Quest for Personal Control over Mobile Location Privacy

Qi He* Dapeng Wu† Pradeep Khosla‡

Abstract

How to protect location privacy of mobile users is an important issue in ubiquitous computing. However, location privacy protection is particularly challenging: on one hand, the administration requires all legitimate users to provide identity (ID) information in order to grant them permission to use its wireless service; on the other hand, mobile users would prefer not to expose any information which enables anyone, including the administration, to get some clue regarding their whereabouts, that is, mobile users would like to have complete personal control of their location privacy. To address this issue, we propose an authorized-anonymous-ID based scheme; this scheme effectively eliminates the need for a trusted server or administration, which is assumed in the previous work. Our key weapon is a cryptographic technique called *blind signature*, which is used to generate an authorized-anonymous-ID that replaces the real ID of an authorized mobile device. With authorized-anonymous-IDs, we design an architecture that is capable of achieving complete personal control over location privacy while maintaining the authentication function required by the administration.

Key Words: security techniques and systems, wireless local area network (WLAN), personal area network (PAN), ubiquitous computing, location information service, location privacy, access

*Carnegie Mellon University, Dept. of Electrical & Computer Engineering, 5000 Forbes Avenue, Pittsburgh, PA 15213, USA. Email: qihe@cmu.edu.

†Please direct all correspondence to Prof. Dapeng Wu, University of Florida, Dept. of Electrical & Computer Engineering, Center Drive, Engineering Building 431, Gainesville, FL 32611, USA. Tel. (352) 392-4954, Fax (352) 392-0044, Email: wu@ece.ufl.edu. URL: http://www.wu.ece.ufl.edu.

‡Carnegie Mellon University, Dept. of Electrical & Computer Engineering, 5000 Forbes Avenue, Pittsburgh, PA 15213, USA. Tel. (412) 268-5090, Fax (412) 268-5787, Email: pkk@ece.cmu.edu. URL: http://www.ece.cmu.edu/about/deptheadbio.shtml.

control, blind signature.

1 Introduction

The convergence of wireless communication infrastructure, mobile computing devices, and embedded systems, has been making a profound shift in the way we live and work, offering the promise of bringing us close to the holy grail of information technology: ubiquitous computing – computing at any place and at any time [1]. To fulfill the promise of ubiquitous computing, information about mobile users' location is a critical and valuable resource which needs to be utilized. Many efforts have been made to get it available, as one of the key services in the ubiquitous computing environment. However, the location information service or functionality can act as a double-edged sword – it can make our life more convenient; yet, it could also provide criminals with powerful weapons to compromise privacy of mobile users. Computer scientists have realized that unless the use of this information is strictly controlled, it can be put to a variety of unsavory situations [1, 2].

To address the location privacy issue, an architecture for location privacy control [2] was designed and experimented on the WirelessAndrew network, an IEEE 802.11 wireless local area network (WLAN) that covers the entire campus of Carnegie Mellon University. The architecture implemented in [2] is illustrated in Fig. 1. Under the architecture, there is a centralized location server, where a mobile user can register and submit her location information along with her "permission rule set" regarding her privacy preferences. Others can send queries to the server for location information about mobile users whose location information is stored in the server. The server processes the query according to the queried user's preference specified within the set of rules, and then the server may return the queried information, deny the query, or return a fake location as described in [2].

This architecture was primitive in the initial phase of the experimental system because it focused on strategic treatments of mobile location privacy rather than the system construction. This simple architecture is essentially identical to the one described in [1]. In [1], it was suggested that a distributed architecture could benefit the control of mobile location privacy, since a centralized architecture has the following drawbacks:

- The location privacy of mobile users is not completely under their own control since

the system administration maintains a central server where the location information of mobile users is stored.

- The central server is a single-failure-point; that is, the location privacy of mobile users would be compromised if an attacker successfully hacked into it.
- The centralized architecture is not scalable.

However, to achieve complete personal control on location privacy by replacing a centralized architecture with a distributed one is not trivial. For instance, the system administration, for the sake of system maintenance and management, has the privilege to check any access point and obtain a list of IP addresses and corresponding MAC (Medium Access Control) addresses of the mobile devices that are connecting to the checked access point. The administration also has the data[1] that can indicate a bijection relationship between MAC addresses (or IP addresses) of authorized mobile devices and registered legitimate mobile users. The location information about a mobile user can be easily figured out by the administration. Then, we face such a dilemma: on one hand, the administration would like to require all legitimate users to provide information for authentication in order to grant them permission to use their wireless service; on the other hand, the mobile users would prefer not to expose any of their information (e.g., IDs and MAC addresses) which would enable anyone, including the administration, to get clues regarding their whereabouts.

To resolve the above dilemma, this paper proposes an authorized-anonymous-ID based scheme. In our scheme, an authorized-anonymous-ID generated by a cryptographic technique called *blind signature* [3], is used to replace the real ID (e.g., an MAC address) of an authorized mobile device (e.g., an WaveLAN card). An anonymous ID can tell nothing more than whether the provider of the ID is an authorized user. This authorized-anonymous-ID is then used as the key for packets authentication, and the message authentication code [4] (generated by the key) is used for access control. In this way, the administration can

[1]In the current solution, a mobile user must register her device (wireless LAN card) before she can use the card to get connection. In current system, the registration is done by submitting MAC of the wireless card and the user's ID. The MAC is used for access points to decide whether the connection is granted. Packets from an unregistered MAC will get dropped.

grant authorized mobile users an access to the wireless communication infrastructure, while mobile users need not divulge their real ID during authorization, which could otherwise lead to compromising their location privacy.

Built on an agent-based architecture,[2] our authorized-anonymous-ID based scheme enables the mobile users to have complete control of their location privacy.

The rest of the paper is organized as follows. Section 2 describes our system architecture for personal control of mobile location privacy. In Section 3, we present a set of protocols for the authorized-anonymous-ID based scheme, which enables location privacy protection. Section 4 discusses the related work. In Section 5, we conclude the paper.

2 System Architecture

To address the location privacy issue in a ubiquitous computing environment, we need to understand the key components for ubiquitous computing. Based on this understanding, we can then design a system to protect location privacy. So we organize this section as below. We first sketch key components in ubiquitous computing from a security perspective in Section 2.1, and then present our agent-based system architecture for location privacy protection in Section 2.2.

2.1 A Sketch of Ubiquitous Computing

For quite some time, a ubiquitous computing environment has been depicted as dynamically-changing self-organized networks, formed by resource-constrained mobile devices, which occasionally join and leave the networks. However, it is hard to believe that this ad hoc infrastructure-less fashion could be the typical formation of what we call ubiquitous computing. We believe that identifying reasonable formations of ubiquitous computing and exploring security implication of ubiquitous computing based on the discovered formations is a fundamentally significant research. Having a similar experience as mentioned in [5], we learn that a ubiquitous computing environment should be formed by a *powerful infrastruc-*

[2] An agent is a computer program/code, which is autonomous.

ture that is highly available, cost effective, and sufficiently scalable to support millions of users, and low-power mobile devices, which are small and lightweight; it does not matter very much what a device can do, but what matters is the possibility that the device can harness tera-bytes of data and the power of supercomputers even while mobile – as long as it has an access to a ubiquitous network [5]. This understanding of the formation of ubiquitous computing will guide the design of our system architecture for location privacy protection.

On the other hand, security, already a thorny problem in the Internet, is greatly complicated by ubiquitous computing, not only because of its security vulnerability due to the sharing nature of the wireless medium, and computational limitation resulting from requirements of low weight, compact size, and good ergonomics of mobile device and embedded systems; but more importantly because of the following challenges:

- Geographically distributed systems are connected to form heterogeneous networks of unlimited scale; so there can be no central authority, no homogeneous security policy, and no ubiquitous security infrastructure for security enforcement or guarantee.
- Ubiquitous computing creates an environment full of computing and communication devices, yet gracefully integrated with human users [1]; so the electronic security mechanisms must be user-centered, and cannot rely on or be controlled by network-infrastructure operators.
- The design of security mechanisms for ubiquitous computing needs to follow the end-to-end principle [6].

The agent technology [7] can effectively address the aforementioned challenges for three reasons. First, agents are autonomous and distributed; so no central authority is needed for security enforcement. Second, agents can act on users' behalf; hence, agent-based security mechanisms can be designed as user-centered. Third, agents are application-oriented, which naturally satisfies the end-to-end principle, i.e., agents communicate on the application layer.

Based on the agent concept, we perceive, from a security perspective, that a ubiquitous computing environment should consist of the following three key components (see Fig. 2).

1. *Personal Trust Computing Base (PTCB)*: is a personal-held computing device, such as personal digital assistant (PDA) and laptop; a PTCB is under the full control of the owner, and only the owner with proper authentication information such as personal identification number (PIN) or biometrics information, can activate a PTCB to work on behalf of the owner.

2. *Personal Area Network (PAN)*: is an architecture that consists of a main home PC, which has a connection to an Internet gateway, and has a wide range of appliances (i.e., PTCBs) connected to the main home PC, by many kinds of means. Each PTCB is associated with some kind of autonomous software, called agent (or proxy). The agent runs on the PTCB if the PTCB is computational capable of running its agent; otherwise, the agent runs on the main home PC.

   To secure the communication within a PAN, we need to consider two cases: 1) an agent runs on the PTCB, and 2) an agent runs on the main home PC. For the first case, a protocol can be designed to initialize a symmetric key shared by the PTCB and the main home PC; and then the messages between the PTCB and the main home PC can be encrypted and authenticated with the shared secret key. For the second case, one method called *resurrecting duckling* [8] can be employed to have a PTCB and its agent share a symmetric key to secure their communication; then, PTCBs can securely communicate with each other through their agents, which can negotiate keys for encryption or authentication. Hence, the communication within a PAN can be secured by symmetric crypto-systems.

   An engineering practice that addresses the second case is described in [9]; there, a device-to-proxy protocol and a proxy-to-proxy protocol were designed and implemented.

3. *Internet*: provides a communication channel between a PTCB and a PAN; however, the channel cannot be trusted.

2.2 Agent-based System Architecture

Since the properties of agents meet the security requirements imposed by ubiquitous computing, we design an agent-based system architecture for location privacy protection. We first introduce the following agents that act on behalf of the players (devices or users) under our architecture.

- *Administrator (A)*: is an agent that acts on behalf of an administration to authenticate legitimate users and grant them an access to the wireless infrastructure.
- *Rover (R)*: is an agent running at a PTCB and acts on behalf of the owner of a mobile device. It is responsible to work out the location of the mobile device, automatically update the location information stored in the home PC (managed by another agent called *manager*, described below), and interact with the users for privacy permission setting [2].
- *Manager (M)*: is an agent running at a home PC and can be delegated to act on behalf of a mobile user. It manages the location information submitted by the Rover and executes the user's control policy [2] for location privacy when it processes location information queries from other users.
- *Connector (C)*: is an agent running at an access point and is delegated by the Administrator agent to authenticate mobile devices and control wireless connections between mobile devices and the access point.
- *Lookup (L)*: is an optional agent that provides Internet users with public look-up service. Lookup agents acting as well-known public service providers, will listen for the location information queries from users and forward the queries to the queried users' Manager agent running at their home.

With the above agents, we propose a multi-agent system architecture as illustrated in Fig. 3. Under the architecture, agents communicate with each other through three types of protocols. The three protocols are the registration protocol, the controlled connection

protocol, and the location query/response protocol, which are are numbered with 1, 2, and 3, respectively in Fig. 3. In the next section, we present the registration protocol and the controlled connection protocol; the description of the location query/response protocol can be found in Ref. [2].

3 Authorized-anonymous-ID Based Scheme

This section presents our authorized-anonymous-ID based scheme, specifically, the registration protocol and the controlled connection protocol.

To authenticate users when they request for accessing the wireless infrastructure, we first need to assign a valid ID to a legitimate user (i.e., authorizing a user), and then only the authorized users are allowed to access the network infrastructure (i.e., access control). Hence, there are two phases in our scheme: 1) the registration phase specified by a registration protocol, and 2) the controlled connection phase specified by a controlled connection protocol. The registration phase is to authorize users while the controlled connection phase is to control the access. In the first phase, the manager (or rover) of a mobile user applies for an authorized-anonymous-ID from the administrator of the wireless infrastructure. After the first phase, the obtained authorized-anonymous-ID is carried by the rover of the mobile user and will be presented when the mobile device is requesting for connection through an access point. In the second phase, the rover presents the ID to request for connection and the ID is also used by the access point to authenticate the packets from the mobile device thereafter for the purpose of access control.

Table 1 lists the notations used in the description of the protocols. Note that since both R_u and M_u have the private key of U, both of them can 'speak for' U. If R_u and M_u are interchangeable in the protocol, we use U to represent them. In other words, U in the following protocols can be replaced by either R_u or M_u.

Table 1: Notations.

U	:	A mobile user, identified by her public key. The corresponding private key is held by her rover running in her PTCB and Manager in home-PC of PAN.
R_u	:	Rover of mobile user U.
M_u	:	Manager of mobile user U.
E_x	:	Public key of X.
D_x	:	Private key of X.
$K_{xy}(m)$	:	Encrypt m by using symmetric crypto-system with a key shared by x and y.
$K_{xy}^{-1}(c)$	:	Decrypt c by using symmetric crypto-system with a key shared by x and y.
$H(x)$	:	One-way hash function with input x.
$E_x(m)$	:	Encrypt m by using asymmetric crypto-system[3] with the public key of x.
$D_x(c)$	:	Decrypt a cipher c with the public key of x.
r_0, r_1	:	Random numbers.
ack	:	Acknowledgement for the last received message.

3.1 Registration Protocol

In our registration protocol, initial authentication of users is required. We assume that there is an infrastructure supporting the initial authentication of users. This infrastructure could be either a public key infrastructure (PKI) or a Kerberos based system [10]. In the case that a PKI is in place, to obtain authentication, a user must sign its request using its digital signature, and send the request to the administrator.

Our registration protocol is based on authorized-anonymous-ID. With an authorized-anonymous-ID as a digital token, a legitimate mobile device can be granted permission to access the wireless infrastructure after a successful authentication; yet the association between the token and the real ID of a legitimate user is eliminated. The registration protocol is outlined in Fig. 4.

As we mentioned previously, the role of a U in the registration protocol could be played by either R_u or M_u, which depends on the environment where the U is currently staying. Usually, when a U is at home with her mobile device, she can have the M_u initiate the protocol to get the authorized-anonymous-ID $(r_1, D_A(H(r_1)))$, and then convey the authorized-

anonymous-ID to the R_u via a secure channel between the R_u and the M_u, which is protected by a symmetric crypto-system as mentioned in Section 2.1. In case that the mobile device already has a connection to the administrator, the rover can also initiate the registration procedure to get an ID in order to make the mobile user 'disappear' with the new ID (refer to re-confusing protocol in Section 3.3). Whoever initiates the protocol, the ID must be passed to the rover in order for the mobile device to get authenticated at access points.

3.2 Controlled Connection Protocol

Once an R obtains an ID, the mobile device can use the controlled connection protocol to get access to the wireless infrastructure via an access point. The procedure is the following. First, the R sends an access request by presenting its authorized-anonymous-ID (encrypted with the administrator's public key) to the C at the access point. Then the C forwards the message to its A for verification. The A decrypts the message, verifies the authenticity of the embedded authorized-anonymous-ID, signs the ID (if it is a valid one), encrypts the ID and the signature with the key shared by the C, and sends the encrypted message back to the C. Once the C receives the encrypted message from the A, it decrypts it and checks the signature signed by the A and sends an "*ack*" to the R if the signature is valid. Thereafter, the R and the C share the ID as a secret for packets authentication, and only successfully authenticated packets can get through the access point to the Internet. This protocol is outlined in Fig. 5.

3.3 Improvements

The basic protocols presented in Sections 3.1 and 3.2 can be improved by the following methods.

- **Re-confusion:**

  It is known that the longer an ID exists, the higher the chances of exposing the association between the ID and the corresponding mobile user. To mitigate this problem, we propose a method called "re-confusion", the objective of which is to generate a new

authorized-anonymous-ID to replace the old authorized-anonymous-ID. Fig. 6 outlines our protocol for the re-confusion method.

Specifically, the process of re-confusion works as below. First, an R sends the administrator a request (encrypted with the public key of the administrator) for a new authorized-anonymous-ID. Different from the registration protocol, in which a real identification (e.g., a public key certificate) is required to be presented, a request for a new authorized-anonymous-ID in re-confusion contains 1) one of the mobile user's current or previous authorized-anonymous-IDs, 2) a random number multiplied by a factor, which is blind or unknown to the administrator, and 3) a symmetric encryption key suggested for this communication session between the R and the A. After a successful verification of the presented ID, the A signs blind signature on the random number, encrypts it with the suggested key, and sends it back to the requesting rover R. The R decrypts the message from the A, removes the blind factor, and gets the new authorized-anonymous-ID. The nice feature of our re-confusion protocol is that any disclosure of the previous ID would not compromise the anonymity of the new ID.

- **Access Authorization Revocation:**

  It is not desirable from the administration perspective, that an authorized-anonymous-ID enables a mobile device to have an *eternal* right to access the infrastructure. Hence, an administration may want to have a function that can revoke or invalidate an issued authorized-anonymous-ID. One way to add this revocation function to our protocol family is that the administrator A periodically expires and changes its own keys for access authorization. The anonymous IDs signed by the revoked keys will no longer valid for authentication. But this solution has a drawback: the mobile users need to periodically update their anonymous IDs, which introduces much communication overhead if the keys of the administrator expire too fast. Another solution is to attach expiration time-stamp with the ID. However, the expiration time-stamp should not be unique to the mobile user; otherwise, the unique association between the expiration time-stamp and the ID, can reveal the identity of a mobile user.

- **Untraceable Routing Infrastructure:**

Frequent communication between a home computer and a mobile device could be another factor exposing the association between the mobile device and its stationary home. Untraceable routing infrastructure [11] can be used to erase the track at certain communication cost.

Remark 1 *A restriction on our protocols is that the standards of current wireless technologies, such as IEEE 802.11 and Bluetooth, require manufacturers to assign an identification number, i.e., MAC address, to every device. The MAC address is like an annoying tag attached to a mobile device, anytime and anywhere. The custom of assigning a number to each wireless communication device is adopted from numbering every network interface card (e.g., Ethernet card) for each stationary computer, where the location privacy does not matter. However, in a ubiquitous computing environment, such a practice exposes the ID of a mobile device at the MAC layer. An ideal way to remedy this is to replace the MAC address with the authorized-anonymous-ID. ID collision should not be a serious problem in this case and can be prevented in many ways, for instance, by adding a time stamp.*

4 Related Work

MobileIP [12] resembles the structure of our system. To support both mobility and privacy, these two systems need to interact, but they are essentially different in two senses. First, they serve different purposes: MobileIP is aimed at packet routing and forwarding, while our location information service/control system is targeted at providing location service under personal control. Second, they are implemented at different layers: MobileIP is used at the network layer, while our system is implemented at the application layer. As suggested in Remark 1, the authorized-anonymous-ID can replace the hardware MAC address, but there is no need to make any change to other layers except the application layer.

There are some efforts called 'privacy extension' to MobileIPv6 [13, 14]. The basic idea of these efforts is to replace the MAC address of mobile device with a random one, called temporal mobile identifier (TMI) [13] or pseudo-random interface identifier (PII) [14]. In these schemes, personal mobile location privacy control relies on either home administration,

or foreign administration, or both. Moreover, it is required for home administration to share some secrets with foreign administration in order to prevent eavesdroppers from having any knowledge about binding users' temporal identifiers and real identifiers. These efforts cannot make mobile location privacy completely controlled by a mobile user since the administration can associate any identifier (PII or TMI) with its corresponding real ID of the mobile user (or device).

Under our scheme, the dilemma arising from two seemingly conflicting expectations, security (or connection access control) and privacy (or location information confidentiality), is resolved by using an authorized-anonymous-ID created with a cryptographic technique – blind signature. The authorized-anonymous-IDs are used by mobile users as permission tokens for connection access controlled by the administration. On the other hand, the authorized-anonymous-IDs, embedded in the packets transmitted to access points would not reveal any information about the mobile users since the IDs being used are completely disassociated from the real IDs of the users.

Since we have noticed that efforts such as [13, 14] have been made to address the location privacy issue at a lower layer (e.g., IP layer) rather than at the application layer, it may be worth mentioning that according to our rationale study, a machine equipped with a lower layer technique may not be able to effectively achieve personal control over the location privacy, because anyhow the lower layer technique will depend on the operators of the infrastructures to hide the identity of a mobile user. Also, in contrast to our solution at the application layer, the solutions at the IP layer are even harder to deploy. A detailed justification can be found in the PUMA (Personal Ubiquitous Multi-Agent) project report [15].

5 Concluding Remarks

In this paper, we investigated the problem of protecting location privacy of mobile users in the setting of ubiquitous computing. We pointed out that location privacy protection is particularly challenging due to the different requirements imposed by the administration and

mobile users. To address this issue, we proposed an authorized-anonymous-ID based scheme. In our scheme, an authorized-anonymous-ID is created by the 'blind signature' technique and is used to replace the real ID of an authorized mobile device. With authorized-anonymous-IDs, we designed an architecture that is able to provide the mobile users with complete control over their location privacy while yet allowing the administration to authenticate the legitimate mobile users.

Our future work will focus on theoretical analysis of the security of this set of protocols. In addition, the system has been built on the Wireless-Andrew network, a WLAN covering the campus of Carnegie Mellon University, and we plan to generalize the protocols for heterogeneous networking environments (such as a hybrid of WLAN, PAN, and wide area network) to accommodate various networking technologies.

References

[1] M. Weiser, "Some computer science issues in ubiquitous computing," *Communication of The ACM,* July 1993.

[2] Q. He, B. Liu, A. Pennington, D. Siewiorek, P. Khosla, and Z. Su, "WaveGuard: secure location service for wireless andrew," *International Conference on Wireless Communications,* 2001.

[3] D. Chaum, "Blind signatures for untraceable payments," in *Proc. of Crypto'82,* 1982.

[4] H. Krawczyk, M. Bellare, and R. Canetti, "HMAC: keyed-hashing for message authentication," *IETF RFC 2104,* Feb. 1997.

[5] E. Brewer, R. Katz, Y. Chawathe, et al, "A Network Architecture for Heterogeneous Mobile Computing," *IEEE Personal Communication,* pp. 8–24, Oct. 1998.

[6] J. H. Saltzer, D. P. Reed, and D. Clark, "End-to-end arguments in system design," *ACM Transactions on Computer Systems,* pp. 277–288, Nov. 1984.

[7] D. N. Chorafas, "Agent technology handbook," McGraw Hill, 1997.

[8] F. Stajano and R. Anderson, "The resurrecting duckling: security issues for ad-hoc wireless networks," in *Proc. 7th International Workshop of Security Protocols,* 1999.

[9] M. Burnside, D. Clarke, T. Mills, A. Maywah, S. Dvadas, and R. Rivest, "Proxy-based security protocols in networked mobile devices," in *Proc. of ACM SAC,* 2002.

[10] C. Kaufman, R. Perlman, and M. Speciner, "Network Security: Private Communication in a Public World," 2nd edition, Prentice-Hall, 2002.

[11] M. Reed, P. Syverson, and D. Goldschlag, "Anonymous connections and onion routing," *IEEE J. Selected Areas in Commun.,* vol. 16, no. 4, pp. 482–494, May 1998.

[12] C. Perkins and D. Johnson, "Mobility support in IPv6," in *Proc. MobiCom,* 1996.

[13] C. Castelluccia and F. Dupont, "A simple privacy extension for mobile IPv6," IETF Internet Draft *Draft-Castellucia-MobileIP-Privacy,* Feb. 2001.

[14] A. Escudero, "Location privacy in IPv6 – tracking binding updates," in *Proc. of IDMS,* Lancaster, UK. Sept. 2001.

[15] Q. He, P. Khosla, and Z. Su, "A practical study on security of agent-based ubiquitous computing," in *Proc. AAMAS'02 Deception, Fraud, and Trust in Agent Societies workshop,* 2002.

Biography

Qi He is a project scientist at Carnegie Mellon University. His research interests lie in cryptography, data security, and mobile/wireless computing and applications. His recent research focuses on leveraging cryptographic methodology to construct "agent-based security infrastructure" to address security issues in ubiquitous computing lieu. He is a member of ACM and IEEE. He holds a BS degree in Mathematics, M.S. degrees in Computer Science (from Tsinghua University, Beijing China, in 1994, and University of Maryland, USA, in 1997, respectively).

Dapeng Wu received B.E. in Electrical Engineering from Huazhong University of Science and Technology, Wuhan, China, in 1990, M.E. in Electrical Engineering from Beijing University of Posts and Telecommunications, Beijing, China, in 1997, and Ph.D. in Electrical and Computer Engineering from Carnegie Mellon University, Pittsburgh, PA, in 2003. Since August 2003, he has been with Electrical and Computer Engineering Department at University of Florida, Gainesville, FL, as an Assistant Professor. His research interests are in the areas of networking, communications, multimedia, signal processing, and information and network security. Currently he is an associate editor for the IEEE Transactions on Vehicular Technology. Dr. Wu received the IEEE Circuits and Systems for Video Technology (CSVT) Transactions Best Paper Award for Year 2001.

Pradeep Khosla is currently the Philip and Marsha Dowd Professor in the College of Engineering and School of Computer Science at Carnegie Mellon University. He is also the Head of both Electrical and Computer Engineering Department and Information Networking Institute, and Founding Director of the CyLab at Carnegie Mellon. From January 1994 to August 1996 Professor Khosla served as a DARPA Program Manager in the Software and Intelligent Systems Technology Office (SISTO), Defense Sciences Office (DSO) and Tactical Technology Office (TTO) where he managed advanced research and development programs in Information Technology and Intelligent Systems.

Professor Khosla is a recipient of several awards including the ASEE 1999 George Westinghouse Award for Education, Siliconindia Leadership award for Excellence in Academics

and Technology in 2000, and the W. Wallace McDowell award from IEEE Computer Society in 2001. He is Fellow of Institute of Electrical and Electronics Engineers (IEEE) and of American Association of Artificial Intelligence (AAAI). He currently serves on editorial boards of IEEE Spectrum, and IEEE Security and Privacy, and was appointed in February 2003 to the National Research Council Board on Manufacturing and Engineering Design for a 3 year term. He also is a consultant to several companies and serves on the Advisory boards of venture capital firms and several startups. Professor Khosla's research has resulted in 3 books and more than 300 articles in journals, conferences, and book contributions.

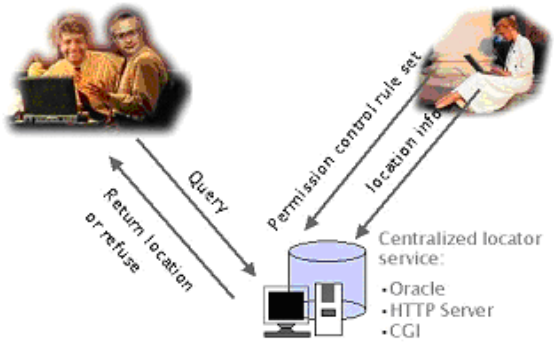

Figure 1: Architecture of WaveGuard

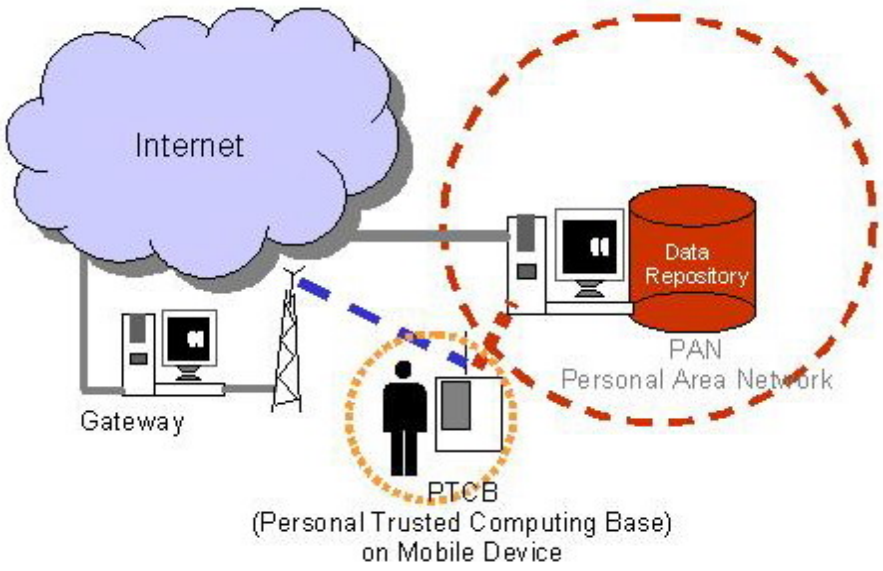

Figure 2: A sketch of ubiquitous computing

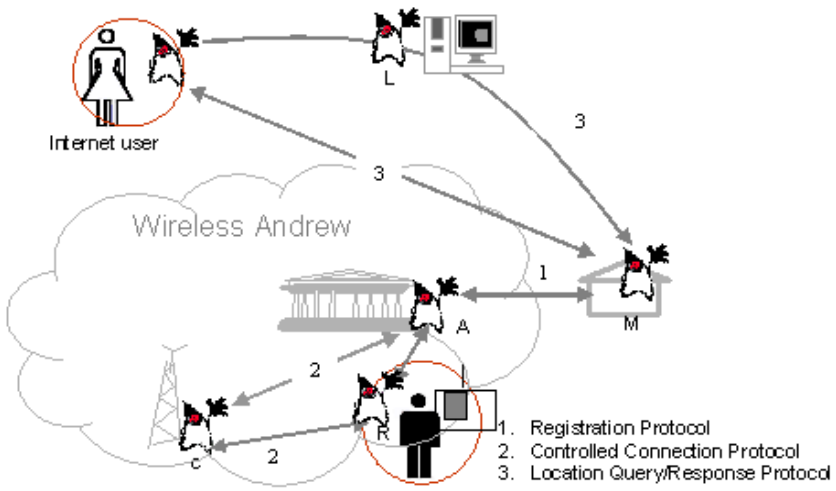

Figure 3: Agent-based system architecture

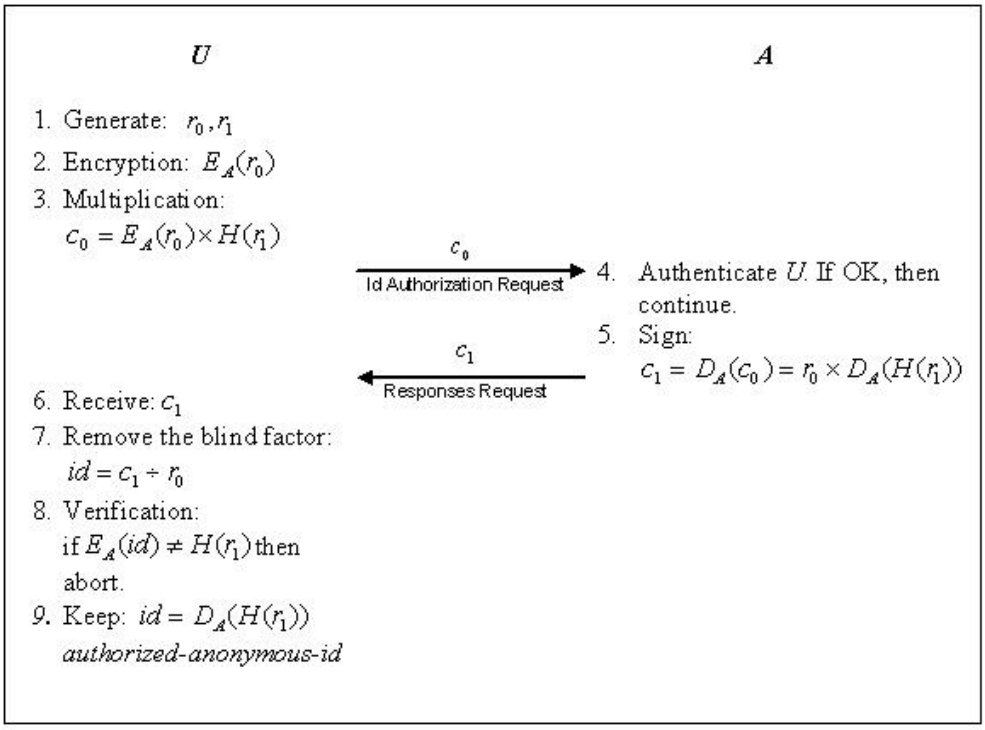

Figure 4: Registration protocol

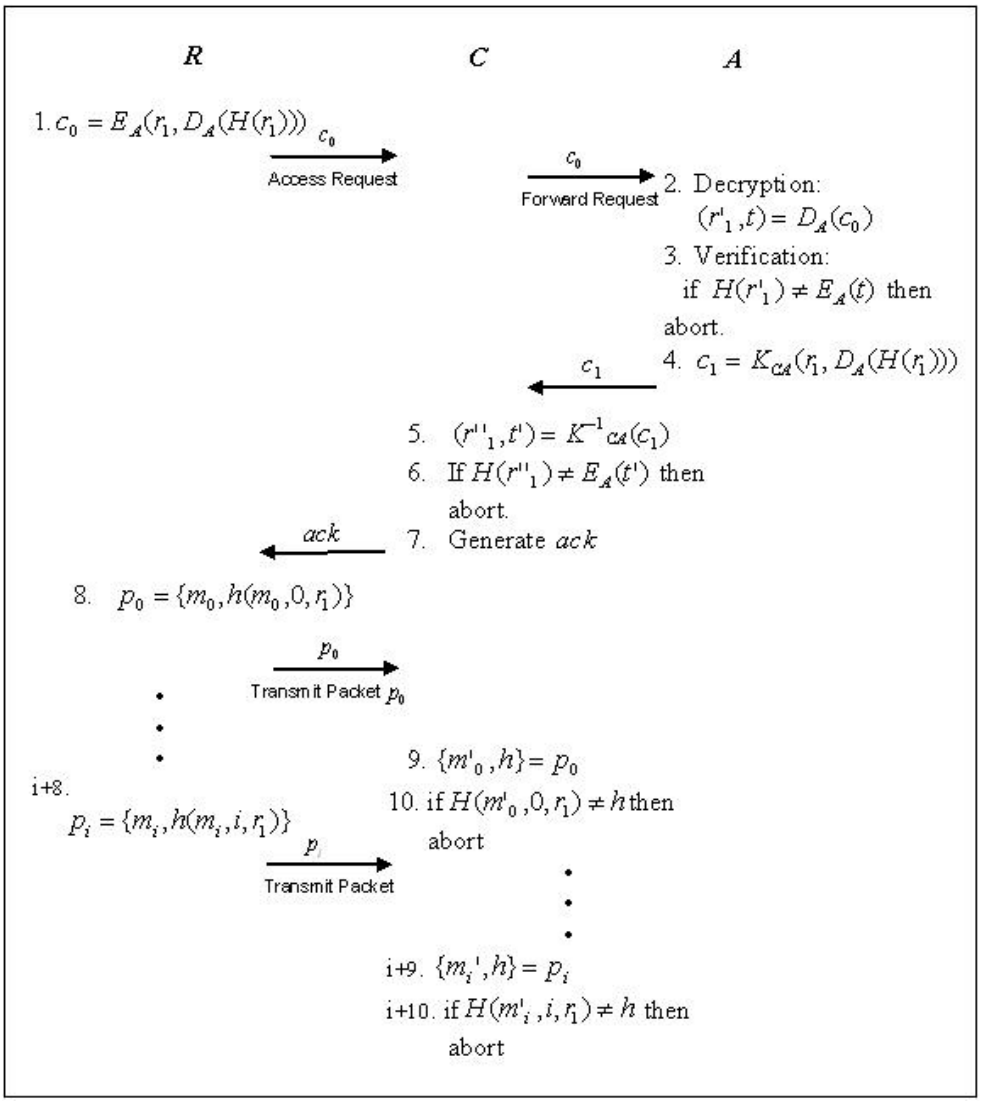

Figure 5: Controlled connection protocol

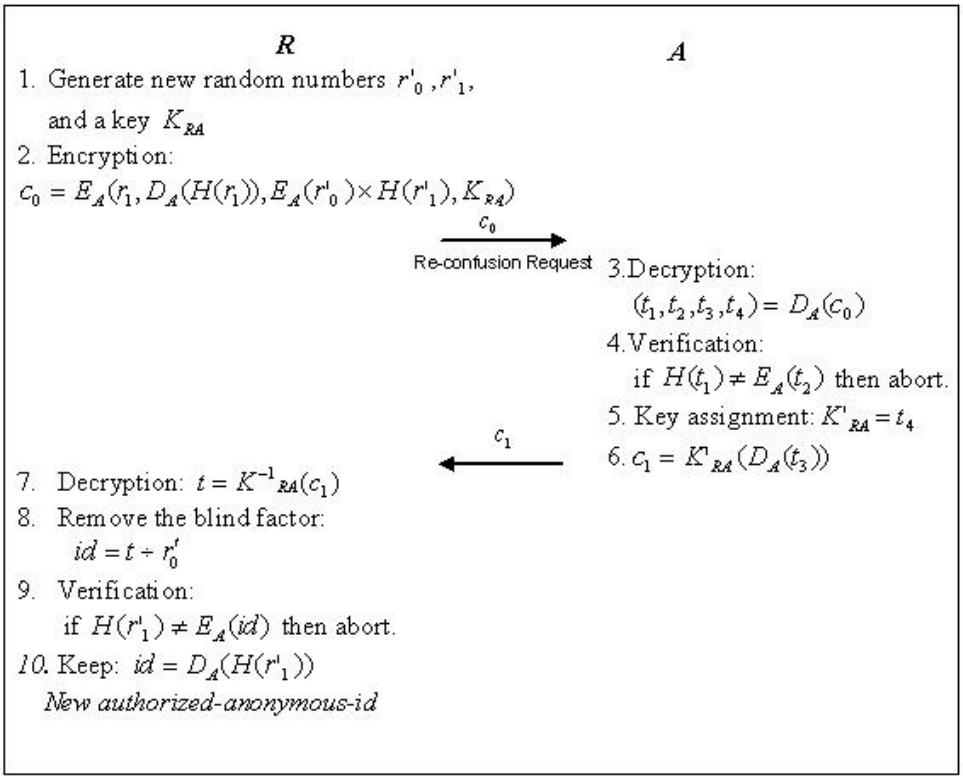

Figure 6: Re-confusion protocol