M

Mix-Zones in Wireless Mobile Networks

Panos Papadimitratos
Networked Systems Security group, KTH Royal Institute of Technology, Kista, Stockholm, Sweden

Definition

Part, corresponding to a physical region, of a wireless mobile network (along with related functionality), within which location information is concealed. The objective is to enhance user location privacy, making it hard to link user (or the user's mobile computing device) actions over time and across space.

Background

The mix-zone concept was first proposed in Beresford and Stajano (2003) and then refined in Beresford and Stajano (2004), considering user location privacy in emerging, at the time of the aforementioned publications, wireless mobile networks towards, eventually, pervasive connectivity and network access. The idea of a mix-zone for location-aware or location-based services and applications is analogous to the notion of a mix-node in an anonymous communication system (Chaum 1988). Simply put, mix-zones allow mixing identities of mobile nodes, temporarily unobservable, thus enhancing the unlinkability of their actions. Mix-zones have been revisited, discussed as relevant, and further investigated in a multitude of settings associated with mobile computing use cases over the years. A well-received and broadly considered concept in the research literature, it remaines, to this date, in the research realm.

Theory and Applications

Nomadic wireless connectivity, thanks to Wi-Fi and cellular data communication (third generation (3G) or fourth generation (4G)), along with mobile computing platforms with Global Navigation Satellite System (GNSS) receivers or other positioning technologies, paved the way for a multitude of location-aware or location-based services and applications. Extensive, over time and possibly across large spaces, and often fine-grained position information can be invaluable to users (e.g., to obtain precise location-relevant data) and network operators (e.g., to optimize functionality). In contrast, such position data can unwillingly reveal to an observer sensitive user information, or allow inferring it based on collected messages (revealing locations, identities, and other user- and application-specific data). This concern motivated a large body of work on preserving or enhancing *location privacy*. A wide gamut of mechanisms designed by the research community, with subsets of those adopted in

S. Jajodia et al. (eds.), *Encyclopedia of Cryptography, Security and Privacy*,
https://doi.org/10.1007/978-3-642-27739-9_1534-2

standards or incorporated in products, address this problem: eliminating or reducing the knowledge of a user's (his/her device's) position, past, current, or future.

The notion of *mix-zones* was introduced exactly with this intent in mind: to enhance user location privacy, that is, to make it hard for an observer to connect, to track, the user whereabouts over long periods of time. The initially considered observer was that of a *not fully trusted* application (Beresford and Stajano 2003), which would typically receive updates on user presence in specific spaces (zones). Mix-zones were introduced as regions within which, in contrast, none of the (present or registered as part of a certain group) users/devices provide location information to the said application. Ensuring this is so, specific middleware was presumed, regulating the flow of such information: when in a mix-zone, no location data are to be revealed by the user/device (*note*: we use, without loss of generality, the terms interchangeably for the rest of this discussion).

This privacy-enhancing approach leveraged the preexisting notion of a *pseudonym*, initially proposed in Chaum (1981), a temporary identifier and credential that does not reveal the actual identity of the device. A pseudonym is to be used in a specific context (e.g., for a short period of time, for a specific application, or a specific region), in lieu of the actual identity (and, possibly, the corresponding credential) of the device. In addition to the mobile device possibly swapping from one pseudonym to another at any time and place, mix-zones were introduced, precisely as regions within which identities, that is, pseudonyms, are mixed. In fact, devices are expected to change to a new unused pseudonym when they enter a mix-zone. As a result, over time, two or more pseudonyms of the same device can be increasingly difficult to link. The larger the number of users/devices associated with a mix-zone, the larger the corresponding *anonymity set*. Intuitively, the more numerous the devices that can be changing from one identity (pseudonym) to another, the higher the uncertainty from the viewpoint of the observer/*adversary*.

Mix-zones are broadly relevant for any location-based or location-aware application, even more so if communications (actions) revealing location (and identity) information are more frequent and extend over significant periods of time. The mix-zone placement, their dimensions, and the management of the user identities (actual and pseudonymous) and credentials depend on the actual mobile computing system design. Accordingly, the instantiation of mix-zones can vary, notably in terms of the mechanism that restricts the flow of location information towards the observer.

Vehicular communication (VC) systems, notably secure and privacy preserving VC systems (Papadimitratos and Hubaux 2011), were a new application area for mix-zones. Naturally so, because their functionality, notably the so-called cooperative awareness messages (CAMs), reveal precise location information of the vehicle on-board unit (OBU), several times per second, throughout a vehicle trip. CAMs and other types of messages can be collected by any passive receiver in a straightforward manner: typically, VC messages are mostly unencrypted, especially those for transportation safety and efficiency.

Aligned with the use of pseudonyms jointly with mix-zones, a main design choice for secure and privacy preserving VCs has been to provision each OBU with multiple pseudonyms, in this context, anonymized certified public keys, each with its corresponding private key. OBUs digitally sign, for example, CAMs with one private key while nearby receivers validate the signatures with the corresponding pseudonym (IEEE 1609.2). Vehicles change to another pseudonym after a (preferably) short period of time, e.g., a few minutes. Swapping to the next pseudonym can be at the discretion of the OBU, perhaps influenced by user preferences, or at predefined points in time, and, overall, based on VC system- or domain-wide policies (Papadimitratos et al. 2008).

An impromptu emergence of a mix-zone is possible, with each vehicle transitioning to another pseudonym during a period of silence. That is, a period during which OBUs temporarily cease to transmit, e.g., CAMs, desirably so in the presence of several other vehicles (Buttyan et al. 2007). With a commonly available, at all vehicles, modus operandi on how (i.e., when and where) to initiate such silent periods, location information can be held from the adversary/observer. In the VC context, the adversary can have, for example, a large set of access points or base stations deployed across a city or along freeway, receiving all or most of the VC transmissions in the same area.

An alternative approach is to deploy mix-zones leveraging existing network infrastructure, notably in VC systems and roadside units (RSUs). The idea is to avoid the silent periods, which may affect the system functionality, but rather construct the necessary concealment of traffic. This is done with the creation of a *cryptographic mix-zone* (CMIX) (Freudiger et al. 2007). Each RSU distributes a symmetric key, the specific CMIX key, to all approaching vehicles, so that these vehicles/OBUs can encrypt all transmissions and effectively conceal location and other information from an external observer. At the same time, while in the CMIX, all vehicles are to change to a new pseudonym. With potentially any vehicle able to essentially join a mix-zone when in proximity and make the needed own pseudonym change, privacy is enhanced. Intuitively, the more numerous the mix-zones, preferably placed in locations that can involve numerous vehicles, the higher the uncertainty for the adversary: the more difficult to link pseudonyms and the less likely it is to track any given vehicle.

Open Problems and Future Directions

Equipping each mobile platform (e.g., smart phone or OBU) with multiple pseudonyms, to be used for a short period of time, is generally applicable, beyond the notion of mix-zones. The more frequent the pseudonym changes are, the shorter the period messages (and related actions) of a given device can be trivially linked. One can consider anonymous authentication, e.g., in the VC context (Calandriello et al. 2011), or single-use pseudonyms (Khodaei et al. 2018) if needed. However, location-aware or location-based applications may require linkability over short periods of time; for example, in the context of pervasive computing and nomadic connectivity, while in one application zone (Beresford and Stajano 2003), or for VC systems, to facilitate transportation safety applications, e.g., predicting a potentially dangerous maneuver (Papadimitratos et al. 2006). In either case, the objective is to seek unlinkability over long(er) periods of time, with a design that assumes and accepts short-term linkability.

It is important to note that it is likely to connect two (or more) successive pseudonyms of the same device, leveraging the pseudonyms alone (that is, information included in the pseudonym, such as its validity period/lifetime or its issuer), or by exploiting data in the transmitted messages (e.g., the coordinates of the transmitting devices), or background knowledge on the mobility patterns of the involved platforms (e.g., movement in known road or building or space layouts). The methodology for linking inferences by an adversarial or curious observer is orthogonal to the notion of mix-zones. But the dimensions and the geometry of each zone, the underlying space limitations (e.g., the shape of an atrium or a hallway, or the shapes of road junctions or highway ramps), as well as the density, spacing, and placement of mix-zones can affect the level of the achieved unlinkability.

Assuming a budget for the deployment of mix-zones, e.g., the number of infrastructure entities, an optimization problem can be formulated to choose a placement that maximizes a location privacy metric and improves significantly over a random placement of mix-zones (Freudiger et al. 2009). The mix-zone geometry can facilitate linking, when vehicles are entering and exiting a mix-zone at times that are not hard to correlate. Taking into account, for VC systems, the road network and the mobility can help improve the mix-zone design towards improving unlinkability

(Palanisamy and Liu 2015). In case of small numbers of mobile users, it remains likely that correlations, based on timing and other information, are not hard.

The remedy can be the generation and transmission of decoy messages around mix-zones, to confuse the adversarial observer (Vaas et al. 2019). The challenge is to design such enhancements to mix-zones without requiring information from the mobile devices/users, while keeping the transmission cost low, and adjusting to the network mobility. Along these lines, a cooperative approach to disseminate the decoy traffic (Khodaei and Papadimitratos 2020) can significantly improve location privacy for differing geometry, density, and mobility situations.

With concrete results in hand, it is interesting to investigate how to broaden the adversary model. For example, along the lines of preserving location privacy in the face of honest-but-curious service providers (Jin and Papadimitratos 2019), (Gisdakis et al. 2016), consider honest-but-curious entities; in this context, for example, RSUs that instantiate a mix-zone. Or, consider collaboration (collusion) of honest-but-curious entities, or entities that undertake non-cooperative actions that can affect the operation (or level) of protection of any mix-zone scheme. With some consideration in pre-standardization investigations, e.g., (ETSI 2018) and based on the aforementioned developments, the concept could be deployed in future systems.

Cross-References

- Geo-Indistinguishability
- Privacy of Intelligent Vehicles
- Pseudonyms for Mobile Networks
- User Tracking and Re-identification

References

Beresford A, Stajano F (2003) Location privacy in pervasive computing. IEEE Pervasive Comput 2(1) Jan-March 2003

Beresford A, Stajano F (2004) Mix zones: user privacy in location-aware services. In: Proceedings of the second IEEE annual conference on pervasive computing and communications workshops

Buttyan L, Holczer T, Vajda I (2007) On the effectiveness of changing pseudonyms to provide location privacy in VANETs. In: Proceedings of ESAS, 2007

Calandriello G, Papadimitratos P, Hubaux J-P, Lioy A (2011) On the performance of secure vehicular communication systems. IEEE Trans Dependable Secure Comput (IEEE TDSC) 8(6):898–912

Chaum D (1981) Untraceable electronic mail, return addresses and digital pseudonyms. Commun ACM 24(2):84–88

Chaum D (1988) The dining cryptographers problem: unconditional sender and recipient untraceability. J Cryptol 1(1):66–75

Freudiger J, Raya M, Félegyházi M, Papadimitratos P, Hubaux JP (2007) Mix-zones for Location Privacy in Vehicular Networks. In: ACM Workshop on Wireless Networking for Intelligent Transportation Systems (ACM WiN-ITS), Vancouver, British Columbia, Canada, August 2007

Freudiger J, Shokri R, Hubaux J-P (2009) On the optimal placement of mix zones. In: Proceedings of the Privacy Enhancing Technologies Symposium (PETS), pp 216–234

Gisdakis S, Giannetsos A, Papadimitratos P (2016) Security, privacy & incentive provision for mobile crowd sensing systems. IEEE Internet Things J (IEEE IoT) 3(5):839–863

IEEE Standard for Wireless Access in Vehicular Environments–Security Services for Applications and Management Messages. https://standards.ieee.org/standard/1609_2-2016.html, January 2016

Intelligent Transport Systems (ITS) Security, Pre-standardization study on pseudonym change management, ETSI TR 103 415 V1.1.1, April 2018

Jin H, Papadimitratos P (2019) Resilient privacy protection for location-based services through decentralization. ACM Transactions on Privacy and Security (ACM TOPS), 22(4), 21:1–36

Khodaei M, Papadimitratos P (2020) Cooperative location privacy in vehicular networks: why simple mix-zones are not enough. IEEE Internet Of Things Journal (IEEE IoT)

Khodaei M, Jin H, Papadimitratos P (2018) SECMACE: Scalable and Robust Identity and Credential Management Infrastructure in Vehicular Communication Systems. IEEE Transactions on Intelligent Transportation Systems (IEEE ITS) 19(5): 1430–1444, May 2018

Palanisamy B, Liu L (2015) Attack-resilient mix-zones over road networks: architecture and algorithms. IEEE TMC 14(3):495–508

Papadimitratos, P and Hubaux, J-P (2011), "Secure vehicular communication systems," in Encyclopedia of cryptography and security (2 nd Edition), H. van Tilborg and S. Jajodia, Eds. Springer, Berlin, pp. 1140—1143

Papadimitratos, P, Gligor, V, and Hubaux, J-P (2006) Securing vehicular communications-assumptions, requirements, and principles. In: Workshop on

Embedded Security in Cars (ESCAR), Berlin, November 2006

Papadimitratos P, Buttyan L, Holczer T, Schoch E, Freudiger J, Raya M, Ma Z, Kargl F, Kung A, Hubaux J-P (2008) Secure vehicular communication systems: design and architecture. IEEE Commun Mag 46(11):100–109

Vaas C, Khodaei M, Papadimitratos P, Martinovic I (2019) Nowhere to hide? Mix-zones for private pseudonym change using chaff vehicles. In: Proceedings of the IEEE Vehicular Networking Conference (VNC), Taipei, Taiwan, Dec 2018