, "Realization of RF distance bounding," in Proc. of USENIX Security. USENIX Association, Aug 2010.

[19]. A. Narayanan, N. Thiagarajan, M. Lakhani, M. Hamburg, and D. Boneh, "Location privacy via private proximity testing," in Proc. of NDSS, Feb 2011.

[20]. P. Traynor, J. Schiffman, T. La Porta, P. McDaniel, and A. Ghosh, "Constructing secure localization systems with adjustable granularity using commodity hardware," in Proc. of GLOBECOM, Dec 2010.

[21]. J. Brassil, R. Netravali, S. Haber, P. Manadhata, and P. Rao, "Authenticating a mobile device's location using voice signatures," in Proc. of WiMob. IEEE, Oct 2012, pp. 458 –465.

[22]. G. Ananthanarayanan, M. Haridasan, I. Mohomed, D. Terry, and C. A. Thekkath, "StarTrack: a framework for enabling track-based applications," in Proc. of MobiSys, Jun 2009, pp. 207–220.

[23]. A. Zugenmaier, M. Kreutzer, and M. Kabatnik, "Enhancing applications with approved location stamps," in Proc. of Intelligent Network Workshop. IEEE, 2001, p. 140.

[24]. A. I. Gonz´alez-Tablas, B. Ramos, and A. Ribagorda, "Path-stamps: A proposal for enhancing security of location tracking applications," in Proc. of Ubiquitous Mobile Information and Collaboration Systems Workshop. Citeseer, 2003.

[25]. J. Manweiler, R. Scudellari, and L. P. Cox, "SMILE: encounter-based trust for mobile social services," in Proc. of CCS. ACM, Nov 2009, pp. 246–255.

[26]. C. A. Ardagna, M. Cremonini, E. Damiani, S. D. C. di Vimercati, and P. Samarati, "Supporting location-based conditions in access control policies," in Proc. of ASIACCS. ACM, 2006, pp. 212–222.

[27]. K. El Defrawy and G. Tsudik, "Alarm: Anonymous locationaided routing in suspicious manets," IEEE Transactions on Mobile Computing, vol. 10, no. 9, pp. 1345–1358, Sept 2011.

[28]. K. El Defrawy and G. Tsudik, "Privacy-preserving location-based on-demand routing in MANETs," IEEE Journal on Selected Areas in Communications, vol. 29, no. 10, pp. 1926–1934, Dec 2011.

[29]. P. Enge and P. Misra, "Special issue on global positioning system," Proc. of the IEEE, vol. 87, no. 1, pp. 3 –15, jan. 1999.

[30]. E. Gabber and A. Wool, "How to prove where you are: tracking the location of customer equipment," in Proc. of CCS. ACM, 1998, pp. 142–149.

[31]. D. E. Denning and P. F. MacDoran, "Location-based authentication: Grounding cyberspace for better security," Computer Fraud & Security, vol. 1996, no. 2, pp. 12–16, 1996.

[32]. K. Bauer, D. McCoy, E. Anderson, M. Breitenbach, G. Grudic, D. Grunwald, and D. Sicker, "The directional attack on wireless localization: how to spoof your location with a tin can," in Proc. of GLOBECOM. IEEE Press, 2009, pp. 4125–4130.

[33]. C. A. Ardagna, M. Cremonini, E. Damiani, S. D. C. di Vimercati, and P. Samarati, "Location privacy protection through obfuscation-based techniques," in Proc. of DBSec. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 47–60.

[34]. C. R. Dunne, T. Candebat, and D. Gray, "A three-party architecture and protocol that supports users with multiple identities for use with location based services," in Proc. of ICPS. ACM, Jul 2008, pp. 1–10.

[35]. M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," in Proc. of MobiSys. ACM, May 2003, pp. 31–42.

[36]. S. Capkun and J. Hubaux, "Secure positioning of wireless devices with application to sensor networks," in Proc. of INFOCOM, vol. 3. IEEE, Mar 2005, pp. 1917–1928.

[37]. N. Sastry, U. Shankar, and D. Wagner, "Secure verification of location claims," in Proc. of WiSe. ACM, Sep 2003, pp. 1–10.

[38]. S. Capkun, M. Cagalj, G. Karame, and N. Tippenhauer, "Integrity regions: Authentication through presence in wireless networks," IEEE Transactions on Mobile Computing, vol. 9, no. 11, pp. 1608–1621, Nov 2010.

[39]. Aruba Networks, Inc., "Dedicated air monitors? you decide." Online at http://www.arubanetworks.com/technology/tech-briefs/dedicated-air-monitors/, 2006.

[40]. S. Pandey, F. Anjum, B. Kim, and P. Agrawal, "A low-cost robust localization scheme for wlan," in Proc. of WICON. ACM, Aug 2006, p. 17.

[41]. P. Tao, A. Rudys, A. Ladd, and D. Wallach, "Wireless lan locationsensing for security applications," Computing Reviews, vol. 45, no. 8, pp. 489–490, 2004.

[42]. M. Youssef, A. Youssef, C. Rieger, U. Shankar, and A. Agrawala, "Pinpoint: An asynchronous time-based location determination system," in Proc of MobiSys. ACM, Jun 2006, pp. 165–176.

[43]. V. Lenders, E. Koukoumidis, P. Zhang, and M. Martonosi, "Locationbased trust for mobile user-generated content: applications, challenges and implementations," in Proc. of HotMobile. ACM, Feb 2008, pp. 60–64.

[44]. S. Saroiu and A. Wolman, "I am a sensor, and i approve this message," in Proc. of HotMobile, 2010, pp. 37–42.

[45]. Z. Zhu and G. Cao, "Toward privacy preserving and collusion resistance in a location proof updating system," IEEE Transactions on Mobile Computing, vol. 12, no. 1, pp. 51–64, 2013.

[46]. X. Wang, J. Zhu, A. Pande, A. Raghuramu, P. Mohapatra, T. Abdelzaher,and R. Ganti, "STAMP: Ad Hoc Spatial-Temporal Provenance Assurance for Mobile Users," in Proc. of ICNP, Gottingen, Germany, Oct 2013.

[47]. K. Muniswamy-Reddy, D. Holland, U. Braun, and M. Seltzer, "Provenance-aware storage systems," in Proc. of USENIX ATC. USENIX Association, May 2006, pp.