Volume 5, Issue 3, March 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Decentralised Security System Using Biometric

Prof. Leena Raut, Ajinkya Kewal, Shivprasad Dhumal
Siddhant Collage of Eng. BE Comp Department
Sudumbare, Pune, Maharashtra, India

Abstract—thesurgingdeploymentof Wi-Fi hotspots in public Places drives the blossoming oflocation-based services (LBSs) Available. A recent measurement reveals that a large portionof the reported locations are either forged or superfluous,which calls attention to location authentication. However, existingauthentication approaches breach user's location privacy, whichis of wide concern of both individuals and governments. Inthis paper, we propose PriLA, a privacy-preserving locationauthentication protocol that facilitates location authenticationwithout compromising user's location privacy in Wi-Fi networks.PriLA exploits physical layer information, namely carrier frequency offset (CFO) and multipath profile, from user's frames.In particular, PriLA leverages CFO to secure wireless transmission between the mobile user and the access point (AP), andmeanwhile authenticate the reported locations without leakingthe exact location information based on the coarse-grainedlocation proximity being extracted from user'multipath profile.

Existing privacy preservation techniques on upper layers can be Applied on top of PriLA to enable various applications. We haveImplementedPriLAon GNU Radio/ USRP platform and off the Shelf Intel 5300 NIC. The experimental results demonstrate thePracticality of CFO injection and accuracy of multipath profile Based location authentication in a real-world environment.

Index Terms—Wi-Fifingerprint-based localization; location privacy; data privacy; holomorphic encryption.

I. INTRODUCTION

Driven by the proliferation of Wi-Fi___33 hotspots in public Places, location-based services (LBS) have experienced surging development in recent years. A basic LBS model consistsof an LBS provider who offers services based on users'physical locations via trusted Access Points(APs), and mobileusers who request specific service along with their own location and identity information. Unfortunately, the measurementstudy from [1] uncovers a truth that there exists a largeamount of forged location data uploaded by mobile users. Onereason behind this phenomenon is that mobile users can abuseservices by lying about their actual positions. One seriousconsequence is resource misallocation, which can be witnessedin the TV white spaces [2], [3] scenario, where malicious userscan gain extra channel access from a spectrum service providerby pretending to be other authenticated users. Several ongoingresearches [4], [5] seek for efficient solutions to authenticatethe knowledge of locations reported by mobile users.

However, while prior works succeed to tackle the locationauthentication problem, they compromise the privacy of mobile users. Sensitive information such as individual's locationshould be protected against leakage. Mobile users have optionsnot to disclose their true locations to the LBS provider. Unfortunately, users' location privacy remains prone to be leakeddue to the broadcast nature of wireless medium, typically inWi-Fi networks. The adversary can easily infer the targeteduser's physical location by collaboratively sniffing frames overthe air from serial untrusted APs. Previous research [6] showsthat only a few APs can determine a node within meter levelresolution based on received signal strength (RSS) of a mobileuser.

To address the situation privacy issue in wireless environments, many approaches area unitplanned. K-anonymity [7] [8], one most generally adopted theme, tries to fuzz the situation resolution by activity a mobile user from an explicitvarytogether with k-1 different mobile users. However, considering the light-weight setup in WLANreadying sites, they're confronted with the challenge of lacking the sure third party whose job is to relay the communication between the mobile users and also the LBS supplier. Another line of connected work like [9], [10] target at protective mobile users' location privacy while notthe assistance of the third party. However, all the work mentioned higher thansolely argue the privacy issue from the mobile users' facet, whereas not considering the authentication downside from the point of view of the LBS supplier.

Existing location privacy conserving approaches cannot apply to location authentication in wireless environments, since concealing mobile users' locations wouldn'tenable the LBS supplier to certify them. Only 1 existing work [11] proposes how to certify location primarily based services without compromising users' location privacy. in contrast tothe problemmentioned in LAN networks, this work concentrates on facilitating mobile users to verify question results from the LBS supplier, that flips the item (mobile users in our case) to be attestedaround. From k candidates is in one specific spot. Sadly, the frame header together withmackintosh address, is visible to anyone by a default setting in LAN networks, therefore, it'sintelligiblydifficult to inscribeeach frame header destined to the LBS supplier. We have a tendency to observe that the carrier frequency offset (CFO), inherent property caused by generator instability of the transceiver, may be exploited to inscribethe full frame.

Each mobile user combating privacy leak, ought to inject an exactCFO into every frame before causing it. Since the CFO is personalinfoillustrioussolely to communication try, solelythe supposed receiver (LBS provider) willdecipher the frame, whereas others capture the all corrupted frame. To wear down the authentication issue, we have a tendency toconjointly observe that multipath profile is said to the situationhowevercan't bewont to localize a mobile user directly because itsolely offers relative location proximity. Additionally, the multipath profiles is difficult to forge because itis decided by Associate in nursing environment's physical layout. No mobile users have to be compelled to report own location to the LBS supplierto any extent further. Instead, the LBS supplierwillcertifythe situation with coarse-grain resolution through distinguishingthe multipath profile for every mobile user.

Our contributions during this paper arq summarized as follows. First, we have a tendency to propose PriLA, a privacy-preserving location authentication protocol in Wi-Fi___33 networks. Second, not like past works, thatcontemplate frequency offset and multipath as harmful, our style leverages these 2items of fine-grained physical info to at the same time address location privacy and authentication problems. Finally, we have a tendency to implement PriLA on GNU Radio/USRP testbed and off-the-peg Intel 5300 NIC to demonstrate its practicability. The remainder of the paper is organized as follows. Section II describes the system model. In Section III, we have a tendency to1stprovidean outline of the protocol framework then detail the complete system style, together with the corporate executiveencodingand therefore the multi- path profile based mostly location authentication.

II. LITERATURE SURVEY

[1] H. Liu, Y. Gan, J. Yang, S. Sidhom, Y. Wang, Y. Chen, and F. Ye, "Push the limit of Wi-Fi based localization for smartphones," in this paper they Now that billions of people carry sensor-enabled mobile devices (e.g., smartphones), employing powerful capability of such commercial mobile products has become a promising approach for large-scale environmental andhuman-behavioural sensing. Such a new paradigm of scalable context monitoring is known asopportunistic sensingand has been successfully applied to a broad range of applications. In this paper, we briefly introduce basic architectureand building blocks on which these emerging systems are based, and then provide a survey of recent progress in theopportunistic sensing technology.

[2] W. Cheng, D. Wu, X. Cheng, and D. Chen, "Routing for information leakage reduction in multi-channel multi-hop ad-hoc social networks," in this paper they proposed.

Communication scheduling in duty-cycled multi-hop wireless sensor networks. Assume that time is divided into time-slots and we group multiple consecutive time-slots into periods. Each node can transmit data at any time-slot while it only wakes up at its active time-slot of every period and thus be allowed to receive data. Under the protocol interference model, we investigate four group communication patterns, *i.e.*, broadcast, data aggregation, data gathering, and gossiping. For each pattern, we develop a delay efficient scheduling algorithm which greatly improve the current state-of-the-art algorithm. Additionally, we propose a novel and efficient design to coherently couple the wireless interference requirement and duty cycle requirement.

[3] R. Shokri, G. Theodorakopoulos, J. Le Boudec, and J. Hubaux, "Quantifying location privacy", in this project they proposed It is a well-known fact that the progress of personal communication devices leads to serious concerns about privacy in general, and location privacy in particular. As a response to these issues, a number of Location-Privacy Protection Mechanisms (LPPMs) have been proposed during the last decade. However, their assessment and comparison remains problematic because of the absence of a systematic method to quantify them. In particular, the assumptions about the attacker's model tend to be incomplete, with the risk of a possibly wrong estimation of the users' location privacy. In this paper, we address these issues by providing a formal framework for the analysis of LPPMs, it captures, in particular, the prior information that might be available to the attacker, and various attacks that he can perform. The privacy of users and the success of the adversary in his location-inference attacks are two sides of the same coin. We revise location privacy by giving a simple, yet comprehensive, model to formulate all types of location-information disclosure attacks. Thus, by formalizing the adversary's performance, we propose and justify the right metric to quantify location privacy. We clarify the difference between three aspects of the adversary's inference attacks, namely their accuracy, certainty, and correctness. We show that correctness determines the privacy of users. In other words, the expected estimation error of the adversary is the metric of users' location privacy. We rely on well-established statistical methods to formalize and implement the attacks in a tool: the Location-Privacy Meter that measures the location privacy of mobile users, given various LPPMs. In addition to evaluating some example LPPMs, by using our tool, we assess the appropriateness of some popular metrics for location privacy: entropy and k-anonymity. The results show a lack of satisfactory correlation between these two metrics and the success of the adversary in inferring the users' actual- - locations...

[4] D. Yang, X. Fang, and G. Xue, "Truthful incentive mechanisms for anonymity location privacy," in this project they are proposed tremendous efforts have been made to protect thelocation privacy of mobile users. Some of them, e.g.,k-anonymity,require the participation of multiple mobile users to impedethe adversary from tracing. These participating mobile usersconstitute an anonymity set. However, not all mobile users areseriously concerned about their location privacy. Therefore, toachievek-anonymity, we need to provide incentives for mobileusers to participate in the anonymity set. In this paper, westudy the problem of incentive mechanism design fork–anonymitylocation privacy. We first consider the case where all mobileusers have the same privacy degree requirement. We thenstudy the case where the requirements are different. Finally,we consider a more challenging case where mobile users cancheat about not only their valuations but also their requirements.We design an auction-based incentive mechanism for each ofthese cases and prove that all the auctions are computationalefficient, individually rational, budget-balanced, and truthful. Weevaluate the performance of different auctions through extensivesimulations.

III. PROPOSED APPROACH FRAMEWORK AND DESIGN

[1] Problem Definition:

Privacy policies are defined in compliance with the existing privacy regulations. In simplest form, privacy policies are encoded in natural language and are directly enforced by users. Manual enforcement is however expensive and thus policiesare often ignored by users. This problem is particularly relevant when users visit websites

[2]System Architecture

Fig. one depicts the system design of location authentication that consists of associate degree LBS supplier, mobile users, and adversaries. In a very location authentication system, a mobile user requests service from the LBS supplier by coverage the user's location info with identity to the sureAP that connects to the LBS servers via secured backhaul. As assumed in several existing location privacy preservation proposals, the mobile user solely reports coarse location info to preserve privacy. Supportedaccording identity and placementinfo, the LBS supplier checks the honesties of the situationinfo. Only if the accordinginfo is confirmed to be truth, the LBS supplier delivers the service to the mobile user via downlink transmission from the sure AP. Here, we tend totake into account.

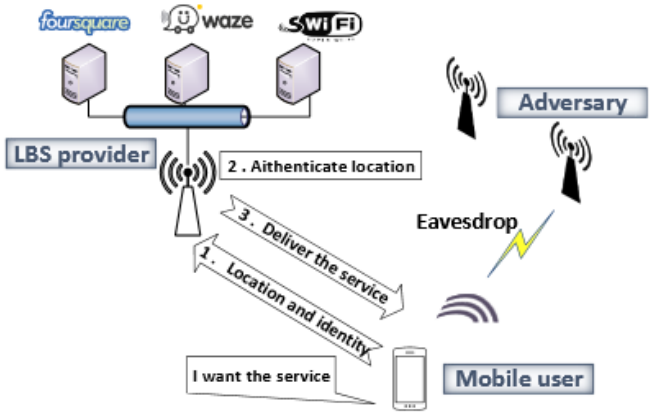


Fig. 1. System architecture of location-based service in WiFi networks

The antagonistis taken into account as auditor in wireless fidelity networks UN agency tries to reap the locations of mobile users and trade them for profit. The antagonistwill intercept all frames over the air in wireless fidelity networks, and take a look atto getthe situation and identity information (e.g., Mack address) by decryption the frames. Moreover, the antagonistmight deploy multiple eavesdroppers and shallfind the mobile user using existing localization techniques. To do this, the antagonistinitial identifies the mobile user's frame, and so use signal strength or angle of arrival data of the frame obtained at multiple eavesdroppers to localize the mobile user.

[3] Mathematical Model:

CFO in Wi-Fi Networks.

$$\triangle f = fc_{TX} - fc_{RX}$$

Where x (t) denotes the transmitted signal, r (t) denoted the received signal, 4fis the carrier frequency offset, and Fs is the sampling frequency.

$$r(t) = A(t)e^{j\theta(t)} * e^{\frac{j2\pi\triangle ft}{F_s}} = A(t) * e^{j(\theta(t)+\frac{2\pi\triangle ft}{F_s})}$$

Where a (t) and (t) are the magnitude and phase component of the received signal respectively.

$$B(\theta) = \mid \sum_{k=0}^{K-1} w(k,\theta) * r_k \mid^2$$

$$w(k,\theta) = e^{-j2\pi kD\cos\theta}$$

Wherew (k, 0) is the complex weight that helps to compensate the signal phase difference between the first andkthantenna.

[4]Work Done

In this section we are discussing the practical environment, scenarios, performance metrics used etc.

4.1 Input

In this user signature is the input for our practical experiment.

4.2 Hardware and Software Configuration

Hardware Requirements:

Processor : Pentium IV 2.6 GHz

Ram : 512 MB DD RAM

Monitor : 15" COLOR
Hard Disk : 20 GB
Software Requirements:
Front End : Java
Tools Used : Net Beans
Operating System : Windows 7/8
Database : MySQL
Cloud server : Amazon.com, somee.com

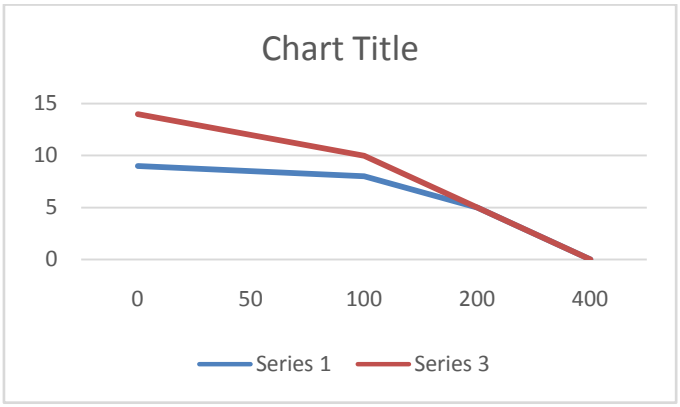
4.3 Results

It is evident that the proposed RSA based scheme communication cost of DPRP scheme is more when compared with the proposed RSA based scheme.

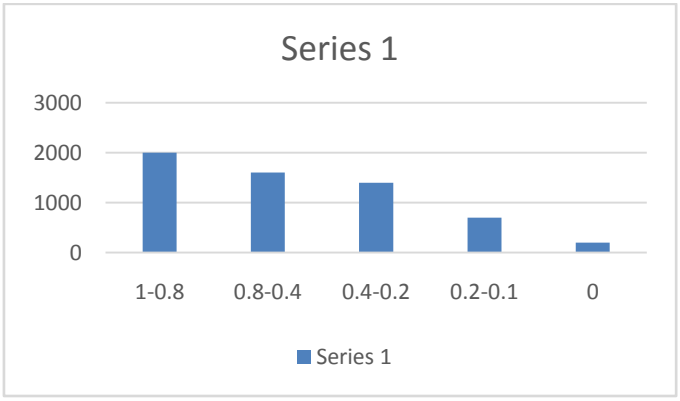
The result of whole data temporal probability

[5] Expected Results

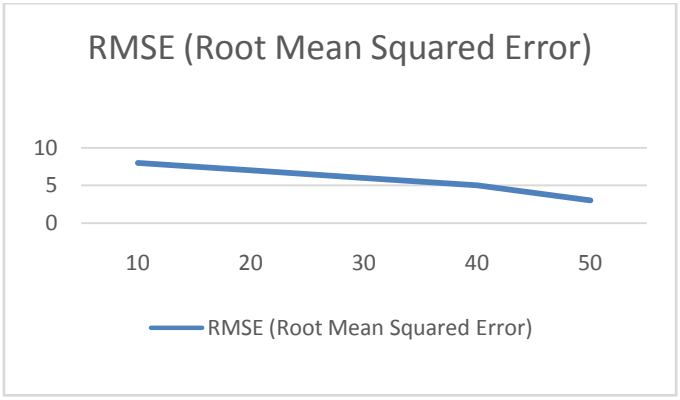
The comparison of experimental data and the model



The result of whole data temporal probability



Probabilistic Matrix Factorization



IV. CONCLUSION

We propose PriLA, a completely unique privacy conserving location authentication protocol in local area network networks. PriLAleverages these 2items of fine-grained physical data to at the same time address location privacy and authentication problems. Specifically, PriLA leverages inherent CFOdatato secure the transmission in physical layer, and

exploits multipath profile to facilitate location authentication while not compromising user's location privacy. We analyze the privacy problems withlocal area network fingerprint-based localization. To thwart the privacy threats, we tend to propose a completely unique Privacy-Preserving local area network Fingerprint Localization theme (PriLA) that utilizes holomorphiccodingto safeguardeach the client's location privacy and therefore the localization service provider's knowledge privacy. What is more, we tend tostylean enclosedquality prediction algorithmic ruleto scale back the machine overhead at the shopperaspect. Togauge this algorithmic rule, we tend to performed the analysis experiment supported the information of Locky.jp .Atlastweknew that this algorithmic rule reduced the privacy invasion to concerning2 hundredth. In future, we'll apply this algorithmic rule to large-scale knowledge. What is more, so asto replyto numerousthings, assaultive experiments also arethought of. Finally, we tend to hope it will beutilized inobserve

REFERENCES

[1] Alia Asheralieva, Kaushik Mahata, "Joint power and bandwidth allocation in IEEE802.22 based cognitive LTE network", Computer Networks 71 (2014) 117–129.

[2] M. Buddhikot, P. Kolodzy, S. Miller, K. Ryan, and J. Evans, "Dimsumnet: new directions in wireless networking using coordinated dynamic spectrum," *Sixth IEEE International Symposium on World of Wireless Mobile and Multimedia Networks (WoWMoM)*, pp. 78–85, June 2005.

[3] Federal Communications Commission (FCC), "Notice of proposed rule making", ET Docket no. 04-113, May 2004.

[4] J. Mitola and G. M. Jr., "Cognitive radio: making software radios more personal," *IEEE Personal Communications*, vol. 6, no. 4, pp. 13–18, Aug. 1999.

[5] "IEEE 802.22 Working Group on Wireless Regional Area Networks." [Online]. Available: http://www.ieee802.org/22/

[6] "IEEE P802.22 draft standard for Wireless Regional Area Networks Part 22: Cognitive Wireless RAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Policies and procedures for operation in the TV bands," 2006.

[7] Federal Communications Commission (FCC), "In the matter of unlicensed operation in the TV broadcast bands," Second Report and Order and Memorandum Opinion and Order, no. FCC-08-260A1, Nov. 2008.

[8] A. Attar, S. A. Ghorashi, M. Sooriyabandara, and A. H. Aghvami, "Challenges of real-time secondary usage of spectrum," *Computer Networks*, vol. 52, no. 4, pp. 816–830, 2008.

[9] H. Liu and S. Li, "Research on the mechanism of wran self-coexistence," *International Symposium on Electromagnetic Compatibility, EMC*, pp. 67–70, 2007.

[10] S. Sengupta, S. Brahma, M. Chatterjee, and S. Shankar, "Enhancements to cognitive radio based ieee 802.22 air-interface," *IEEE International Conference on Communications (ICC)*, pp. 5155–5160, 2007.

[11] G. Ganesan and Y. Li, "Cooperative spectrum sensing in cognitive radio networks, part i: Two user networks and part ii:Multiuser networks," *IEEE Transactions on Wireless Communications*, vol. 6, no. 6, pp. 2204–2222, June 2007.

[12] A. Ghasemi and E. S. Sousa, "Spectrum sensing in cognitive radio networks: the cooperation-processing tradeoff," *Wireless Communications and Mobile Computing*, vol. 7, no. 9, pp. 1049–1060, 2007.

[13] X. Liu and N. Sai-Shankar, "Sensing-based opportunistic channel access," *Mobile Networks and Applications*, vol. 11, no. 4, pp. 577–591, 2006.

[14] A. Sahai, N. Hoven, and R. Tandra, "Some fundamental limits on cognitive radio," *Forty-second Allerton Conference on Communication, Control and Computing*, Oct. 2004.

[15] N. Han, S. Shon, J. Chung, and J. Kim, "Spectral correlation based signal detection method for spectrum sensing in IEEE 802.22 WRAN systems," *8th Intl. Conference on Advanced Communication Technology (ICACT)*, vol. 3, pp. 1–6, 2006.

[16] H.-S. Chen, W. Gao, and D. Daut, "Signature based spectrum sensing algorithms for IEEE 802.22 wran," *IEEE International Conference on Communications (ICC)*, pp. 6487–6492, June 2007.

[17] N. Kundargi and A. Tewfik, "Sequential pilot sensing of atsc signals in ieee 802.22 cognitive radio networks," *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 2789–2792, 2008.

[18] W. Hu, D. Willkomm, M. Abusubaih, J. Gross, G. Vlantis, M. Gerla, and A. Wolisz, "Cognitive radios for dynamic spectrum access - dynamic frequency hopping communities for efficient IEEE 802.22 operation," *IEEE Communications. Magazine, vol. 45, no. 5, pp. 80–87, May 2007.*

[19] X. Gelabert, I. F. Akyildiz, O. Sallent, and R. Agust´ı, "Operating point selection for primary and secondary users in cognitive radio networks," Computer Networks, vol. 53, no. 8, pp. 1158–1170, 2009.

[20] S. Khanna and K. Kumaran, "On wireless spectrum estimation and generalized graph coloring," *IEEE INFOCOM*, vol. 3,pp. 1273–1283 vol.3, Mar-2 Apr 1998.

[21] A. Koster, "Frequency assignment: Models and algorithms," Ph.D. dissertation, Universiteit Maastricht, Maastricht, TheNetherlands, 1999.

[22] L. narayanan, "Channel assignment and graph multicoloring," *Handbook of wireless networks and mobile computing*, pp.71–94, 2002.

[23] A. Safwat, "Distributed connection admission control and dynamic channel allocation in ad hoc-cellular networks,"*International Conference on Digital Telecommunications (ICDT)*, pp. 52–52, Aug. 2006.

[24] A. Mishra, S. Banerjee, and W. Arbaugh, "Weighted coloring based channel assignment for WLANs", *SIGMOBILE MobileComputer Communication Rev.*, pp. 19–31, 2005.

[25] S. Avalallone, I. Akyldiz, "A channel assignment algorithm for multi-radio wireless mesh networks", *Computer Communications*,pp. 1343–1353, 2008.

[26] W. Wang and X. Liu, "Dynamic channel sharing in open-spectrum wireless networks," *IEEE VTC Fall 2005*, Sep. 2005.

[27] J. Tang, S. Misra, and G. Xue, "Joint spectrum allocation and scheduling for fair spectrum sharing in cognitive radiowireless networks," *Computer Networks*, vol. 52, no. 11, pp. 2148–2158, 2008.

