Secure Spaces: Location-based Secure Wireless Group Communication

Suman Banerjee *suman@cs.umd.edu*

Arunesh Mishra *arunesh@cs.umd.edu*

Department of Computer Science, University of Maryland, College Park, MD 20742, USA

We define "Secure Space" as an enclosed area within which wireless devices can participate in secure group communication. A device is able to join a secure space group by the virtue of its location within the enclosure. The devices communicate with each other using IEEE 802.11 wireless LAN or other similar wireless access technologies. There are two important aspects of this problem — (a) determining and authenticating the location of a wireless device at the granularity of a secure space, and (b) defining scalable mechanisms to (re)-distribute a common group key among the device inside the secure space, as new devices enter and existing devices leave the space. We solve the location determination and authentication problem using signal strength based techniques. Results from actual wireless experiments show the feasibility of this scheme. We leverage scalable solutions for secure group communication in other environments to propose a hybrid scheme for the key redistribution problem.

I. Introduction

Consider a business conference in a hotel environment. The various delegates in the conference are equipped with different wireless devices. Different groups of delegates meet in different conference rooms to discuss business plans. Our work defines an infrastructure which allows all and only the occupants of a given space (usually a room) to be able to securely communicate with each other within that space. Thus, our infrastructure prevents "wireless eavesdropping", i.e. data can be exchanged over the wireless securely by delegates inside the conference room, without being intercepted by unauthorized people (who are outside the room). We call this infrastructure, Secure Spaces.

To implement the Secure Spaces environment, we need to (1) determine and authenticate the location of the wireless device to within the Secure Space, and (2) scalably distribute a group key to all and only those wireless devices that are determined to be within this space to enable secure group communication. This allows us to decompose the problem into the following two subcomponents, which we describe next.

II. Location Determination and Authentication

We define a Location Determination and Authentication System (LDAS) using RF signal-strength based techniques. Our scheme requires the use of one or more trusted wireless devices (typically access points) in the infrastructure. The trusted devices periodically transmit *beacon* frames on the wireless channel, and the untrusted devices are authenticated if they can prove to the LDAS that they "correctly" received these frames. The definition of correct depends on the location being authenticated.

Before the authentication process is initiated, we create a *radio map* of the space. For each physical location in the space, the radio map tabulates the power with which beacons transmitted by the different trusted devices and with different transmission powers are received at that location. During the authentication process, each trusted device transmits the beacon frame using some randomly chosen transmission power. The source identifier information is suppressed in these beacon frames. Instead, each beacon is marked by an unique identifier, which allows the LDAS to infer the source of the beacon, and the power level with it was transmitted by the trusted device. This information is not available outside the LDAS.

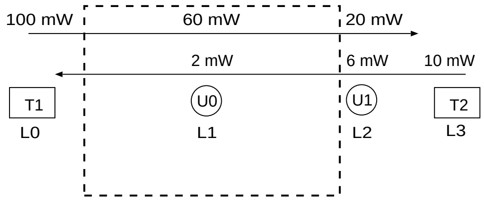

Figure 1: Simplified example of the LDAS in one dimension.

On receiving the beacon frames from all the trusted devices, the untrusted device is expected to present a *signal strength tuple* back to the LDAS. The tuple consists of the set of ⟨ *beacon identifier, received signal strength*⟩ pairs for all the beacons it received. The LDAS checks if the received signal strength value matches the corresponding value in the radio map, for each of the beacons, in which case the location is identified and considered authenticated. If the match fails, the authentication is considered a failure.

This is shown using a simple one-dimensional example in Figure 1. Consider the two trusted devices T_1 and T_2 that are trying to authenticate the location of the untrusted devices, U_0 and U_1. T_1 transmits a beacon frame, b_1, with some randomly chosen power value, say 100 mW. The signal gets attenuated over the medium and is received by U_0 with power 60 mW and by U_1 with power 20 mW. Similarly, T_2 transmits its beacon,

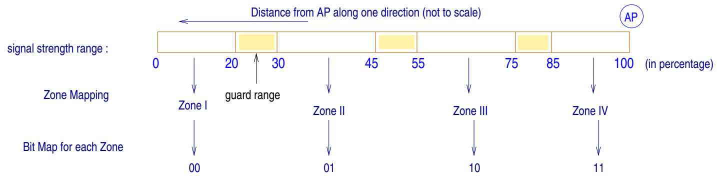

Figure 2: Mapping a zone to a bit-string for a trusted device.

b_2, with another randomly chosen power value, say 10 mW, which is received by U_0 with power 2 mW and by U_1 with power 6 mW. If U_0 and U_1 returns the signal-strength tuples as $\{\langle b_1, 60mW\rangle, \langle b_2, 2mW\rangle\}$ and $\{\langle b_1, 20mW\rangle, \langle b_2, 6mW\rangle\}$ respectively, then their locations are correctly determined and authenticated with respect to the radio map available at LDAS.

For U_1 to mislead the LDAS to believe that its location as L_1, it needs to return the signal strength tuple to be: $\{\langle b_1, 60mW\rangle, \langle b_2, 2mW\rangle\}$, i.e. the tuple which is correct for the location of U_0. However, U_1 is not aware as to which trusted device transmitted which beacon (this beacon source information is suppressed). Also, the trusted device transmits each beacon with a randomly chosen power value. This prevents U_1 from using any location-based inference scheme to evaluate the correct received signal strengths at any other position for the different beacons. The security of the random power LDAS is based upon the anonymity of the beacon source and the random choice of power value with which the beacon is transmitted.

In realistic scenarios, however, the signal strength measurements are never accurate due to channel fading, other sources of noise, and multipath effects. To mitigate the effect of such measurement inaccuracies, we partition the received signal strength values into a set of equivalence classes, or *zones*. Typically received signal strength at different rooms, in the business conference example, will fall in different zones for the same access points. Zones are separated by *guard ranges*. Such a coarse granularity of differentiation is sufficient in the Secure Spaces environment, since we are concerned in determining and authenticating location to the granularity of rooms.

An untrusted device infers a *location-specific authentication key* from the signal strength tuple as follows: The received signal strength of beacons from each access point corresponds to a zone, which in turn is mapped to a bit-string. This mapping is shown in Figure 2. By concatenating the bit-strings of different trusted devices in a deterministic sequence, the location-specific key is generated. For example, in Figure 1, the signal strength tuple at location L_0 maps to zones 3 and 1 respectively for the two access points. Therefore the generated key, using the mapping shown in Figure 2, is the string $10-00$. Clearly different rooms will have different location-specific authentication keys. The untrusted device authenticates its location to the LDAS by encrypting a well-known text (together with some randomly chosen value to prevent re-play attacks) using the location-specific authentication key and sending it to the LDAS server for verification. Our experimental data suggests that even by using a small set of trusted devices it is possible to distinguish between locations inside and outside such enclosed areas.

III. Secure Group Communication

Typical group communication systems rely on a *single* group key known to all and only the group members. Once this group key is securely distributed to all group members, secure messages can be exchanged by encrypting them with this key. The location-specific authentication key is used for location authentication and is not used for secure group communication. Instead, there is a single key server in the system that is responsible for generating *location-specific communication keys* for the secure spaces.

Each device authenticated to be in a secure space needs the corresponding location-specific communication key for group communication within that space. Each time a new device moves into or an existing device departs from a secure space, a new communication key needs to be distributed. All subsequent group communication in that secure space must use this new key. This is the process of *group re-keying*.

We leverage the existing of three different schemes for group re-keying; the exact choice of the correct scheme depends on the number of devices that are located within the secure space. The first scheme is called *Pair-wise key exchange*. In this simple solution, the key server maintains a pair-wise key with each of the devices in the secure space (established using protocols like Diffie-Hellman [2]). On each change to the membership in the secure space, the key server chooses a new communication key and distributes it to each existing member encrypted by the corresponding pair-wise key. This scheme incurs $O(N)$ overheads at the key server for storage, cryptographic operations, and communication. When the number of members at a secure space increases, we use other scalable mechanisms. The *Key Graphs* scheme [3] creates a hierarchy of keys to achieve scalability and incurs $O(\log N)$ overheads at the key server. The *Hierarchical clustering* scheme [1] creates a hierarchy of members and asymptotically incurs $O(1)$ overheads at the key server.

Therefore, there exists a clear tradeoff between the simplicity of the key distribution scheme and its scalability.

References

[1] S. Banerjee and B. Bhattacharjee. Scalable Secure Group Communication over IP Mulitcast. *JSAC Special Issue on Networked Group Communication*, 20(8), October 2002.

[2] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6), November 1976.

[3] C.K. Wong, M. Gouda, and S. Lam. Secure group communications using key graphs. *Proceedings of Sigcomm*, September 1998.