

Location Authentication Methods for Wireless Network Access Control

Lichun Bao

Computer Science Department, Donald Bren School of ICS
University of California, Irvine CA 92697, U.S.A.

Abstract—Location-based service provisioning is of great interests to wireless Internet service providers. However, the essential mechanism, location authentication, can easily become the target of network hackers for free-riding and attacks. We identify two aspects for improvements at the network providers to enforce location authentication for network access control — location-based key distribution and run-time location verification, and propose solutions to enforce network access control based on locations, which we refer to as LENA (Location-Enforced Network Access). First, we designed a location authentication and authorization protocol based on Diffie-Hellman algorithm, which securely authenticates the location claims of mobile wireless devices, and distributes shared keys for data encryption purposes. Secondly, we employ a mobility management protocol to guarantee that the mobile devices are physically at where they claim to be when they access the network. These two steps can separately enforce location based network access control, or be combined. LENA eliminates the dependence on expensive hardware devices in order to localize the mobile devices, and solves a couple of possible attacks to the system. The computational, communication, and the memory requirements are evaluated and validated using simulations.

Keywords: Location based access control, wireless LAN, security management, Diffie-Hellman, Personal AP.

I. INTRODUCTION

With the growing number of high speed wireless portable devices, wireless LAN (WLAN) systems based on IEEE 802.11 a/b/g are becoming the prevailing access technologies in the commercial markets. Network resource access control is among the top priorities for wireless Internet service providers (WISPs), and requires proper authentication architectures. One of the intuitive approaches to authentication was to use contextual knowledge. User identity-password or token-ticket based access control are the most popular approaches [35], [20], [25]. SecureID is a token-based authentication scheme for a user remotely logging into corporate networks using a combination of both a password and a random number token [34]. Kerberos is another widely used ticket-based network authentication protocol today [20]. It is designed to provide strong authentication for client/server applications based on the secret key cryptography, which is derived from the Needham-Schroeder key distribution protocol [25]. Likewise, the access control list (ACL) is commonly used for access control by modern operating systems [37]. Zhang *et al.* [42] proposed the use of location-based keys using identity based public-key cryptography (ID-PKC) [6], [7].

Although the contextual knowledge guarantees sufficient network access privileges, it inevitably introduces ahead-of-

time setup overhead and user involvements in the authentication process. In reality, some network accesses are allowed with less stringent requirements than provided by the contextual knowledge, such as those needed by location-based value-added services in service advertisements or product marketing, which only require geographic locations. On the other hand, such location-based authentication for network access control is of particular interests because it does not require pre-established user-agreement, key distribution, communication overheads. The Global Positioning System (GPS) is a perfect example for its simplicity in the architecture [13].

Location based access control has actually become one of the formal methods in network access control mechanisms [15]. Ardagna *et al.* presented an approach to formalize location-based access control into the generic access control architecture [4], in which an Access Control Broker relays the access request/response between the Network Client and the Network Service Provider. The location information was explicitly presented using cell ID, signal level, timestamp etc. information. Ray *et al.* proposed a formal method to describe the location and operation dependencies, and associate location information with security levels so as to control classified objects according to locations [31].

The Cricket system is a decentralized indoor location-support system that requires the combination of RF (radio-frequency) and ultrasonic signals in order to trace user locations and to provide location services to users and applications [28]. PAC is based on the Cricket system for location tracing, and adopts the INS/Twine [5] architecture for scalable resource discovery [24]. Sastry *et al.* described an Echo protocol to compute node location based on the round-trip latency of messages and ultrasonic signals in location computations [32]. They proposed the concept of *Region of Acceptance* in order to combat malicious location-provers from submitting location claims that overstate the true processing delay. Water *et al.* proposed a similar protocol for proving the location of tamper-resistant devices, based on the RF message exchanges [40]. Zhang *et al.* applied power adaptation mechanisms on multiple access points to verify mobile stations' location claims with the help of challenge-response handshakes [41].

In this paper, we study the scenarios where the locations are defined by areas, the coarse-grained location information, and provide the location-based access control using localization and protocol designs. In contrast to other research that relies on exact coordinates of mobile stations, our access privileges are granted to areas instead of specific points. Such consider-

ations are especially applicable in situations such as airport, Internet cafe, hotels where network access is granted within the premises.

Our solution is a location authentication and network access control protocol, called LENA (Location-Enforced Network Access). In LENA, the location areas are defined by the shared coverage of multiple wireless access points (APs). The fact that a mobile node is located at certain places is proved by the mobile node collecting and presenting all the key information from the corresponding access points. If sectorized antennas are available for deployment, we can further specify the desired shapes of the areas.

LENA uses the Diffie-Hellman algorithm to securely authenticate the location claims of mobile wireless users in the areas, then securely distribute the shared keys for data encryption purposes between each mobile node and access point pair. We enumerate possible attacks to the system and analyze their countermeasures. The computational, communication, and the memory requirement are evaluated, and further validated using simulations.

We are not the first to utilize location areas to control network access. Garg *et al.* acquired multiple patents that used wireless signal strength to derive location area information [14]. However, he defined the authorized access areas by the confinement of physical walls, not through APs' coverage. Our location areas are instead "soft", defined by the overlapping areas of multiple APs.

The rest of the paper is organized as follows. Section II provides an overview of the algorithms and protocols used by LENA. Section III specifies the network assumptions and the protocol operations of LENA using two mechanisms. We evaluate the efficiency and security features of LENA in Section IV. Section V concludes the paper.

II. BACKGROUND REVIEW

A. Personal AP Protocol

In WLAN systems based on IEEE 802.11 protocols and architecture, mobility management handles three planes of networking functionalities: data plane, control plane and management plane functions. In the data plane, the mobility management needs to guarantee minimum data packet loss during the mobility transitions; in the control plane, the mobility management has to quickly re-establish control states, such as MAC flow control parameters; in the management plane, the mobility management needs to allocate sufficient network resources and establish states for the new connections, such as creating authentication, association state information.

In [38], Wang *et al.* proposed a Personal AP protocol for mobility management in WLAN systems. In contrast to the other mobility management protocols which expedite the mobile stations' ReAssociation process for fast handoffs between WLAN access points [3], [8], [11], [10], [30], [33], Personal AP protocol replicates the complete association parameters between the pair of mobile stations (MSs) and access points (APs), and reinstate the association parameters at the target AP that is best-connected to the MS. The association parameters include state information such as the MS MAC address, AP

MAC address, data frame sequence number, MS association ID (AID), security keys etc. This way, the MSs perceive the newly connected AP as its old AP, and are totally unaware of the mobility management protocol that works in the WLAN backend.

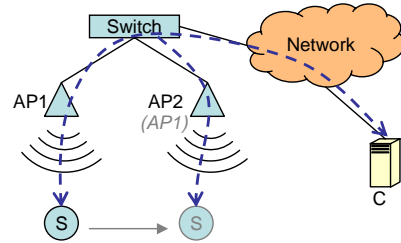


Fig. 1. A Simple Mobility Scenario in Personal AP System

Fig. 1 illustrates a simple mobility management scenario using Personal AP protocol, where a mobile station S is originally connected to a correspondent node C through an access point $AP1$. When the mobile S moves from the vicinity of $AP1$ and gets into a good signal coverage of access point $AP2$, the Personal AP protocol detects the signal quality change, and creates an image of the MS-AP association states between nodes S and $AP1$ on access point $AP2$, therefore keeping MAC layer management information intact and avoiding re-establishing the association states between the MS and the WLAN backend.

The wireless link quality between MSs and APs is monitored by the APs through measuring the RSSI (received signal strength indicator) values of the MSs and reporting the RSSI information to a mobility management controller in Personal AP protocol. When the signal strength between the current MS-AP association drops below certain level, the mobility management controller initiates the handoff operations, in which Personal AP protocol transfers the context information from the old AP to the new better-connected AP. Because Personal AP system shares similar context transfer operations as IEEE 802.11f IAPP [2], Personal AP protocol can be an extension over the existing IEEE standard.

Once the mobility context information is transferred, Personal AP updates layer-2 routing information in the switching table of the WLAN backend by the new AP broadcasting a dummy data frame with the MS's MAC address as the source address. This broadcast message updates the intermediate switches' learning table for layer-2 routing purposes.

The Personal AP system can easily integrate with other mobility management schemes. If a mobile station falls into sleep or does not have continuous and intensive traffic, the mobility support mechanism can fall back to other handoff mechanisms, such as the regular IEEE 802.11 or Mobile IP. In addition, Personal AP protocol enforces the requirement of IEEE 802.11 that an STA may have only one association with the infrastructure at any given time.

B. Diffie-Hellman Key Exchange

Diffie-Hellman key exchange scheme is used to agree on a shared key, K_{AB} , securely between two parties/nodes A and B [12], [23].

In Diffie-Hellman algorithm, two publicly-known numbers are distributed beforehand — a prime number p , and a generator g of the cyclic group Z_p^* . In order to derive a shared key between nodes A and B , node A chooses random private key value $X_A \in Z_{p-1}$, then computes a public key value $Y_A = g^{X_A} \bmod p$. Similarly, node B chooses random private key value $X_B \in Z_{p-1}$, and computes $Y_B = g^{X_B} \bmod p$. Nodes A and B now exchange the public keys Y_A and Y_B of each other explicitly, and derive the shared secret key using the modulo arithmetic as follows:

$$K_{AB} \equiv Y_A^{X_B} \equiv g^{X_A X_B} \equiv Y_B^{X_A} \equiv K_{BA} \pmod{p}. \quad (1)$$

Once the shared key is established, secure communication between two parties can be established using any symmetric key encryption scheme, like Data Encryption Standard (DES).

III. LOCATION-ENFORCED NETWORK ACCESS (LENA)

In this section, we first describe our network assumptions, then propose two schemes to enforce location-based access control. The first scheme uses the Diffie-Hellman key exchange algorithm for user location authentication, network-access authorization and data encrypting key distribution, which we call LENA-SK (LENA Using Security Keys). The second scheme utilizes the mobility management protocol, Personal AP, to physically guarantee the authenticity of the location claims, which we call LENA-PAP (LENA Using Personal AP Protocol).

A. Network Assumptions

In IEEE 802.11, the Basic Service Set (BSS) is the building block of a wireless system, and consists of a single AP and a number of MSs associated with the AP in a typical deployment. Multiple BSSs are interconnected with each other through a distribution system and form an Extended Service Set (ESS). The associated MSs communicate with each other or with Internet hosts through APs. The IEEE 802.11 standard [1] specifies two WLAN architectures, *infrastructure mode* and *ad-hoc mode*. We address the network access control problem in infrastructure-based WLAN systems.

For location based access control purpose, we define the *location group* as a set of select APs, whose wireless coverage shares the *access-granted area*. The location groups that an AP belongs to are designated by the network administrators or an automated bootstrapping process when the WLAN system is initially designed and deployed. Furthermore, the access-granted areas can be custom-made into special shapes according to customer requirements using directional antennas by adjusting the angle and distance of the signal propagation [27].

In Fig. 2 illustrates two access-granted areas as defined by the shaded areas of two AP location groups $G_1 = \{AP_1, AP_2\}$ and $G_2 = \{AP_3, AP_4\}$, where the directional antenna of each access point spreads 90° .

We assume that APs operate in the same frequency channel, and that mobile stations have sufficient computational and communication capacities to carry out the simple cryptographic operations required in LENA.

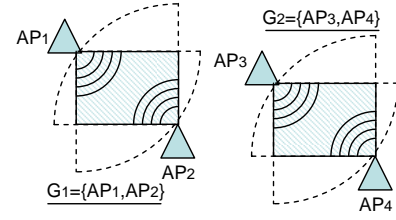


Fig. 2. Defining Access-Granted Network Areas.

B. LENA-SK: LENA Using Security Keys

The LENA-SK architecture includes the three elements – mobile stations (MSs), access points (APs) and a key server (KS). The key server is the central point of control in the location-based access control process, responsible for the key exchange and location group management. For convenience, the key server also hosts the access controller module.

In LENA-SK, the key server creates a private key for each AP in the location groups, and distributes the corresponding public key to each AP using the Diffie-Hellman algorithm. The APs broadcast their public keys in their beacon messages, which can be collected by mobile stations in the network. If the mobile station is located within a access-granted area, it can gather all the public keys of the APs in the corresponding location group, and therefore derive a shared secret using a modified Diffie-Hellman algorithm. Then, the shared secret can be used to authenticate the mobile station's location claims.

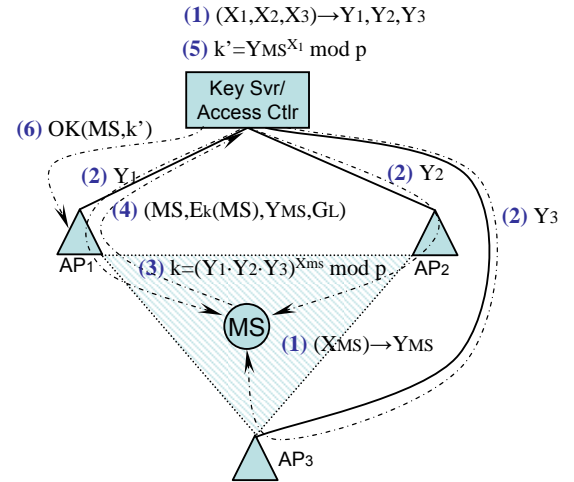


Fig. 3. Key Distribution for Location Group $G_L = AP_1, AP_2, AP_3$ in LENA-SK.

Fig. 3 shows an example WLAN system to illustrate LENA-SK protocol operations. In particular, the mobile station MS is located in the access-granted area confined by the location group $G_L = AP_1, AP_2, AP_3$. The key server KS connects to each AP by *low-latency* and *secure* connections, provided by the infrastructure networks. The LENA-SK operation steps are marked by numbers, and the message flows are indicated by arrows. For simplicity, we omitted the location group descriptor in all of the messages in Fig. 3.

We describe LENA-SK protocol operations in two phases according to Fig. 3: the authentication phase in steps (1)-(5),

and the key generation phase in step (6).

1) *LENA-SK Authentication Phase:*

(1) The key server generates three private keys $\{X_1, X_2, X_3\}$, and derives the corresponding public keys $\{Y_1, Y_2, Y_3\}$ using the Diffie-Hellman algorithm for the APs in location group $G_L = \{AP_1, AP_2, AP_3\}$, respectively. The public key Y_i is called the *location key* of the corresponding AP i . The private keys of the location keys are kept as secrets by the key server. The location keys are then periodically generated and redistributed to the APs. Similarly, the mobile station MS also generate its own private/public key pair X_{MS}/Y_{MS} .

(2) After receiving the location keys, the APs broadcast these keys within their wireless cell or BSS (basic service set) via their beacon messages. When a mobile station is located within the access-granted areas, the station can listen to the channel and gather all location keys of the location group.

As shown in Step (2) of Fig. 3, the MS collects the public keys $\{Y_1, Y_2, Y_3\}$ of the location group $G_L = \{AP_1, AP_2, AP_3\}$.

(3) The MS derives a location claim key k by multiplying all the location keys from the APs of the location group G_L , then raising the product to the power of X_{MS} using modulo arithmetic, which gives the location claim key k as

$$k = (Y_1 \cdot Y_2 \cdot Y_3)^{X_{MS}} \equiv g^{(X_1+X_2+X_3) \cdot X_{MS}} \pmod{p}.$$

Such computation is similar to the shared key computation in the Diffie-Hellman algorithm, but with a little complication to the base. Such scheme first appeared similarly in [36]. X_{MS} is the private key kept by the mobile station MS .

(4) After deriving the location claim key k , the MS composes the location claim with a four-element tuple $(MS, E_k(MS), Y_{MS}, G_L)$, which includes the MS identifier MS , the encrypted mobile station ID $E_k(MS)$ using the location claim key k , the current MS public key Y_{MS} derived from X_{MS} , and the location group descriptor G_L . The location claim is sent to the key server via the currently contacted or associated access point, which is AP_1 in Fig. 3.

The purpose of sending MS and its encrypted form $E_k(MS)$ is to show the key server that the MS has derived the location claim key, and can encrypt the plaintext using the key. A more complicated location claim is to include the BSS time stamp and location group indicator G_L in the encrypted message so as to defend against the message-replay attack.

(5) The key server exams the location claim of the MS by deriving the same location claim key k . According to the location claim tuple, the key server first retrieves the private keys $\{X_1, X_2, X_3\}$ of the location group G_L , which were generated in Step (1) originally. Then the key server KS computes k using

$$k = Y_{MS}^{X_1+X_2+X_3} \equiv g^{X_{MS} \cdot (X_1+X_2+X_3)} \pmod{p},$$

and encrypts MS using the key k . If the result is the same as $E_k(MS)$, the key server authenticates that the MS has received the location keys of the location group G_L , and is located in the corresponding access-granted area. That is, the MS location claim is authenticated. Otherwise, the location claim is invalid, and data packets from and to the MS will be blocked in the future.

2) *LENA-SK Key Generation Phase:*

(6) If the MS location claim is authentic, the key server will generate the shared key k' for encrypting the AP- MS communication link by again using the Diffie-Hellman algorithm. The shared key k' between MS and AP_1 in Fig. 3 is

$$k' = Y_{MS}^{X_1} \equiv g^{X_{MS} \cdot X_1} \pmod{p},$$

in which, the public key belongs to the MS , and the private key belongs to the associated AP of the MS . The associated AP can be easily derived from whoever forwarded the location claim, or be explicitly indicated in location claim messages, which was omitted in Fig. 3. Afterward, the key server directly sends the key k' to AP_1 , along with an OK message for the AP to communicate with MS .

Similarly, the MS would have derived the same key k' from its collected key information. In Step (3) of Fig. 3, after MS receives the three location keys $\{Y_1, Y_2, Y_3\}$ from the APs, the key k' is derived by

$$k' = Y_1^{X_{MS}} \equiv g^{X_1 \cdot X_{MS}} \pmod{p}.$$

Therefore, the MS and its corresponding AP can use the symmetric key k' for secure data communication later.

3) *Implementation Issues:*

a) *Key Renewal::* Although the fact that an MS gathers all the location keys of a location group proves that the MS is located with the corresponding access-granted areas, it is still possible that the MS walks out of the access-granted area, but is still able to communicate with the associated AP. In this case, the key server has no means to detect the errand.

Therefore, we improve the location authentication by renewing the location keys of the location groups periodically, thus forcing the MS s to re-authenticate themselves with the key server, and derive new shared keys for data communication purpose. For instance, when we implement this renewal mechanism in our simulations for LENA-SK evaluation purposes, we set the key renewal period to 5 seconds. If a mobile cannot re-authenticate itself with 1 seconds after the key renewal, the mobile will no longer be able to send data packets through its associated APs.

b) *Sybil Attack::* One of the practical security vulnerabilities in LENA-SK is due to the Sybil attack [13], [26], in which an adversary impersonates multiple network entities by assuming their identities. In the LENA-SK system, Sybil attack can be staged by a malicious MS impersonating an AP (Rogue AP) of a location group by broadcasting bogus location keys as if it were the legitimate access point, henceforth preventing MS s to acquire legitimate keys and access the networks.

LENA-SK can be easily extended to resist the Sybil attacks by requiring the APs to include a PKI certificate in the public key broadcast messages, and asking MSs to authenticate the APs. Assuming that the mobile stations have sufficient computational and communication capacities, the public keys of a location group can be easily verified by the MSs. However, for simplicity in LENA-SK, we have not provided such authentication mechanisms.

c) *Bootstrapping*:: The initialization of LENA-SK system includes several steps.

- 1) The key server and the access points need to recognize each other by sending HELLO messages through multicast packets. Because LENA addresses the network access control issues, LENA-related messages are carried within data link layer packets, such as Ethernet dataframes, and WiFi dataframes.
- 2) The key server distributes location group membership and security key information to the APs, as well as periodically updates the key information. When APs receive their keys, the keys are broadcast to the WLAN networks in Beacon messages.
- 3) When a new mobile station starts to access the network by associating with an AP, certain management data frames from the mobile station are allowed to go through the network so as to pass the security information of the mobile station to the network. However, further data communication depends on whether the mobile station can collect all the security keys and present the secret key to the key server correctly. Security information from the mobile station is attached to the periodic ReAssociation Request dataframes.
- 4) The key server maintains a table of authenticated mobile stations. If a mobile station is not authenticated through LENA-SK, all the data packets from and to the mobile station are dropped at the proper network switches or routers.

C. LENA-PAP: LENA Using Personal AP Protocol

1) *The Wormhole Attack*: LENA-SK provides a key-based location claim authentication and key distribution mechanism for location based access control. However, another major type of attacks, the *wormhole attack*, is still possible in LENA-SK systems. The simplest wormhole attack is usually staged by two colluding attackers, one of which intercepts the traffic on one side of the network, and tunnels the packets to the other attacker for replaying on another side of the network. The wormhole attack is very difficult to detect, since it can be launched without compromising any host, or attacking the integrity and authenticity of the protocols [19], [17], [18].

In the LENA-SK system, wormhole attackers can forge legitimate location claims by gathering the location keys from different points of the network, even though none of the locations is authorized to access the network.

Fig. 4 shows that two mobile stations MS_1 and MS_2 can collect the two location keys of a location group $G_1 = \{AP_1, AP_2\}$ by exchanging the missing keys of each other,

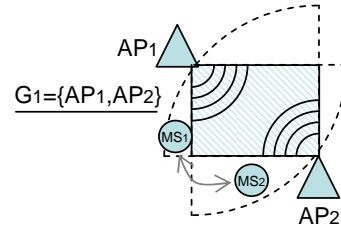


Fig. 4. Wormhole Attack to LENA-SK.

and successful access the network through the corresponding AP visible to each MS. It is also possible that an MS quickly moves between the coverage areas of the APs in a location group, thereby gathering all the location keys for location authenticating purposes.

In light of such attacks to LENA-SK, we implement another layer of location enforced network access control by requiring each access-granted mobile station to communicate with each and every access point of the location group. The iterative association with different APs can be achieved by the key server instructing the currently associated AP to explicitly disassociate with the MS, and disallow the MS to associate with the same AP again shortly after. Such policy forces the MS to connect with all the APs of the location group. However, association-based implementation to enforce physical location authentication may cause excessive control overhead, and could interrupt on-going communication sessions of the MS unexpectedly. Therefore, seamless mechanisms are desirable to make such scheme work. We propose to utilize aforementioned Personal AP protocol [38] to achieve the seamless switching between APs of a location group. We call this enhanced LENA-SK with Personal AP protocol as LENA-PAP.

2) *LENA Assisted by Personal AP Protocol*: In LENA-PAP, the transferal of MS-AP connection contexts between APs happens periodically, in contrast to the original application of Personal AP protocol where mobility management was triggered by MS's signal quality changes at the APs. The context transferal is scheduled by the access controller located on the key server, such that the MS-AP connection reinstatement iterates between the APs of the corresponding location group in the access-granted area.

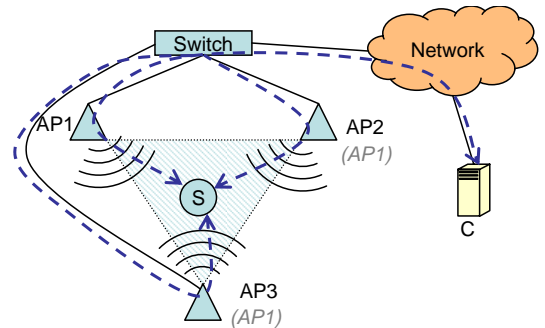


Fig. 5. Communication Pattern to Enforce Location-based Network Access through Personal AP Protocol.

Fig. 5 illustrates a network access control scenario using LENA-PAP, in which a mobile station S communicates with

a correspondent node C through the WLAN systems in an access-granted area, defined by location group $G_L = AP_1, AP_2, AP_3$. Using Personal AP mobility management protocol, the LENA-PAP access controller periodically moves node S - AP_1 association context among the APs of location group G_L so that APs AP_2 and AP_3 appear as AP_1 to node S , and the three APs take turns to forward data packets between nodes S and C . The packet flows that are forwarded by the APs are indicated by the dashed lines.

Personal AP protocol guarantees that the mobility context switching between the APs is invisible to mobile station S , and that the mobile station can communicate through the WLAN system if and only if the mobile station is located within the access-granted area.

In LENA-PAP, the security key of each AP in location groups is distributed the same as LENA-SK, and the mobile stations authenticate themselves to the key server whenever the AP security keys are updated.

IV. EVALUATIONS

A. Efficiency Estimation

LENA-SK and LENA-PAP are two orthogonal access control mechanisms that can work hand-in-hand. LENA-SK distributes security key information to the APs and MSs, and collects authentication information from the MSs, while LENA-PAP provides a physical means to guarantee the locations of the MSs using Personal AP mobility management protocol, and enhances LENA-SK in face of wormhole attacks. In addition, LENA-SK also generates security key information for data encryption purposes.

Neither of LENA-SK and LENA-PAP requires special hardware such as GPS or ultrasonic devices for localization purposes, therefore providing low-cost efficient way to location-based access control operations.

As far as we can see, the overhead of operating LENA protocols comes from the storage, computation and communication complexities. With regard to the storage complexity, we consider the three elements of a typical access controlled WLAN systems.

- The *key server* is required to store all the private keys of the APs in the WLAN system for the Diffie-Hellman algorithm computations, as well as the location group information for access control purposes. Using the private keys and the location group information, the key server can derive all other information, such as the location keys of APs and location claim keys. Therefore, the space requirement for the key server is linear to the numbers of APs and location groups in the WLAN system.
- Each AP is required to store *only one* public key, regardless of how many location groups the AP is in. Furthermore, each AP stores the shared keys and association states between the AP and their associated MSs. Therefore, the storage requirement for an AP is constant for its own public key, and linear to the number of MSs within an access-granted area.
- The MSs are required to store the public keys of their respective location groups, and the shared keys between

themselves and their associated APs. Therefore, the memory space requirement for each MS is linear to the size of the location group that the MS belongs to.

With regard to the computation complexity in LENA-SK and LENA-PAP, APs require no additional computations other than their normal 802.11 functions. However, the *key server* and the *access controller* modules are required to generate the public keys for the APs, authenticate each MS of the WLAN system and schedule Personal AP mobility context transfers. Therefore, the computation task increases linearly with the number of APs and MSs in the system. The MSs has constant computation overhead in each location group.

With regard to the communication complexity, the complete LENA-SK protocol operations involve six steps as illustrated in Fig. 3, in which case four messages went through the wireless interfaces, and five messages through the wired infrastructure network for authenticating the particular single MS; and LENA-PAP requires coordination overhead when the access controller schedules mobility context transfers over the wired LANs. Therefore, the communication overhead is linear to the total number of MSs and APs in each round of the basic LENA-SK and LENA-PAP operations. Over the air, because that the public keys for the APs can be broadcast piggybacked with 802.11 Beacon messages of the corresponding APs and that the MSs can send back their location claims piggybacked with 802.11 ReAssociation messages, the communication overhead is negligible over the air in WLAN systems.

Moreover, LENA-SK and LENA-PAP reduce the computation and communication overhead as compared with previous systems [21], [22], [9], [16], because LENA-SK adopts the Diffie-Hellman key distribution protocol, and does not require any pre-deployment phase for location authentication and key generation purposes, while LENA-PAP only involve control overhead on the wired side of the network.

B. Experimental Performance

In order to evaluate the effectiveness of LENA mechanisms in more practical scenarios, we implemented LENA-SK and LENA-PAP in NCTUns v4.0 [39], which was produced by SimReal Inc.. The reason what we chose NCTUns v4.0 was that it provides comprehensive and realistic simulations of IEEE 802.11 standards and other networking protocols. The essential network management functions complies with the standards to the fullest extend, such as WLAN channel estimation, probing, association, disassociation, re-association procedures, which were mostly unavailable in other simulators, such as NS2[29]. In addition, NCTUns v4.0 directly integrates with existing command line programs, such as FTP, HTTP applications, so that the simulator evaluates real application performance in its simulated networks.

Fig. 6 illustrates our simulated scenario, in which three APs, nodes 1, 2, 3, form a location group $\{AP_1, AP_2, AP_3\}$, and the access-granted area is defined by the triangular area marked with a random pattern. The key server and the access controller modules run on the switch, node 4, in Fig. 6. All wireless links operate at 11 Mbps data rate.

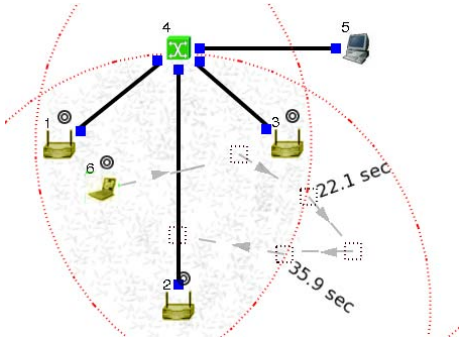


Fig. 6. Simulation Setup

The LENA-SK protocol starts with the key server identifying the APs, which form the location group $\{AP_1, AP_2, AP_3\}$. Afterward, the key server at the switch periodically generates and distributes individual keys $\{Y_1, Y_2, Y_3\}$ to the corresponding APs, which in turn broadcast the keys in their beacon messages. In IEEE 802.11, the beacon period is 100 ms by default, thus guarantees prompt delivery of the keys to the MS in the access-granted areas. We set the location key refresh period to 5 seconds on the key server. The location claims are carried in 802.11 ReAssociation messages sent by the MSs every second. In case of LENA-PAP which uses Personal AP mobility management protocol, we set the iterative connection context transfer interval to 1 second. That is, the connection between a mobile station and an AP will be transferred to a new AP every second.

In order to test the impact of LENA mechanisms to data traffic, we simulated two traffic patterns — one TCP stream and one CBR stream, respectively, both are directed from the MS (node 6) to the fixed host (node 5) in Fig. 6. Furthermore, we created a mobility pattern such that there are two critical points in the simulations — the MS moves out of the access-granted area at 22.1s, and comes back into the area at 35.9s. For comparison purposes, the data traffic simulations were carried out in three settings: the first setting has no access control, the second with LENA-SK implemented, and the third with LENA-PAP enforced, respectively.

As long as the mobile stations are granted network access, access control mechanisms have no impacts on the mobile stations' traffic characteristics, such as packet collisions, delay and network throughput, and secondly, because access control mechanisms are only meant for network access purpose alone, we do not evaluate the data packet loss, packet delay aspects, except for the data throughput.

Fig. 7 shows the throughput changes of the TCP connection between nodes 6 and 5 when the network operates with and without LENA enforcement, respectively, when the mobile stations move into and out of the access granted areas. As shown in Fig. 7, all TCP streams with and without LENA enforcement were disrupted at time 22.1s because the MS lost the WiFi connection with the originally associated AP (node 1) in Fig. 6. However, the TCP stream without network access control mechanism came back quickly to the normal throughput after associating with another AP (node 3), whereas the TCP streams with LENA-SK and LENA-PAP enforcement were not able to recover their TCP throughput until the MS

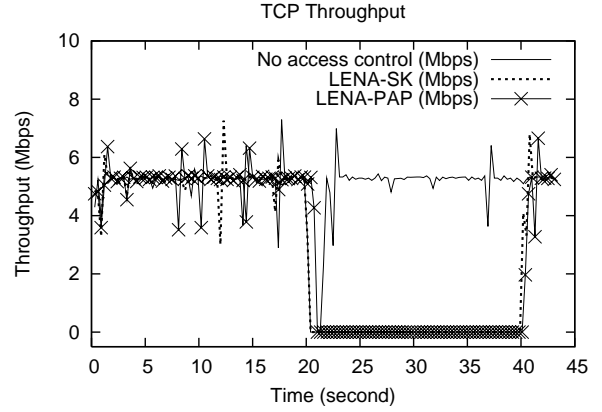


Fig. 7. TCP Throughput with or without Access Control Mechanisms.

returned to the access-granted area at time 35.9s, at which point both TCP streams in LENA-SK and LENA-PAP were restored to the original throughput. Note that the TCP streams with LENA-SK and LENA-PAP had a 4-second lag before recovering to its normal throughput because of TCP congestion control and flow control timing mechanisms.

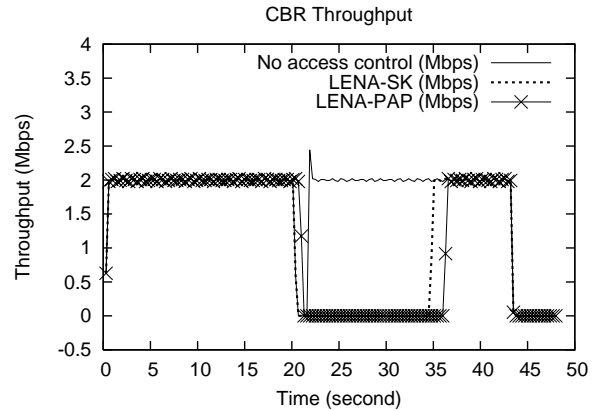


Fig. 8. CBR Throughput with or without Access Control.

The second set of traffic simulations were to carry out a CBR transmission from the MS to the fixed host in the same setup as shown in Fig. 6. The CBR traffic was generated at 2 Mbps data rate. Fig. 8 shows the throughput of the CBR connection with and without LENA enforcement. We can see that the CBR throughput was disrupted at time 22s, but came back within 1 second in case of the network that has no access control mechanism. In case the network implements either of LENA-SK and LENA-PAP access control protocols, the CBR traffic came back up almost immediately to 2 Mbps once the MS got back to the access-granted area at time 35.9s.

Interestingly, both LENA-SK and LENA-PAP performed similar with regard to both TCP and CBR throughput, except for about 1 second lag during their recovery phases after the mobile station came back to the access-granted area. This proves that LENA-SK and LENA-PAP achieve the same access control goal, although they are different in terms of protocol operations.

V. CONCLUSION

We have described and evaluated LENA, a secure Location-Enforced Network Access control based on the new location group and location key concepts. LENA is implemented in two schemes, one of which is called LENA-SK based on security key exchange using the Diffie-Hellman algorithm, and the other is called LENA-PAP, which includes a novel utilization of the Personal AP mobility management protocol to improve to the security features of LENA-SK. Compared to previous systems, LENA provides the minimum communication and computational overhead, thus is a promising technique for network access control based on coarse-grain location information. Nonetheless, LENA opens up several practical deployment issues to be addressed in our future research, such as scalability, stronger authentication based on PKI etc.

REFERENCES

- [1] IEEE Std 802.11. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Technical report, IEEE, Jul. 1997.
- [2] IEEE Std 802.11f. IEEE Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation. Technical report, IEEE, Jul. 2003.
- [3] I.F. Akyildiz, J. Xie, and S. Mohanty. A survey of mobility management in next-generation all-IP-based wireless systems. In *Wireless Communications, IEEE (See also IEEE Personal Communications)*, pages 16–28, Aug. 2004.
- [4] C.A. Ardagna, M. Cremonini, E. Damiani, S. De Capitani di Vimercati, and P. Samarati. Supporting Location-Based Conditions in Access Control Policies. In *Proc. of the ACM Symposium on Information, Computer and Communications Security (ASIACCS)*, Taipei, Taiwan, Mar. 21-24 2006.
- [5] M. Balazinska, H. Balakrishnan, and D. Karger. INS/Twine: A Scalable Peer-to-Peer Architecture for Intentional Resource Discovery. In *Proc. of the First International Conference on Pervasive Computing*, pages 32–43, Aug. 2002.
- [6] P. S. L. M. Barreto, H. Kim, B. Bynn, and M. Scott. Efficient Algorithms for Pairing-Based Cryptosystems. *Advances in Cryptology - Crypto 2002*, Lecture Notes on Computer Science 2442:354–368, 2002.
- [7] D. Boneh and M. Franklin. Identify-based encryption from the weil-pairing. *SIAM Journal of Computing*, 32(3):586–615, 2003.
- [8] A. T. Campbell, J. Gomez, S. Kim, Z. Turanyi, C-Y. Wan, and A. Valko. Comparison of IP Micro-Mobility Protocols. *IEEE Wireless Communications Magazine*, 9(1), Feb. 2002.
- [9] S. Capkun, L. Buttyan, and J. Hubaux. SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks. In *Proc. of SASN 2003*, Virginia, Oct. 2003.
- [10] S. Das, A Mcauley, A Dutta, A. Misra, and S K Das. IDMP: An Intra-Domain Mobility Management Protocol for Next Generation Wireless Networks. *IEEE Wireless Communications Magazine (Special Issue on Mobile and Wireless Internet: Architecture and Protocols)*, 9(3):38–45, Jun. 2002.
- [11] S. Das, A. Misra, P. Agrawal, and S.K. Das. TeleMIP: Telecommunications-Enhanced Mobile IP Architecture for Fast Intradomain Mobility. *IEEE Personal Communications*, Aug. 2000.
- [12] W. Diffie and M. Hellman. New Directions in Cryptography. *IEEE Transaction on Information Theory*, 22:644–654, Nov. 1976.
- [13] J. R. Douceur. The Sybil attack. In *First International Workshop on Peer-to-Peer Systems (IPTPS)*, Mar. 2002.
- [14] S. Garg, M. Kappes, and M. Mani. Location-Based Access Control for Wireless Local Area Networks. Technical report, AVAYA TECHNOLOGY CORP, 2003. CA20032489698; WO2004004278 (A1); US2004203748 (A1); EP1527583 (A0); AU2003234539 (A1).
- [15] C.A. Gunter, M. J. May, and S.G. Stubblebine. A Formal Privacy System and its Application to Location Based Services. In *Proceedings of the Workshop on Privacy Enhancing Technologies*, May 2004.
- [16] U. Hengartner and P. Steenkiste. Implementing access control to people location information. In *Proceedings of 9th ACM Symposium on Access Control Models and Technologies (SACMAT)*, pages 11–20, Yorktown Heights, NY, Jun. 2004.
- [17] Y. Hu, A. Perrig, and D. Johnson. Packet Leashes: A Defense Against Wormhole Attacks in Wireless Ad Hoc Networks. In *Proc. of INFOCOM*, San Francisco, CA, USA, Apr. 2003.
- [18] Y. Hu, A. Perrig, and D. Johnson. Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols. In *Proc. of ACM Workshop on Wireless Security (WISE 2003)*, Oct. 2003.
- [19] I. Khalil, S. Bagchi, and N. B. Shroff. LITEWOP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Network. In *The International Conference on Dependable Systems and Networks (DSN)*, Yokohama, Japan, 2005.
- [20] J. Kohl and B. C. Neuman. RFC 1510 - The Kerberos Network Authentication Service (Version 5). Technical report, IETF, Sep. 1993.
- [21] L. Lazos and R. Poovendran. SeRLoc: Secure Range-Independent Localization for Wireless Sensor Networks. In *2004 ACM workshop on Wireless security (ACM WiSe 2004)*, Philadelphia, PA, 2004.
- [22] N. Malhotra, M. Krasniewski, C. Yang, S. Bagchi, and W. Chappell. Location Estimation in Ad-Hoc Networks with Directional Antennas. In *25th International Conference on Distributed Computing Systems (ICDCS)*, 2005.
- [23] R. C. Merkle. Secure Communication over an Insecure Channel. *Communication of ACM*, 21:294–99, Apr. 1978.
- [24] N. Michalakis. PAC: Location Aware Access Control for Pervasive Computing Environments. Technical report, MIT Laboratory of Computer Science, 200 Technology Square, Cambridge MA, 02139 USA, 2002.
- [25] R. M. Needham and M. D. Schroeder. Using Encryption for Authentication in Large Networks of Computers. In *Communication of the ACM*, pages 993–999, Dec. 1978.
- [26] J. Newsome, E. Shi, D. Song, and A. Perrig. The Sybil Attack in Sensor Networks: Analysis and Defenses. In *Proc. of IPSN 2004*, Berkeley, CA, Apr. 2004.
- [27] D. M. Pozar and D. H. Schaubert. *Microstrip Antennas: The Analysis and Design of Microstrip Antennas and Arrays*. Wiley-IEEE Press, May 1995.
- [28] N. B. Priyantha, A. Chakraborty, and H. Balakrishnan. The Cricket Location-Support System. In *6th ACM International Conference, Mobile Computing and Networking (MOBICOM)*, Aug. 2000.
- [29] VINT Project. The Network Simulator - ns-2. <http://www.isi.edu/nsnam/ns/>.
- [30] R. Ramjee, K. Varadhan, L. Salgarelli, S. R. Thuel, S. Wang, and T. La Porta. HAWAII: A Domain-Based Approach for Supporting Mobility in Wide-Area Wireless Networks. *IEEE/ACM Transactions on Networking*, 4:45–54, Jun. 2002.
- [31] I. Ray and M. Kumar. Towards a Location-Based Mandatory Access Control Model. In *Computers and Security*, volume 25(1), 2006.
- [32] N. Sastry, U. Shankar, and D. Wagner. Secure Verification of Location Claims. In *Proc. of ACM Workshop on Wireless Security (WISE)*, 2003.
- [33] H. Schulzrinne, S. Shin, A. G. Forte, and A. S. Rawat. Reducing MAC layer handoff latency in IEEE 802.11 wireless LANs. In *ACM International Workshop on Mobility Management and Wireless Access (MobiWac 2004)*, 2004.
- [34] RSA Security. RSA SecureID, Jun. 2003.
- [35] R.E. Smith. *Authentication: From Passwords to Public Keys*. Addison Wesley, 2002.
- [36] M. Steiner, G. Tsudik, and M. Waidner. Diffie-Hellman Key Distribution Extended to Group Communication. In *Proc. of the 3rd ACM conference on Computer and communications security*, pages 31–37, New Delhi, India, 1996.
- [37] A. S. Tanenbaum. *Modern Operating Systems, Second Edition*. Prentice Hall, 2001.
- [38] J. Wang and L. Bao. Layer-2 Mobility Management in Hybrid Wired/Wireless Systems. In *The Second International Conference on Quality of Service in Heterogeneous Wired/Wireless Networks (QSHINE)*, Orlando, FL, Aug. 22 - 24 2005.
- [39] S.Y. Wang, C.L. Chou, Y.H. Chiu, Y.S. Tseng, M.S. Hsu, Y.W. Cheng, W.L. Liu, and T.W. Ho. NCTUns 4.0: An Integrated Simulation Platform for Vehicular Traffic, Communication, and Network Researches. In *1st IEEE International Symposium on Wireless Vehicular Communications*, Baltimore, MD, USA, Oct. 1 2007.
- [40] B. Waters and E. Felten. Proving the Location of Tamper Resistant Devices. Technical report, Princeton University, 2000.
- [41] Y. Zhang, Z. Li, and W. Trappe. Power-modulated challenge-response schemes for verifying location claims. In *Proc. IEEE Global Telecommunication Conference (GLOBECOM)*, pages 39–43, 2007.
- [42] Y. Zhang, W. Liu, W. Lou, and Y. Fang. Securing Sensor Networks with Location-Based Keys. In *IEEE Wireless Communications and Networking Conference (WCNC)*, New Orleans, LA, Mar. 2005.