STAMP ENABLING PRIVACY-PRESERVING LOCATION PROOF FOR MOBILE USERS

MAKHAVARAPU JHANSI PRIYANKA, B. LATHA
Mtech Scholar, Assistant Professor
Department of of CSE
ISTS Women's Engineering College, Rajanagaram, Rajamahendravaram, A.P, India.

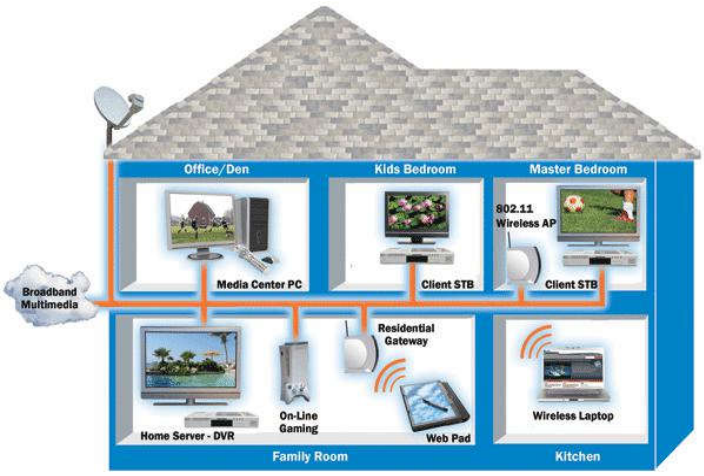
ABSTRACT:

Location-based services are quickly becoming immensely popular. In addition to services based on users' current location, many potential services rely on users' location history, or their spatial-temporal provenance. Malicious users may lie about their spatial-temporal provenance without a carefully designed security system for users to prove their past locations. In this paper, we present the Spatial-Temporal provenance Assurance with Mutual Proofs (STAMP) scheme. STAMP is designed for ad-hoc mobile users generating location proofs for each other in a distributed setting. However, it can easily accommodate trusted mobile users and wireless access points. STAMP ensures the integrity and non-transferability of the location proofs and protects users' privacy. A semi-trusted Certification Authority is used to distribute cryptographic keys as well as guard users against collusion by a light-weight entropy-based trust evaluation approach. Our prototype implementation on the Android platform shows that STAMP is low-cost in terms of computational and storage resources. Extensive simulation experiments show that our entropy-based trust model is able to achieve high collusion detection accuracy.

1. INTRODUCTION

1.1 WHAT IS NETWORKING?

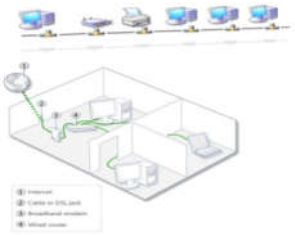
Networking is the word basically relating to computers and their connectivity. It is very often used in the world of computers and their use in different connections. The term networking implies the link between two or more computers and their devices, with the vital purpose of sharing the data stored in the computers, with each other. The networks between the computing devices are very common these days due to the launch of various hardware and computer software which aid in making the activity much more convenient to build and use.



Structure of Networking between the different computers

How networking works?

General Network Techniques - When computers communicate on a network, they send out data packets without knowing if anyone is listening. Computers in a network all have a connection to the network and that is called to be connected to a network bus. What one computer sends out will reach all the other computers on the local network.



Above diagrams show the clear idea about the networking functions For the different computers to be able to distinguish between each other, every computer has a unique ID called MAC-address (Media Access Control Address). This address is not only unique on your network but unique for all devices that can be hooked up to a network. The MAC-address is tied to the hardware and has nothing to do with IP-addresses. Since all computers on the network receives everything that is sent out from all other computers the MAC-addresses is primarily used by the computers to filter out incoming network traffic that is addressed to the individual computer.When a computer communicates with another computer on the network, it sends out both the other computers MAC-address and the MAC-address of its own. In that way the receiving computer will not only recognize that this packet is for me but also, who sent this data packet so a return response can be sent to the sender.

On an Ethernet network as described here, all computers hear all network traffic since they are connected to the same bus. This network structure is called multi-drop.

One problem with this network structure is that when you have, let say ten (10) computers on a network and they communicate frequently and due to that they sends out there data packets randomly, collisions occur when two or more computers sends data at the same time. When that happens data gets corrupted and has to be resent. On a network that is heavy loaded even the resent packets collide

with other packets and have to be resent again. In reality this soon becomes a bandwidth problem. If several computers communicate with each other at high speed they may not be able to utilize more than 25% of the total network bandwidth since the rest of the bandwidth is used for resending previously corrupted packets. The way to minimize this problem is to use network switches.

Characteristics of Networking:

The following characteristics should be considered in network design and ongoing maintenance:

1. **Availability** is typically measured in a percentage based on the number of minutes that exist in a year. Therefore, uptime would be the number of minutes the network is available divided by the number of minutes in a year.
2. **Cost** includes the cost of the network components, their installation, and their ongoing maintenance.
3. **Reliability** defines the reliability of the network components and the connectivity between them. Mean time between failures (MTBF) is commonly used to measure reliability.
4. **Security** includes the protection of the network components and the data they contain and/or the data transmitted between them.
5. **Speed** includes how fast data is transmitted between network end points (the data rate).
6. **Scalability** defines how well the network can adapt to new growth, including new users, applications, and network components.
7. **Topology** describes the physical cabling layout and the logical way data moves between components.

Types of Networks:

Organizations of different structures, sizes, and budgets need different types of networks. Networks can be divided into one of two categories:

- peer-to-peer
- server-based networks

1. Peer-to-Peer Network:

A peer-to-peer network has no dedicated servers; instead, a number of workstations are connected together for the purpose of sharing information or devices. Peer-to-peer networks are designed to satisfy the networking needs of home networks or of small companies that do not want to spend a lot of money on a dedicated server but still want to have the capability to share information or devices like in school, college, cyber cafe

2. Server-Based Networks:

In server-based network data files that will be used by all of the users are stored on the one server. With a server-based network, the network server stores a list of users who may use
network resources and usually holds the resources as well. This will help by giving you a central point to set up permissions on the data files, and it will give you a central point from which to back up all of the data in case data loss should occur.

Network Communications:

- Computer networks use signals to transmit data, and protocols are the languages computers use to communicate.
- Protocols provide a variety of communications services to the computers on the network.
- Local area networks connect computers using a shared, half-duplex, baseband medium, and wide area networks link distant networks.
- Enterprise networks often consist of clients and servers on horizontal segments connected by a common backbone, while peer-to-peer networks consist of a small number of computers on a single LAN.

Advantages of Networking:

1. Easy Communication:

It is very easy to communicate through a network. People can communicate efficiently using a network with a group of people. They can enjoy the benefit of emails, instant messaging, telephony, video conferencing, chat rooms, etc.

2. Ability to Share Files, Data and Information:

This is one of the major advantages of networking computers. People can find and share information and data because of networking. This is beneficial for large organizations to maintain their data in an organized manner and facilitate access for desired people.

3. Sharing Hardware:

Another important advantage of networking is the ability to share hardware. For an example, a printer can be shared among the users in a network so that there's no need to have individual printers for each and every computer in the company. This will significantly reduce the cost of purchasing hardware.

4. Sharing Software:

Users can share software within the network easily. Networkable versions of software are available at considerable savings compared to individually licensed version of the same software. Therefore large companies can reduce the cost of buying software by networking their computers.

5. Security:

Sensitive files and programs on a network can be password protected. Then those files can only be accessed by the authorized users. This is another important advantage of networking when there are concerns about security issues. Also each and every user has their own set of privileges to prevent those accessing restricted files and programs.

6. Speed:

Sharing and transferring files within networks is very rapid, depending on the type of network.
This will save time while maintaining the integrity of files.

1.2 WHAT IS SECURE COMPUTING?

Computer security (Also known as cyber security or IT Security) is information security as applied to computers and networks. The field covers all the processes and mechanisms by which computer-based equipment, information and services are protected from unintended or unauthorized access, change or destruction. Computer security also includes protection from unplanned events and natural disasters. Otherwise, in the computer industry, the term security -- or the phrase computer security -- refers to techniques for ensuring that data stored in a computer cannot be read or compromised by any individuals without authorization. Most computer security measures involve data encryption and passwords. Data encryption is the translation of data into a form that is unintelligible without a deciphering mechanism. A password is a secret word or phrase that gives a user access to a particular program or system.

Diagram clearly explain the about the secure computing

Working conditions and basic needs in the secure computing:

If you don't take basic steps to protect your work computer, you put it and all the information on it at risk. You can potentially compromise the operation of other computers on your organization's network, or even the functioning of the network as a whole.

1. **Physical security:**

Technical measures like login passwords, anti-virus are essential. (More about those below) However, a secure physical space is the first and more important line of defense.

Is the place you keep your workplace computer secure enough to prevent theft or access to it while you are away? While the Security Department provides coverage across the Medical center, it only takes seconds to steal a computer, particularly a portable device like a laptop or a PDA. A computer should be secured like any other valuable possession when you are not present.

Human threats are not the only concern. Computers can be compromised by environmental mishaps (e.g., water, coffee) or physical trauma. Make sure the physical location of your computer takes account of those risks as well.

2. **Access passwords:**

The University's networks and shared information systems are protected in part by login credentials (user-IDs and passwords). Access passwords are also an essential protection for personal computers in most circumstances. Offices are usually open and shared spaces, so physical access to computers cannot be completely controlled.

To protect your computer, you should consider setting passwords for particularly sensitive applications resident on the computer (e.g., data analysis software), if the software provides that capability.

3. **Prying eye protection:**

Because we deal with all facets of clinical, research, educational and administrative data here on the medical campus, it is important to do everything possible to minimize exposure of data to unauthorized individuals.

4. **Anti-virus software:**

Up-to-date, properly configured anti-virus software is essential. While we have server-side anti-virus software on our network computers, you still need it on the client side (your computer).

5. Firewalls:

Anti-virus products inspect files on your computer and in email. Firewall software and hardware monitor communications between your computer and the outside world. That is essential for any networked computer.

6. Software updates:

It is critical to keep software up to date, especially the operating system, anti-virus and anti-spyware, email and browser software. The newest versions will contain fixes for discovered vulnerabilities.

Almost all anti-virus have automatic update features (including SAV). Keeping the "signatures" (digital patterns) of malicious software detectors up-to-date is essential for these products to be effective.

7. Keep secure backups:

Even if you take all these security steps, bad things can still happen. Be prepared for the worst by making backup copies of critical data, and keeping those backup copies in a separate, secure location. For example, use supplemental hard drives, CDs/DVDs, or flash drives to store critical, hard-to-replace data.

8. Report problems:

If you believe that your computer or any data on it has been compromised, your should make a information security incident report. That is required by University policy for all data on our systems, and legally required for health, education, financial and any other kind of record containing identifiable personal information.

2. LITERATURE SURVEY

1) A Secure verification of location claims

AUTHORS: N. Sastry, U. Shankar, and D. Wagner,

With the growing prevalence of sensor and wireless networks comes a new demand for location-based access control mechanisms. We introduce the concept of secure location verification, and we show how it can be used for location-based access control. Then, we present the Echo protocol, a simple method for secure location verification. The Echo protocol is extremely lightweight: it does not require time synchronization, cryptography, or very precise clocks. Hence, we believe that it is well suited for use in small, cheap, mobile devices.

2) Location Verification using Secure Distance Bounding Protocols. AUTHORS: D. Singelee and B. Preneel,

Abstract— Authentication in conventional networks (like the Internet) is usually based upon something you know (e.g., a password), something you have (e.g., a smartcard) or something you are (biometrics). In mobile ad–hoc networks, location information can also be used to authenticate devices and users. We will focus on how a prover can securely show that (s)he is within a certain distance to a verifier. Brands and Chaum proposed the distance bounding protocol as a secure solution for this problem. However, this protocol is vulnerable to a so– called **"**terrorist fraud attack**"**. In this paper, we will explain how to modify the distance bounding protocol to make it resistant to this kind of attacks. Recently, two other secure distance bounding protocols were published. We will discuss the properties of these protocols and show how to use it as a building block in a location verification scheme.

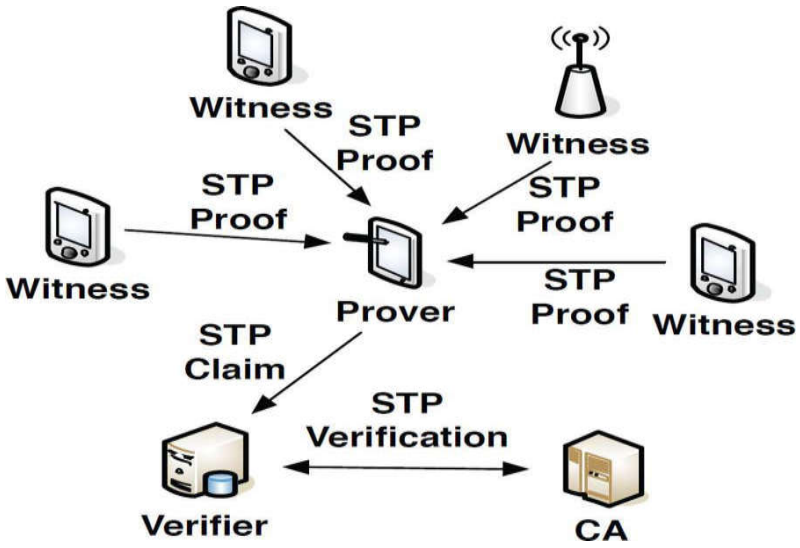
3) **A privacy-aware location proof architecture**
AUTHORS: W. Luo and U. Hengartner,
Recently, there has been a dramatic increase in the number of location-based services, with services like Foursquare or Yelp having hundreds of thousands of users. A user's location is a crucial factor for enabling these services. Many services rely on users to correctly report their location. However, if there is an incentive, users might lie about their location. A location proof architecture enables users to collect proofs for being at a location and services to validate these proofs. It is essential that this proof collection and validation does not violate user privacy. We introduce VeriPlace, a location proof architecture with user privacy as a key design component. In addition, VeriPlace can detect cheating users who collect proofs for places where they are not located. We also present an implementation and a performance evaluation of VeriPlace and its integration with Yelp.

4) **Distance-bounding proof of knowledge to avoid real-time attacks,**
AUTHORS: L. Bussard and W. Bagga
Traditional authentication is based on proving the knowledge of a private key corresponding to a given public key. In some situations, especially in the context of pervasive computing, it is additionally required to verify the physical proximity of the authenticated party in order to avoid a set of real-time attacks. Brands and Chaum proposed distance-bounding .protocols as a way to compute a practical upper bound on the distance between a prover and a verifier during an authentication process. Their protocol prevents frauds where an intruder sits between a legitimate prover and a verifier and succeeds to perform the distance-bounding process. However, frauds where a malicious prover and an intruder collaborate to cheat a verifier have been left as an open issue. In this paper, we provide a solution preventing both types of attacks.

5) **Practical and provably-secure commitment schemes from collision-free hashing**
AUTHORS: S. Halevi and S. Micali,
We present a very practical string-commitment scheme which is provably secure based solely on collision-free hashing. Our scheme enables a computationally bounded party to commit strings to an unbounded one, and is optimal (within a small constant factor) in terms of interaction, communication, and computation. Our result also proves that constant round statistical zero-knowledge arguments and constant-round computational zero-knowledge proofs for NP exist based on the existence of collision-free hash functions.

3. SYSTEM DESIGN

3.1 SYSTEM ARCHITECTURE:



3.2 DATA FLOW DIAGRAM:

1. The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system.
2. The data flow diagram (DFD) is one of the most important modeling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system.
3. DFD shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations that are applied as data moves from input to output.
4. DFD is also known as bubble chart. A DFD may be used to represent a system at any level of abstraction. DFD may be partitioned into levels that represent increasing information flow and functional detail.

4. SYSTEM ANALYSIS

4.1 EXISTING SYSTEM:

- Today's location-based services solely rely on users' devices to determine their location, e.g., using GPS. However, it allows malicious users to fake their STP information. Therefore, we need to involve third parties in the creation of STP proofs in order to achieve the integrity of the STP proofs. This, however, opens a number of security and privacy issues.
- Hasan *et al.*proposed a scheme which relies on both location proofs from wireless APs and witness endorsements from Bluetooth-enabled mobile peers, so that no users can forge proofs without colluding with both wireless APs and other mobile peers at the same time.

- In Davis *et al.*'s alibi system, their private corroborator scheme relies on mobile users within proximity to create alibi's (i.e., location proofs) for each other.

4.2 DISADVANTAGES OF EXISTING SYSTEM:

- Most of the existing STP proof schemes rely on wireless infrastructure (e.g., WiFi APs) to create proofs for mobile users. However, it may not be feasible for all types of applications, e.g., STP proofs for the green commuting and battlefield examples certainly cannot be obtained from wireless APs.
- Most of the existing schemes require multiple trusted or semi-trusted third parties.

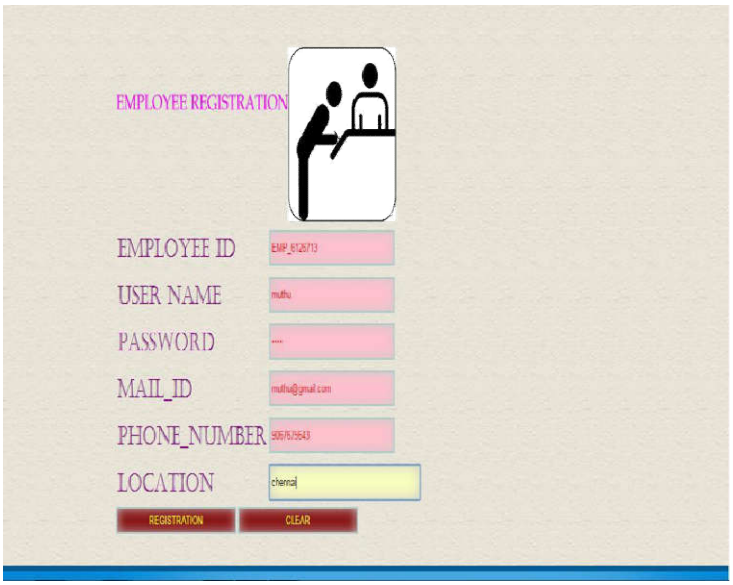
4.3 PROPOSED SYSTEM:

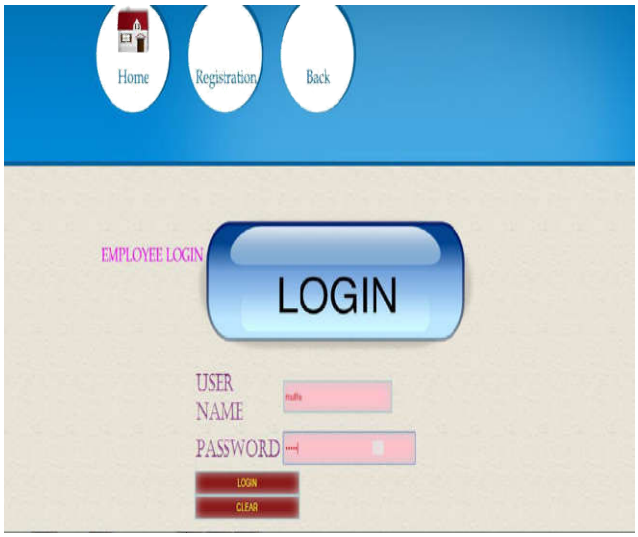
- In this paper, we define the past locations of a mobile user at a sequence of time points as the *spatial-temporal provenance* (STP) of the user, and a digital proof of user's presence at a location at a particular time as an *STP proof*.
- In this paper, we propose an STP proof scheme named Spatial-Temporal provenance Assurance with Mutual Proofs (STAMP). STAMP aims at ensuring the integrity and non-transferability of the STP proofs, with the capability of protecting users' privacy.
- We propose an entropy-based trust model to detect the collusion scenario.
- A distributed STP proof generation and verification protocol (STAMP) is introduced to achieve integrity and non-transferability of STP proofs.
- No additional trusted third parties are required except for a semi-trusted CA.
- STAMP is designed to maximize users' anonymity and location privacy. Users are given the control over the location granularity of their STP proofs.
- STAMP is collusion-resistant. The Bussard-Bagga distance bounding protocol is integrated into STAMP to prevent a user from collecting proofs on behalf of another user.
- An entropy-based trust model is proposed to detect users mutually generating fake proofs for each other.
- STAMP uses a entropy-based trust model to guard users from prover-witness collusion. This model also encourages witnesses against selfish behavior.

4.4 ADVANTAGES OF PROPOSED SYSTEM:

- Target a wider range of applications.
- STAMP is based on a distributed architecture.
- STAMP requires only a single semi-trusted third party which can be embedded in a Certificate Authority (CA).
- We design our system with an objective of protecting users' anonymity and location privacy.
- No parties other than verifiers could see both a user's identity and STP information (verifiers need both identity and STP information in order to perform verification and provide services).
- STAMP requires low computational overhead.
- A security analysis is presented to prove STAMP achieves the security and privacy objectives.

11. SCREEN SHOTS:





CONCLUSION

In this projet we have presented STAMP, which aims at providing security and privacy assurance to mobile users' proofs for their past location visits. STAMP relies on mobile devices in vicinity to mutually generate location proofs or uses wireless APs to generate location proofs. Integrity and non-transferability of location proofs and location privacy of users are the main design goals of STAMP. We have specifically dealt with two collusion scenarios: P-P collusion and P-W collusion. To protect against P-P collusions, we integrated the Bussard-Bagga distance bounding protocol into the design of STAMP. To detect P-W collusion, we proposed an entropy-based trust model to evaluate the trust level of claims of the past location visits. Our security analysis shows that STAMP achieves the security and privacy objectives. Our implementation on Android smartphones indicates that low computational and storage resources are required to execute STAMP. Extensive simulation results show that our trust model is able to attain a high balanced accuracy with appropriate choices of system parameters.

REFERENCES

[1]S. Saroiu and A. Wolman, “Enabling new mobile applications with location proofs,” in Proc. ACM HotMobile, 2009, Art. no. 3.

[2]W. Luo and U. Hengartner, “VeriPlace: A privacy-aware location proof architecture,” in Proc. ACM GIS, 2010, pp. 23–32.

[3]Z. Zhu and G. Cao, “Towards privacy-preserving and colluding-resistance in location proof updating system,” IEEE Trans. Mobile Comput., vol. 12, no. 1, pp. 51–64, Jan. 2011.

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

[5]R. Hasan and R. Burns, “Where have you been? secure location provenance for mobile devices,” CoRR 2011.

[6]B. Davis, H. Chen, and M. Franklin, “Privacy preserving alibi systems,” in Proc. ACM ASIACCS, 2012, pp. 34–35.

[7]I. Krontiris, F. Freiling, and T. Dimitriou, “Location privacy in urban sensing networks: Research challenges and directions,” IEEE Wireless Commun., vol. 17, no. 5, pp. 30–35, Oct. 2010.

[8]Y. Desmedt, “Major security problems with the ‘unforgeable’ (feige)- fiat-shamir proofs of identity and how to overcome them,” in Proc. SecuriCom, 1988, pp. 15–17.

[9]L. Bussard and W. Bagga, “Distance-bounding proof of knowledge to avoid real-time attacks,” in Security and Privacy in the Age of Ubiquitous Computing. New York, NY, USA: Springer, 2005.

[10]B. Waters and E. Felten, “Secure, private proofs of location,” Department of Computer Science, Princeton University, Princeton, NJ, USA, Tech. Rep., 2003.

[11]X. Wang et al., “STAMP: Ad hoc spatial-temporal provenance assurance for mobile users,”in Proc. IEEE ICNP, 2013, pp. 1–10.

[12]A. Pfitzmann and M. Köhntopp, “Anonymity, unobservability, and pseudonymity-a proposal for terminology,” in Designing Privacy Enhancing Technologies. New York, NY, USA:Springer, 2001.

[13]Y.-C. Hu, A. Perrig, and D. B. Johnson, “Wormhole attacks in wireless networks,” IEEE J. Sel. Areas Commun., vol. 24, no. 2, pp. 370–380, Feb. 2006.

[14]S. Halevi and S. Micali, “Practical and provably-secure commitment schemes from collision-free hashing,” in Proc. CRYPTO, 1996, pp. 201–215.

[15]I. Damgård, "Commitment schemes and zero- knowledge protocols," in Proc. Lectures Data Security, 1999, pp. 63–86.
[16]I. Haitner and O. Reingold, "Statistically-hiding commitment from any one-way function,"in Proc. ACM Symp. Theory Comput., 2007, pp. 1–10.
[17]D. Singelee and B. Preneel, "Location verification using secure distance bounding protocols," in Proc. IEEE MASS, 2005.
[18]J. Reid, J. Nieto, T. Tang, and B. Senadji, "Detecting relay attacks with timing-based protocols," in Proc. ACM ASIACCS, 2007, pp. 204–213.
[19]C. Kim, G. Avoine, F. Koeune, F. Standaert, and O. Pereira, "The Swiss-knife RFID distance bounding protocol," in Proc. ICISC, 2009, pp. 98–115.
[20]H. Han et al., "Senspeed: Sensing driving conditions to estimate vehicle speed in urban environments," in Proc. IEEE INFOCOM, Apr. 2014, pp. 727–735.
[21]I. Afyouni, C. Ray, and C. Claramunt, "Spatial models for context aware indoor navigation systems: A survey," J. Spatial Inf. Sci., no. 4, pp. 85–123, 2014.
[22]N. Roy, H. Wang, and R. R. Choudhury, "I am a smartphone and I can tell my user's walking direction," in Proc. ACM MobiSys, 2014, pp. 329–342.
[23]R. Steinbach, J. Green, and P. Edwards, "Look who's walking: Social and environmental correlates of children's walking in London," Health Place, vol. 18, no. 4, pp. 917–927, 2012.
[24]K. Brodersen, C. Ong, K. Stephan, and J. Buhmann, "The balanced accuracy and its posterior distribution," in Proc. IEEE ICPR, 2010, pp. 3121–3124.
[25]B. Peterson, R. Baldwin, and J. Kharoufeh, "Bluetooth inquiry time characterization and selection," IEEE Trans. Mobile Comput., vol. 5, no. 9, pp. 1173–1187, Sep. 2006.
[26]J. Zhu, K. Zeng, K.-H. Kim, and P. Mohapatra, "Improving crowdsourced Wi-Fi localization systems using Bluetooth beacons," in Proc. 9th Annu. IEEE SECON, Jun. 2012, pp. 290–298.