LAAC: A Location-Aware Access Control Protocol

YounSun Cho, Lichun Bao and Michael T. Goodrich
Department of Computer Science
University of California, Irvine, CA 92697
{yscho,lbao,goodrich}@ics.uci.edu

***Abstract*— With the proliferation of wireless communication technologies and mobile computing devices, research interest has grown for location-aware systems and services. We propose LAAC, a novel Location-Aware Access Control protocol based on a coarsely defined location area that is enclosed by overlapping areas of multiple access points. Accordingly, a location key for location claim is derived from the overlapping access points' beacon information. In addition, the fact that a mobile device derives the location key enables us to track the location of the mobile device. LAAC does not require additional hardwares such as GPS or ultrasonic devices in order to localize the mobile devices. We enumerate possible attacks to the system and analyze their countermeasures. The computational and communicational costs and the memory requirement are evaluated, and the simulation results are presented.**

I. Introduction

With the growing prevalence of high speed wireless portable devices, the security requirements have significantly increased in recent years, especially for wireless LAN (WLAN) systems. While WLANs provide an easy access medium to users, it is vulnerable to misuses because of open-air transmissions in untethered hostile environments. Therefore, a natural course is to authenticate network access according to various user certificates.

User identity-based access control has been a promising approach. A user's identity [27] can be based on a password, a token, a ticket, an administered access control list (ACL), or a biometrics [15], [28]. SecureID is a token-based authentication scheme for remotely logging into corporate networks [2]. It requires the user to provide both a password and a random number token. Kerberos is another ticket-based network authentication protocol [15], and is widely used today. 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 [28]. Likewise, the access control list (ACL) is commonly used for access control by modern operating systems [3].

However, identification-based approaches do not satisfy certain security requirements that depend on user information such as the location. For instance, courtesy network access provisioning in hotels, restaurants or gas stations may only depend on whether the users are within the perimeters of the establishment. Moreover, identification-based approaches require user-agreement, information management, software, hardware and communication overheads in order to procure the related identities.

We propose a Location-Aware Access Control protocol (LAAC) for such scenarios, where location-aware security keys are used to access the network resources.

The rest of the paper is organized as follows. We describe related works in section II, and introduce the LAAC protocol operation and its security analysis in section III. Then in section IV, we evaluate LAAC efficiency and simulation results. We present a case study in V. Section VI concludes the paper.

II. Related Work And Over Approach

The Cricket system is a decentralized indoor location-support system that requires the combination of RF (radio-frequency) and ultrasonic signals in order to triangulate the user locations and to provide location services to users and applications [20]. PAC adopts the INS/Twine [18] architecture for scalable resource discovery and the Cricket system for location discovery [22]. In PAC, The client first receives a Location ID (LID) along with a time-varying Location Code (LIDCODE) from its surrounding access points' beacons, and sends them to a location authentication server, which in turn returns a ticket, granting the client service request. PAC requires synchronization between beacons and the location authentication server, and keeps track of the corresponding LIDCODEs as they change with time.

Sastry *et al.* describe an Echo protocol to compute node location based on the round-trip time of messages [23], also based on both RF and ultrasonic signals in location computations. They proposed the Region of Acceptance in order to combat malicious provers from submitting location claims that overstate the true processing delay. A similar protocol, based on the exchange RF messages, was proposed by Water *et al.* [4] for proving the location of tamper-resistant devices.

Zhang *et al.* [33] proposed the use of location-based keys using identity based public-key cryptography (ID-PKC) , which solves the Bilinear Diffie-Hellman Problem (BDHP) [7], [26].

In many cases, exact localization is not required, however, coarse location information is sufficient and much cheaper than other approaches in order provide location-based access control, such as the locations confined by building perimeters at an airport, Internet Cafe, hotel, etc. For these scenarios, we propose to define that access to the WLAN systems is granted if and only if the clients are located within areas covered by multiple access points/access points. Using sectored antennas, we can further specify the areas in desired shapes. To our knowledge, we are the first to combine WLAN coverage

TABLE I

NOTATION

M	The number of mobile stations.
N	The number of access point groups.
L	The number of access points responsible for an access-granted area.
MS_i	The identifier of mobile station i, where $i = 1 \ldots M$.
AP_j	The identifier of access point j, where $j = 1 \ldots L$.
r_j	The nonce of access point AP_j generated by random number generator(RNG).
k_i	The location key of mobile station MS_i.
$G_j^k,\ k = 1, \ldots, N$	The AP (access point) group that access point AP_j is a member of them.
$\mathcal{H}(.)$	The strong collision-resistant hash function.
T	The location key lifetime.
τ	The beacon broadcast interval of each access point.
$\|$	A binary operator concatenating its operands.
$\oplus$	A binary operator carrying out the Exclusive-OR of its operands.

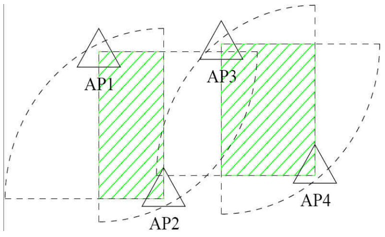


Fig. 1. Defining areas granted network access

and security mechanisms to provide access control at minor overhead to the clients.

III. PROTOCOL DESCRIPTION

A. Assumptions

Table I gives the notation used in this paper to describe various components of our LAAC.

In LAAC, we assume an infrastructure WLAN system based on IEEE 802.11 [1], and an wireless mobile devices (e.g. wireless laptops, PDAs) can communicate with each other through access points.

Moreover, we assume that access points can be equipped with directional antennas [8] so as to control the angle and distance of the signal transmission and to have precise signal coverage area without additional cost, and that signals do not bounce. Mobile devices have sufficient computational and communicational capacities to carry out the simple cryptographic operations required in LAAC. If necessary, each mobile device may carry the public key of each access point for mutual authentication purposes [6].

We assume that access control areas are divided into two types, access-granted and access-denied areas. Specifically, the access-granted areas are the spots covered by multiple access points, and can be custom-made into special shapes according to particular applications. For example in Fig. 1, two access-granted areas are defined as the shaded overlapping coverage areas of two AP groups $G_1 = \{AP1, AP2\}$ and $G_2 = \{AP3, AP4\}$, where the directional antenna of each access point spreads 90°. The access-denied areas are those areas outside access-granted areas. The access points that determine an access-granted area are called an *AP group* of the access-granted area. The AP groups that an access point belongs to are designated by network administrators when the WLAN system is initially designed and deployed.

B. LAAC Protocol Operation

In LAAC, each access point periodically broadcasts its nonce generated by a random number generator (RNG). We can't use pseudo-random number generators (PRNG's), since once you know one value, it is easy to compute the rest of the sequence if you know the algorithm being used. That is, we should not use security through obscurity. It is better to simply assume the AP's know each others nonces through a secure channel. If a mobile station MS_i is located in the access-granted area, it collects all nonces of the access points in the corresponding AP group of the area, and derives its location key k_i by simply XOR-ing all the nonces of access points. Afterward, MS_i constructs its access request (AR) using the strong collision-resistant hash function value of k_i and claims its location to its associated access point with it.

Note that the access points of an AP group exchange their nonces through the distribution system (DS) of the WLAN infrastructure, so that they are consistent with their nonces. That is, access points of a AP group are aware of each other, and exchange their nonces, thus the associated access point can derive the same location key with a mobile device. Consequently, the access point can authenticate the mobile station, and authorizes the mobile station to use the access point for communication purposes.

In addition, each access point can be a shared member of each AP group. For instance in Fig. 2, there are two AP groups G^1 and G^2 such that G^1 has three access points, $AP1$, $AP2$, $AP3$ and G^2 has three access points, $AP3$, $AP4$, $AP5$ (i.e., $G_1 = \{AP1, AP2, AP3\}$, $G_2 = \{AP3, AP4, AP5\}$). In this case, $AP3$ is a member of both AP group G^1 and G^2. Whenever each access point broadcasts its nonce (r_j), its ID (AP_j), it also broadcasts its group(s) (G_j^k).

Thus, $AP3$ broadcasts its groups G_3^1, G_3^2 with its nonce (r_3) and ID ($AP3$). This means "I am $AP3$, my nonce is r_3 and I am a member of two AP groups G^1 and G^2. Any mobile station that receives my broadcast message has to collect all nonces of access points in a group to construct the location key."

In this case, the $AP1$ and $AP2$ broadcast their AP group G^1, the $AP4$ and $AP5$ broadcast their AP group G^2, and $AP3$ broadcasts its AP group G^1 and G^2.

If a mobile station receives the broadcasting messages of $AP1$, $AP2$, $AP3$, $AP4$, then it selects the AP group G^1, since it only receives all members' broadcasting messages of G^1, and does not receive all members' broadcasting message

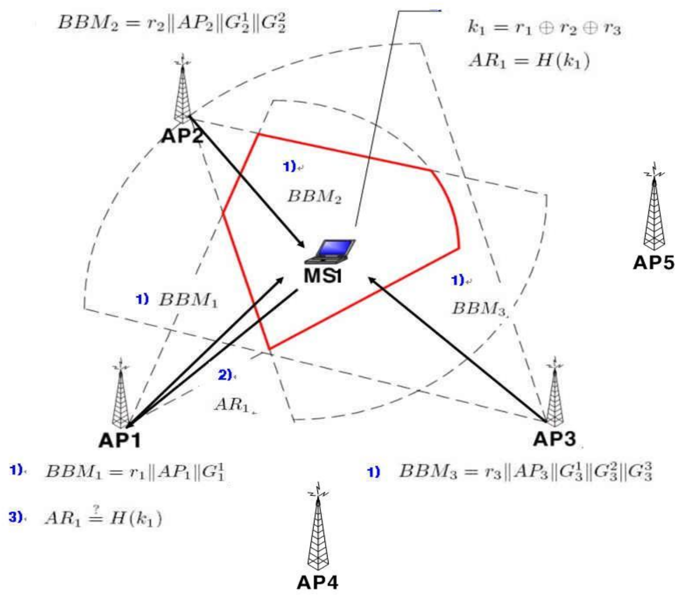

$BBM_2 = r_2\|AP_2\|G_2^1\|G_2^2$
$k_1 = r_1 \oplus r_2 \oplus r_3$
$AR_1 = H(k_1)$
AP2
1)
BBM_2
MS1
AP5
1) BBM_1
1)
BBM_3
2)
AR_1
AP1
AP3
1) $BBM_1 = r_1\|AP_1\|G_1^1$
1) $BBM_3 = r_3\|AP_3\|G_3^1\|G_3^2\|G_3^3$
3) $AR_1 \overset{?}{=} H(k_1)$
AP4

Fig. 2. Location-aware access control protocol

of G^2. On the other hand, if mobile station receives all members' broadcasting messages of both location groups G^1 and G^2 such as $AP1,\ AP2,\ AP3,\ AP4,\ AP5$, it may select one of them randomly or based on signal strengths to join the group's access-granted area.

C. LAAC Protocol

We describe LAAC step by step in this section.

1) Each access point AP_j generates its nonce r_j by a random number generator (RNG), constructs its broadcasting beacon message (BBM) such that $BBM_j = r_j\|AP_j\|G_j^k$ where $j = 1..L$ and $k = 1..N$ and broadcasts it in every τ. We assume the APs are aware of each other's nonces, e.g., by using a secure communication channel.
2) Each mobile station MS_i receives each AP's BBM_j, checks the AP groups of each BBM_j and selects one AP group among them as we described in section III-B. Afterwards MS_i computes its location key k_i by XOR-ing all nonces of APs (r_j) of the selected group such as $k_i = r_1 \oplus \ldots \oplus r_j$. Then MS_i constructs its access request (AR) using a strong-collision resistant hash function H such as $AR_i = H(k_i)$ and transmits it with its association request.
3) The association requested access point $AP_{j'}$ (from MS_i) can also construct the location key k_i as we described in section III-B. Thus access point $AP_{j'}$ verifies the hash value with this location key k_i, authenticates and authorizes mobile station MS_i[1].

For better understanding, we exemplify LAAC protocol in Fig. 2. In this figure, the number of access points is five $(AP1, AP2, AP3, AP4, AP5)$ and the number of mobile stations in the access-granted area is one (MS_1). Let $G_1^1 = \{AP1, AP2, AP3\},\ G_2^1 = \{AP1, AP2, AP3\},\ G_2^2 = \{AP1, AP2, AP4\},\ G_3^1 = \{AP1, AP2, AP3\},\ G_3^2 = \{AP1, AP2, AP4\},\ G_3^3 = \{AP1, AP2, AP5\}$.

1) Each access point $AP1, AP2, AP3$ constructs its BBM such as $BBM_1 = r_1\|AP_1\|G_1^1$, $BBM_2 = r_2\|AP_2\|G_2^1\|G_2^2$, $BBM_3 = r_3\|AP_3\|G_3^1\|G_3^2\|G_3^3$ and broadcasts it in every τ.
2) The mobile station MS_1 receives each AP's BBM_1, BBM_2, BBM_3, checks the AP groups of them and selects one AP group. After that, MS_i derives its location key k_i by XOR-ing all nonces of APs (r_j) of the selected group such as $k_1 = r_1 \oplus r_2 \oplus r_3$. Next, MS_1 constructs its access request (AR_1) such as $AR_1 = H(k_1)$ and transmits its AR with its association request to AP_1.
3) The association requested access point AP_1 can also construct the location key k_1. Thus it verifies the hash value with this location key k_1, authenticates and authorizes mobile station MS_1.

D. Security Analysis

We analyze possible attacks and its countermeasures in this section.

1) **Insecure nonce combination**

   Each mobile station constructs its location key by XOR-ing all nonces of access points in an AP group. This is very simple and almost zero cost computation, but we have to carefully observe this computation.

   If at least two nonces are the same in an AP group, the location key cannot be constructed because of the XOR property. Suppose three access points $AP1, AP2$ and $AP3$ broadcasts their 4-bit nonces such as $r_1 = 0001, r_2 = 0001$ and $r_3 = 0101$. In this case, the r_1 and r_2 are the same and it is canceled out (i.e. $r_1 \oplus r_2 = 0000$) and only r_3 is useful key. Thus any mobile station that receives r_3 can construct the location key and can be authorized without any effort.

   To resist this vulnerability, each access point should select its nonce not to be duplicated with other access points in the same group. We adopted RNG to generate nonces and if the nonce are sufficiently long (e.g., 80 bits), then it avoids such weak nonce combination because the probability of success to guess an nonce is 2^{-k} where k is the nonce size of each access point.

   Even though with this negligible probability, we can derive a more robust system as follows. We assumed the infrastructure network in our protocol and this means we can control each access point by communicating though the wired system (e.g. Ethernet) under the central server that creates the nonces of each access points and distributes to each access point to avoid the weak nonce combination as explained above.
2) **Bogus location claim**

   In LAAC, mobile stations that reside outside of an

[1] Because an access point accepts or rejects the association request, it can authorize/unauthorize MS_i by accepting/rejecting the association.

access-granted area are unable to claim their location, because they do not obtain all nonces of access points in an AP group and cannot construct their location key unless they collude with each other. However, it is possible for mobile stations to keep their authorized status even though they are not in the access-granted area. The possible scenario is as follows. We introduced two types of time intervals in LAAC: the beacon broadcasting interval of nonces τ and the location key lifetime T. The former is how often the nonces of the access points are broadcasted, and the latter is how often the location key is updated and this should be more considered for security.

Suppose the location key lifetime is 6 seconds ($T = 6$ seconds). If the mobile station stays in the access-granted area for 3 seconds and moves out, but still in the same ESS (Extended Service Set) [1] (e.g. nearby the granted-area[2]), then it can still keep its authorized status outside of the access-granted area. This false positive should be reduced or minimized.

We assume that the mobility speed of a mobile station is about the speed of a human walking (i.e., the mobile stations do not move as fast as a speed of vehicles (e.g. car, bus, etc.). This means that we can reduce the false positive rate to zero by controlling the location key lifetime. If the location key lifetime interval is reasonably smaller than the speed of the mobility of mobile station, we can achieve a near-zero false positive rate in this vulnerable scenario.

Furthermore, as compared with other location claim schemes based on the geographic properties [18], [20], [22], our scheme avoids a number of additional sources of false positives. For example, in the geographic-based location sensing schemes, there are errors and ambiguities related with the mis-measurement of the distances of the nodes (e.g., GPS error, sector error, and localization error.

3) **Wormhole attack**

In the wormhole attack, an adversary initially establishes a direct wormhole link between two nodes in the network and tunnels messages received at one location of the network to another over an invisible, a out-of-band, low-latency channel, which is typically a multi-hop distance away. Once the wormhole link is established, an adversary eavesdrops on messages, records packets at one location, referred to as the source point, and tunnels through the wormhole link to replay them at the other end, which is referred to as the destination point. The wormhole attack is very difficult to detect, since it can be launched without compromising any host, or the integrity and authenticity of the communication [12], [25], [29], [31], [32].

In the LAAC system, there are two possible wormhole attacks. Suppose there are two access points $\{AP1, AP2\}$ with directional antenna coverage of 90° defining an area C (Fig. 3). Let the signal area of access point $AP1$ be A and access point $AP2$ be B. Then the shared overlapping coverage area of A and B is C and this is an access-granted area that is outside of C ($A\ or\ B$, not the shared area of $A\ and\ B$).

In Fig. 3(a), a malicious mobile station MS_i' resides in A and receives nonce r_1 of $AP1$ and moves quickly to B within the broadcasting interval τ and receives nonce r_2 of $AP2$. In this scenario, MS_i' can construct the location key $k_{i'}$ such as $k_{i'} = r_1 \oplus r_2$. However, if τ is reasonably small (e.g. $\tau = 1$ second), and the number of access points in a AP group is many (e.g., $L \geq 3$), the probability of success for MS_i' to collects all nonces of access points is a quite difficult task.

Another possible attack is a collusion between malicious mobile devices in Fig. (3(b)). Suppose there are two malicious nodes, MS_i' and MS_i'', residing outside of the area C. That is, the node MS_i' is in area B and receives nonce r_1 of $AP1$ and MS_i'' is in area A and receives nonce r_2 of $AP2$. If MS_i' and MS_i'' collude with each other and share their nonces of access points, then MS_i' and MS_i'' can construct the location key. However, this is quite an expensive attack, because they should develop a hacking program to share their information in real-time.

4) **The Sybil attack**

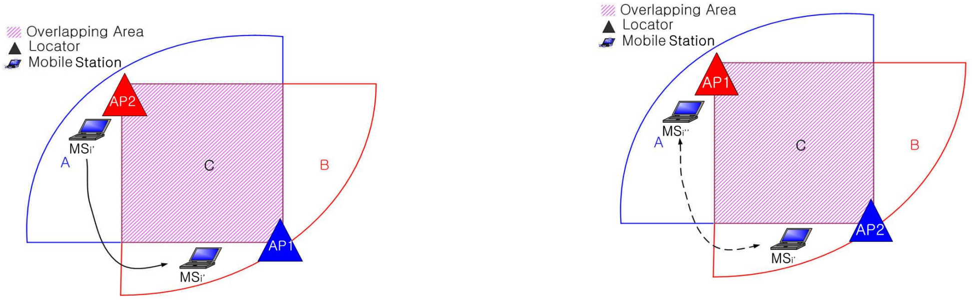
In the Sybil attack [13], [16], an adversary might impersonate multiple network entities by assuming their identities as if it were a large number of nodes, for example, by impersonating other nodes or simply claiming multiple forged identities. Unlike the wormhole attack, the attacker is able to compromise communications, gain access to the cryptographic quantities usually by compromising network entities, obtaining multiple node identities and injecting bogus data into the network [5], [16].

As we describe above, a powerful malicious mobile station might impersonate an access point by broadcasting bogus nonce r_j' as if it is a legitimate access point $AP_{j'}$ in LAAC. For simplicity, we did not provide for the authentication of an access point. However, our system can be easily extended to resist this attack.

We reasonably assume that the mobile stations have sufficient computational and communication capacities. Thus, each mobile station might have a certificate (or a public key) of each access point[3]. Under this condition, each access point broadcasts a timestamped broadcasting beacon message (BBM) and its signature such that $BBM_j, Sign_{AP_j} = (r_j \| AP_j \| G_j^k), Sign_{AP_j}(H(r_j \| AP_j \| G_j^k)|\ TS_j)$ where $j = 1..L$, $k = 1..N$, $TS_j = timestamp\ of\ AP_j$.

[2] This means the mobile station has the same IP address as well as the same MAC address. Therefore, the network is not disconnected. If the mobile station moves to a different subnet, the network will be disconnected.

[3] Actually, this needs a pre-installation phase.



(a) Wormhole Attack1

(b) Wormhole Attack2

Fig. 3. Two possible wormhole attacks

Then each mobile station can verify the signature of each access point. Furthermore, an adversary cannot replay the BBM of each access point because each access point includes its timestamp in the BBM and signature pair.

IV. EVALUATIONS

A. *Efficiency Estimation*

Various location sensing schemes have been reported. One of the simplest approaches is to estimate the position of a given source based on the received signal strength. However, this system is not trustworthy, since a malicious mobile station can transmit stronger signal or distract signal of other devices. Obstacles such as walls, furniture and other objects found in buildings create a much harsher radio propagation environment. A variety of ranging and positioning techniques with different technologies such as RF, ultrasound, infrared, electromagnetic, and etc. have been proposed to solve this problem [13], [14].

One of the most well known location sensing systems is using GPS that is widely used to track moving objects located outdoors. However, GPS has several inherent drawbacks of accurately determining the location of objects inside buildings. Thus, GPS is not desirable for an indoor environment. Furthermore, GPS requires an expensive and energy-consuming electrical machine and a precise synchronization with a satellite's clock. The ultrasonic round trip time technology [23] is commonly used as a means of obtaining range information via signal propagation time, but this mechanism requires a large fixed infrastructure throughout ceilings and is rather sensitive to the precise placement of the ceiling sensors thus its scalability is questionable. GPS and other round trip time technologies present a costly and inefficient solution to find a mobile object in a wireless network. Therefore, finding the location of mobile objects inside buildings is a challenge.

We propose a novel approach based on a location key to verify the location claim of a mobile station in a wireless network. Our system does not require specific additional hardwares such as GPS or ultrasonic devices in base stations or in mobile stations. Therefore, our systems achieves the ability to locate objects inside and outside buildings efficiently with a very low cost (assuming we use wireless signals that do not bounce well).

TABLE II

VARIOUS HASH FUNCTION COMPUTATION TIMES (μSECONDS) BASED ON THE CRYPTO++ 5.2.1 BENCHMARKS [10], [19]

Algorithm	10Byte	100Byte	1KByte	10KByte	100KByte
MD5	.046	.46	4.6	46	460
SHA1	.147	1.47	14.7	147	1,470

Moreover, our system enormously reduces the computation and communication overhead to measure the location of a mobile station as compared with previous systems [17], [21], [29], [30] and does not require any pre-deployment/pre-installation/setup phase. Now we analyze the computation and communication efficiency as well as the storage requirements of LAAC.

Table II shows the results of Cryptographic benchmark tested on the AMD Opteron 1.6 GHz processor under Linux 2.4.21. Suppose there are L access points in an AP group and N AP groups. Let the size of the nonce of an access point be 80 bits and ID of each access point be 8 bits. We adopt 160-bit SHA-1 for hash function.

To make an access request, each mobile station just computes the hash value of the location key, which takes only 0.147 μseconds. For the same reason, to authenticate each mobile station, an access point takes the same time to compute the hash value of the location key.

The size of the broadcasting beacon message (BBM) of each access point is at most $80 + 8 + 8 * |L| * |N|$ bits (=nonce size + ID size + IDs sizes of AP groups) and the access request size is 160 bits.

For the mobile stations, there is no storage requirement for LAAC.

B. *Simulation Study*

We carried out experiments with J-Sim [11], which is the network simulator constructed in JAVA. In the simulations, we created twenty five nodes including mobile stations and two access points, numbered from 0 to 24, which were deployed in a linear fashion, spaced 80 meters apart in a 400 meter × 400 meter area - node 0 and node 18 are two access points and the rest of other nodes are mobile stations. We adopted the 802.11 propagation and path-loss model and the free-space model without a routing protocol between mobile stations, and two access points broadcast beacons with nonces 1000 times in every broadcasting interval τ.

In the first experiment, we used the `RANDOM` method in JAVA API package as the nonces r_1 and r_2 of two access points with $|r_1| = |r_2| = 4, 8, 16$-bit without mobility of mobile stations with $\tau = 1$ second (Fig. 4(a)) such a random-number generator is not Cryptographically secure but its time performance should be comparable to that of a random lookup table. In the second experiment, we adopted 16-bit $|r_1|$ and $|r_2|$ with random mobility of mobile stations and tested the location key lifetime $T = 1, 2, 4, 8$ seconds with $\tau = 1$ second(Fig. 4(b)).

Fig. 4(a) presents the false positive rate under the various nonce sizes such as $|r_1| = |r_2| = 4, 8, 16$ bits for access points. Theoretically, we usually require at least a 80-bit nonce to resist brute-force attacks. However, the first experiment shows that only 10% of the safe nonce size guaranteed a 0% false positive rate under our practical topology in our simulation model. Thus, our protocol is quite secure, efficient and easily adopted in the real world.

Our protocol guarantees the bogus location claim free[4] under the condition that $T = \tau$ and τ is reasonably smaller than the speed of mobile stations[5]. However, if $T > \tau$, then it is possible to have a false positive. The second experiment shows this relationship between the location key lifetime T and the nonce τ (Fig 4(b)). We increased the $T = 1, 2, 4, 8$ seconds exponentially with $\tau = 1$ second. The figure presents that the false positive rate is increased as T is increased and also shows that it guarantees false positive free with $T = \tau = 1$ second in the figure.

Furthermore, we conclude that the longer nonce size of access points permits the longer location key lifetime, because an adversary takes longer time to perform a brute-force attack on this nonce as its size is longer from the simulation results.

V. Case Study

Our LAAC can be applied to location-based access control systems [20], [22], [23] and location tracking systems [24]. In the location-based access control system, once a location of a mobile station has been verified by the LAAC protocol, the mobile station is granted to be able to access a particular resource according to a desired policy.

Access control for the wireless network resource of a Cyber cafe can be a typical example. Suppose Alice goes to New York for a business trip with her wireless laptop or PDA and wants to check out email or access to the Internet in a Cyber cafe, which provides a wireless network resource. In this case, only users in the Cyber cafe should be allowed to ac,cess to the wireless network, and if Alice is outside of she should not be granted access to the wireless network.

That is, if a mobile station moves into the Cyber cafe, it receives BBMs of access points, constructs its location key, claims its location with it, and authorized to access to the wireless network in the Cyber cafe. After this authorization is completed, the IEEE 802.11 standard wireless LAN protocol can start. We can also apply our LAAC to trace mobile stations (e.g. wireless laptop or PDA).

VI. Conclusion

We have described a novel location aware technique based on location keys for reducing costly hardware dependency and improving efficiency securely without any pre-installation/setup phase. Compared to previous systems, our system provides low communication and computational overhead and requires zero storage per mobile station without additional expensive hardware such as GPS and ultrasonic devices.

Acknowledgment

Special thanks to Dehn Sy for helping us finish the simulations.

References

[1] IEEE Std 802.11. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Technical report, IEEE, 1999.

[2] RSA SecureID. June 2003. Available at http://rsasecurity.agora.com/rsasecured/guides/imp_pdfs/adtran_ace5.pdf.

[3] A. S. Tanenbaum. *Modern Operating Systems, Second Edition*. Prentice Hall, 2001.

[4] B. Waters and E. Felten. Proving the Location of Tamper Resistant Devices. Technical report, Princeton University.

[5] C. Karlof and D. Wagner. Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures. In *Proceedings of IEEE International Workshop on Wireless Sensor Network Protocols and Applications*, 2004.

[6] C. Kaufman, R. Perlman and M. Speciner. *Network Security: Private Communication in a PUBLIC World*. Prentice Hall, 2002.

[7] D. Boneh and M. Franklin. Identify-based encryption from the weil-pairing. *SIAM Journal of Computing*, 32(3):586–615, 2003.

[8] D. M. Pozar and D. H. Schaubert. *Microstrip Antennas: The Analysis and Design of Microstrip Antennas and Arrays*. Wiley-IEEE Press, May 1995.

[9] W. Dai. Speed benchmarks for various ciphers and hash functions. Available at http://www.eskimo.com/w̃eidai/benchmarks.html.

[10] H. Tyan. J-Sim. Available at http://www.j-sim.org/.

[11] I. Khalil, S. Bagchi, and N. B. Shroff. LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Network. In *the International Conference on Dependable Systems and Networks (DSN)*, Yokohama, Japan, 2005.

[12] J. Douceur. The Sybil Attack. In *Proceedings of IPTPS 2002*, Cambridge, MA, USA, March 2002.

[13] J. Hightower and G. Borriello. Location Systems for Ubiquitos Computing, August 2001. IEEE Computer Magazine.

[14] J. Kohl and B. C. Neuman. The Kerberos Network Authentication Service (Version 5), September 1993. Internet Request for Comments RFC-1510.

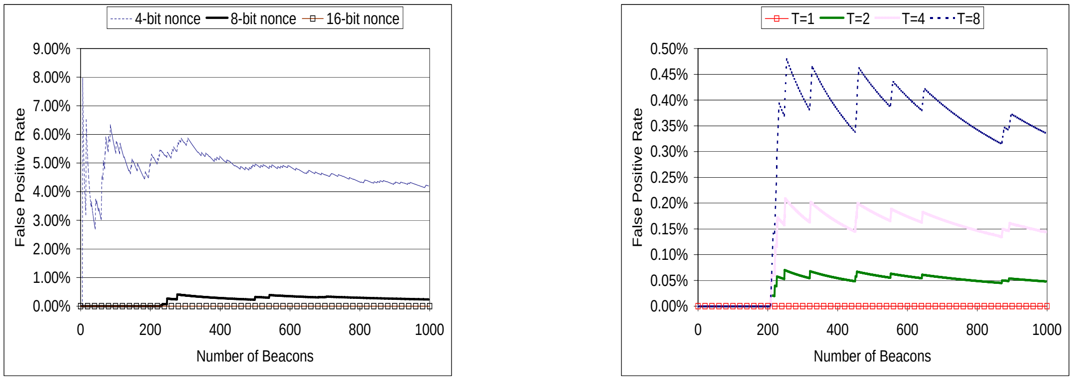
[15] J. Newsome, E. Shi, D. Song and A. Perrig. The Sybil Attack in Sensor Networks: Analysis and Defenses. In *Proceedings of IPSN 2004*, Berkeley, CA, April 2004.

[16] 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.

[17] M. Balazinska, H. Balakrishnan, and D. Karger. INS/Twine: A Scalable Peer-to-Peer Architecture for Intentional Resource Discovery. In *Proceedings of the First International Conference on Pervasive Computing*, pages 32–43, August 2002.

[4] We described this in section III-D.

[5] We assume that the speed of mobile station is about human's walking speed because the mobile station does not move fast in the access-granted area such as inside a room of a building.



(a) False positive rate with various nonce size where $\tau = 1$ second, static mobile station

(b) False positive rate with various location key lifetime T where $\tau = 1$ second, nonce size=16 bits, randomly moving mobile station with =1m/second

Fig. 4. Comparison of False Positive Rate

[18] M.T. Goodrich. Leap-Frog Packet Linking and Diverse Key Distributions for Improved Integrity in Network Broadcasts. In *IEEE Symposium on Security and Privacy (SSP)*, pages 196–207, 2005.

[19] N. B. Priyantha, A. Chakraborty, and H. Balakrishnan. The Cricket Location-Support System. In *6th ACM International Conference, Mobile Computing and Networking (ACM MOBICOM)*, August 2000.

[20] 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)*, 2005.

[21] 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.

[22] N. Sastry, U. Shankar and D. Wagner. Secure Verification of Location Claims. In *Proceedings of ACM Workshop on Wireless Security (WISE 2003)*, 2003.

[23] P. Juang, H. Oki, Y. Wang, M. Martonosi, L. Peh, and D. Rubenstein. Energy-Efficient Computing for Wildlife Tracking: Design Tradeoffs and Early Experiences with ZebraNet. In *ASPLOS-X*, San Jose, CA, October 2002.

[24] P. Papadimitratos and Z. J. Haas. Secure Routing for Mobile Ad Hoc Networks. In *Proceedings of CNDS 2002*, January 2002.

[25] 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.

[26] R. E. Smith. *Authentication: From Passwords to Public Keys*. Addison Wesley, 2002.

[27] R. M. Needham and M. D. Schroeder. Using Encryption for Authentication in Large Networks of Computers. In *Communication of the ACM*, pages 993–999, December 1978.

[28] S. Capkun, L. Buttyan, and J. Hubaux. SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks. In *Proceedings of SASN 2003*, Virginia, October 2003.

[29] U. Hengartner and P. Steenkiste. Proceedings of 9th ACM Symposium on Access Control Models and Technologies (SACMAT 2004). In *SACMAT*, pages 11–20, Yorktown Heights, NY, June 2004.

[30] Y. Hu, A. Perrig, and D. Johnson. Packet Leashes: A Defense Against Wormhole Attacks in Wireless Ad Hoc Networks. In *Proceedings of INFOCOM*, San Francisco, CA, USA, April 2003.

[31] Y. Hu, A. Perrig, and D. Johnson. Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols. In *Proceedings of ACM Workshop on Wireless Security (WISE 2003)*, October 2003.

[32] Y. Zhang, W. Liu, W. Lou, and Y. Fang. Securing Sensor Networks with Location-Based Keys. In *IEEE Wireless Communications and Networking Conference (WCNC'2005)*, New Orleans, LA, March 2005.