Virtual Operator based AAA in Wireless LAN Hot Spots with Ad-hoc Networking Support

Junbiao Zhang[a] **Jun Li**[a] **Stephen Weinstein**[b] **Nan Tu**[c]
zhangj@tce.com *lijun@tce.com* *weinstein5@comcast.net* *nan@nec-lab.com*
[a] Thomson Multimedia Corporate Research, Princeton, New Jersey, U.S.A. *
[b] Independent Consultant, IEEE Director
[c] C&C Research laboratories, NEC USA, Princeton, New Jersey, U.S.A.

Sound and effective authentication, authorization and accounting (AAA) schemes for convenient and secure mobile wireless accesses are of great importance given the increased popularity and business opportunities in public wireless LAN hot spots. One possible scheme, which uses the mobile users' service providers as the single point of contact for all AAA transactions, is emerging as a very promising solution. We refer to such service providers as "virtual operators". In this paper, we discuss various existing virtual operator AAA solutions and present our solution that is entirely based on IP. By converging both the AAA process and data transmission at the IP layer, our solution is extremely flexible and extensible. Compared with existing solutions, it works across multiple air interfaces and is interoperable with wireless LAN cards from different vendors. Further, it supports the scenario where access points use intermediate mobile terminals and ad-hoc networking to extend their service coverage. Service credits can be properly assigned to these intermediate terminals as incentives for providing relay services. Our solution is especially useful for a public access LAN environment where multiple wireless access technologies, a diverse set of wireless products and different types of wireless operators may coexist to provide mobile users with convenient and comprehensive wireless access solutions.

I. Introduction

Wireless LAN (WLAN) technologies, especially the IEEE 802.11 standards [1], have received great attention in recent years. Commercial products such as Apple's Airport (http://www.apple.com/airport), Lucent's ORiNOCO (http://www.orinocowireless.com) and Cisco's Aironet (http://www.cisco.com/warp/public/cc/pd/witc/ao350ap) are widely available on the market and are making wireless LAN access fast, convenient and economical. Wireless LAN Access Points (AP) are not only installed in corporate environments as a convenient extension to the wired LANs, but are starting to be deployed in public hot spots such as airports, hotels and Internet cafes as a means for public Internet access. Mobile users can get fast and reliable Internet access at these hot spots using their laptop computers or other mobile devices. A mobile terminal (MT) connects to an AP through a WLAN and uses the wired LAN to which the AP attached as a gateway for Internet access. Further, it is possible that an MT that is out of the coverage area of an AP may use other MTs as relay points to reach the AP. These MTs thus form an ad-hoc network to effectively extend the service coverage of a wireless LAN hot spot. Figure 1 illustrates the usage scenario of a wireless LAN hot spot with virtual operator and ad-hoc networkig support.

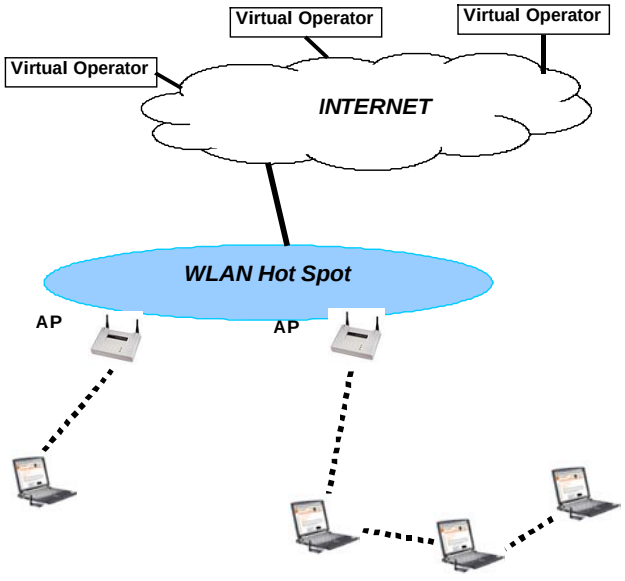

Figure 1: Hot spot WLAN with virtual operator and ad-hoc networking support

Two business models are possible for a commercial WLAN at a hot spot: free access to attract customers (e.g. Internet Caf), or paid access. In this paper, we assume the latter model. In order to ensure the proper operation under

*Part of the work described in this paper was done while the authors were with C&C Research Laboratories, NEC USA

this model, it is critical that Authentication, Authorization and Accounting (AAA) be carefully done. Due to the transient nature of the WLAN usage scenario, it would be quite inconvenient if a mobile user has to maintain an account with each WLAN provider or has to go through the payment transaction process (e.g. credit card) each time he/she starts using a WLAN. Such an inconvenience would reduce the user's interest in using the WLAN services and would mean less business opportunities for the WLAN operators. One promising solution to this problem is to use the mobile users' existing service providers for all AAA transactions. These service providers could be any type of entities that offer the users certainly types of services and maintain the users' accounts. These may include, for example, Internet Service Providers (ISP) (e.g. AOL), Content Providers (e.g. Yahoo!), cellular operators (e.g. VoiceStream), or even any pre-paid card issuers. In this context, the roles of these service providers are the mobile users' anchor points that bridge between the mobile users and the various wireless LAN operators. In effect, these service providers serve as virtual operators that maintain contractual relationships with WLAN providers. The use of these virtual operators relieves the mobile users from the burden of having to maintain a trust relationship (account) with each wireless LAN that the user wishes to use. Such a solution is mutually beneficial: It allows the virtual operators to provide additional revenue generating services and increase their user base. The convenience and the security assurance from the existing service providers also give mobile users greater interest and confidence in using the WLAN services.

It can be envisioned that a single WLAN operator may maintain contracts with several virtual operators. To each virtual operator, the WLAN appears as a dedicated LAN for the virtual operator's mobile subscribers. Such a conceptually dedicated LAN is important for many reasons such as per virtual operator Service Level Agreement (SLA) provisioning, security enforcement and service billing.

In essence, the goal of any virtual operator AAA scheme is to build the trust relationships among mobile users, access points and virtual operators. With service extension using ad-hoc networking, it is further required that the APs be able to properly identify the intermediate MTs. Based on all these considerations, there are many challenges to the design of a sound and efficient AAA scheme. Among them, the following are most prominent:

- Mutual authentication:
  - Access points need to authenticate wireless users to ensure that only authorized users can access the Internet and local services/resources
  - Wireless users need to make sure that the access point is not a "rogue access point" which intercepts user traffic and steals information
- Key distribution: Because mobile users can use wireless services at any public hot spots, it cannot be assumed that the users know the shared key (broadcast key or per session key) with each access point.
- Open air problem: Before a shared key is agreed upon by both the mobile user and the access point, the transmission between the user and the access point may be captured by anyone. No sensitive information (e.g. clear text password) can be exchanged at this stage.
- Relay MT identity: The WLAN operator must provide incentives for MTs to serve as relay points to extend service coverage. Accordingly, a sound mechanism must be in place to properly identify these relay MTs and prevent dishonest MTs from falsely claiming credits.

In this paper, we discuss various existing virtual operator AAA solutions and present our solution that is entirely based on IP. By converging both the AAA process and data transmission at the IP layer, our solution is very simple and flexible. IPSEC is used between access points and mobile terminals for per-packet authentication, or if desired, per-packet encryption. This provides a widely available strong security solution that gets around the problems in the current WEP (Wired Equivalence Privacy) algorithm [2] and the lack of multiple session key support in most access point products. A packet filtering function employed at an access point, similar to the firewall function, serves as a transparent mechanism for controlling not only authentication and authorization, but also packet level accounting. Compared with existing solutions, our solution works across multiple air interfaces and is interoperable with wireless LAN cards from different vendors. It is thus especially useful for a public access wireless LAN environment where multiple wireless access technologies, a diverse set of wireless products and different types of wireless operators may coexist to provide mobile users with convenient and comprehensive wireless access solutions. We shall explain the operation details of our scheme and compare it with other solutions. Because our AAA mechanism is based on IP and aims at building trust relationship between an MT and an AP, relay MTs connected through ad-hoc networking can be treated as a transparent IP transport cloud. We will therefore present our AAA solution without considering the ad-hoc networking case for the ease of presentation. The additional AAA requirements incurred by ad-hoc networking support will be specifically discussed after we present the overall AAA architecture. For convenience, we focus our discussion on IEEE 802.11b WLANs. But it should be pointed out that all the discussions also apply to other types of Wireless LANs.

The paper is organized as follows: In section 2, we list a few most representative types of virtual operators and explain their specific characteristics. In section 3, we describe existing virtual operator AAA solutions and discuss their strength and weakness. In section 4, we present the overall framework and the general procedure of our AAA scheme. Major differences between our scheme and existing solutions are also explained. Finally, we conclude the paper in section 5.

II. Types of Virtual Operators

As we mentioned earlier, there could be various types of virtual operators as long as they provide certain types of services to the wireless users and maintain accounts for them. Such accounts will then be used as the basis of AAA services for public WLAN accesses. In this section, we shall pay special attention to a few specific types of potential virtual operators and discuss their characteristics in the roles as virtual operators. These include ISPs, cellular operators and pre-paid card providers.

II.A. Internet Service Providers

It is likely that ISPs will be the earliest adopters of the virtual operator concept and become the most common type of virtual operators for the following reasons:

- The business models of ISPs and the wireless LAN operators are closely related: both provide commercial Internet accesses to their subscribers. This potentially results in simple and consistent business relationship arrangement. Service Level Agreement (SLA) including QoS parameters, authorization policies and charging models would be relatively easy to be set up and mutually understood.
- A consistent user experience can be maintained. Obtaining Internet access is the user's primary goal. By having the user's ISP as his/her virtual operator, it appears to the user that his/her ISP has a large footprint extending to wireless hot spots. The user can potentially maintain the same user interface and on-line access experience.

It should be noted that the virtual operator ISPs are not necessarily (and most likely not) the same as the ISPs who provide Internet connections to the WLAN operators.

II.B. Cellular operators: Interworking

Wireless LANs have become a serious threat to cellular operators who are starting to provide data services through their existing 2nd generation (2G) cellular networks and preparing to deploy 2.5G/3G networks for higher data throughput. While cellular networks offer far bigger coverage than wireless LANs and are good for ubiquitous access scenarios, the data throughput and overall cost simply could not compete with WLANs in hot spots. For example, cellular operators have spent a fortune on the 3G spectra, yet the peak rate a 3G cell can provide will be only 2 Mbps. This is no comparison with IEEE 802.11b based wireless LANs that are already near commodity type of price while offering up to 11 Mbps peak throughput.

Realizing the relative strength and weakness of cellular data and wireless LAN services, people from both technology areas are now working towards interworking solutions that allow mobile wireless users to roam between cellular data networks and wireless LANs seamlessly. Standardization efforts are going on within major cellular network and

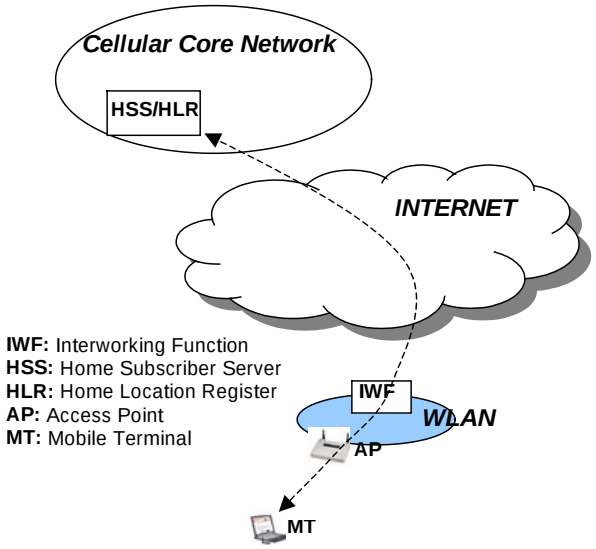

Figure 2: An IP based cellular/WLAN interworking architecture

wireless LAN standardization bodies such as the 3rd Generation Partnership Project (3GPP), ETSI/BRAN HiperLAN/2 and IEEE 802.11. As an example, the WLAN interworking effort within 3GPP Service Architecture 1 (SA1) has identified six interworking service scenarios ranging from simple authentication interworking to seamless service integration. ETSI/BRAN has broadly classified interworking architectures into two categories: Tight coupling, in which interworking WLAN traffic passes through 3GPP Core Network (CN) and both the data planes and control planes of these two networks are coupled, and loose coupling, in which only the control planes of these two networks are coupled while the data planes are connected based on a common IP platform. Figure 2 illustrates such an interworking architecture. Currently, most of the standardization efforts concentrate on the loose coupling approach as it is less complex and more cost effective to deploy. Such an architecture relies on IP as the convergence layer for AAA, mobility as well as QoS interworking. Due to interference problems, it is not technically feasible to deploy multiple wireless LANs covering the same hot spots by different operators. Given the importance of seamless roaming cellular users are so used to, it is necessary that the hot spot WLANs, either deployed by cellular operators or independently owned, provide virtual operator support for various cellular operators.

II.C. Pre-paid card providers

In the telecommunication world, pre-paid calling cards are becoming increasingly popular. Nearly anybody can offer such services by setting up an 800 access number and leasing a telephone trunk from a long distance company or a fiber optics line from a fiber network infrastructure owner. The same idea can be easily applied to the wireless data

access area: any third party can set up a AAA server and sell pre-paid cards to mobile users for wireless access at hot spots. In the ideal scenario, a user may purchase a pre-paid card from any legitimate provider. The card contains a pin number and the URL of an authentication server. At any wireless LAN hot spots, the user just specifies the URL to the wireless LAN. This URL is used by the wireless LAN to contact the pre-paid card operator's AAA server to initiate the authentication process. During this process, the pin number is securely transmitted to the AAA server and is used to identify the user's account. Based on the balance in the account, the wireless LAN can then properly control the user access. In effect, a pre-paid card provider simply provides AAA service for the user and shares revenue with the wireless LAN operators. Such a model could significantly boost the use of public wireless LAN accesses. This requires that the virtual operator model be widely deployed in wireless LANs in hot spots.

III. Current solutions

Several companies are now offering Wireless LAN products with AAA support, most notably among them are Cisco, Lucent and Nokia. We shall explain their solutions and discuss their strength and weakness in this section. Another important sector in the wireless LAN market is the public wireless LAN solution providers and service aggregators such as Boingo, Wayport and Nomadix. We will categorize and present these solutions. The AAA aspects of mobile IP will also be explained as a general comparison. In addition, we shall examine the ad-hoc network architecture provided by MeshNetworks and explain how it is related to our solution.

III.A. Cisco

Cisco's wireless LAN products are based on the technologies acquired from Aironet. The AAA support is based on the draft standard proposal jointly submitted to the IEEE 802.11 standard group by Cisco, Microsoft, Intel, Symbol and Informed Technology. The proposed authentication procedure is described in the following.

The proposal uses IEEE 802.1x [3] and EAP [4] to provide a virtual link between the access point and the mobile terminal. The AP maintains a trust relationship with a remote authentication server. EAP messages are carried over IEEE 802.1x on the air link and RADIUS [5] on the path between the AP and the remote authentication server. These EAP messages are intended end to end between the MT and the authentication server and are completely transparent to the AP. A mobile terminal associates with an AP using open authentication (no encryption). After the association, the MT communicates with the AP through a controlled port that only allows the regular MT traffic when the port is in the authorized state. The MT uses the AP as a relay point and mutually authenticates with the AAA server. Upon authentication, the AAA server sends both the access point and the MT a per session key (encrypted). This key is used between the MT and the AP for a secure channel. The access point then sends the MT the WEP broadcast key through this channel. Note that this channel can be trusted by the MT because the AP is authenticated by the user.

The Cisco solution relies on IEEE 802.1x and dynamic WEP key set-up for authentication and access control. Given the security problem associated with the current WEP algorithm, it may take some time before this solution becomes very secure. Further, such a solution is not backward compatible with legacy access points that do not support IEEE 802.1x and per session keys. Thus at least for now, it is not a generic solution that can be deployed in all the wireless LANs. Another problem with the current solution is that all session keys between the MTs and the APs are assigned by the authentication server even though these keys should be local to each AP. This is clearly undesirable, especially when multiple virtual operators are involved. The current Cisco solution does not have virtual operator support in mind. The access point cannot dynamically select the authentication servers based on user request, but rather is configured to communicate with a fixed authentication server for EAP based authentication and key assignment. However, it is possible to configure the authentication server as a proxy that redirect user requests to their actual authentication server destination.

III.B. Lucent Technologies

Lucent Technologies offers the ORiNOCO family of wireless LAN products. Its spin-off company, Agere, is now taking over the ORiNOCO family of products. The ORiNOCO access points have built-in mechanisms for remote server based authentication using the RADIUS protocol. The basic procedure is as follows:

Immediately after association, the MT and the AP start a shared key generation process using the Diffie-Hellman algorithm: First, each side generates a pair of (private key, public key). Then, they exchange their public keys. Finally, a shared secret key can be generated by each side from its private key and the other's public key. This is a per session key and can be used to encrypt all communication between the AP and the MT. After this communication channel is established, the mobile user then initiates a login session with the RADIUS server through the AP. Only a one way authentication (user is authenticated by the RADIUS server) is done.

The major problem with this approach is that mutual authentication is not considered and it is well known that Diffie-Hellman algorithm is prone to "man in the middle" attack, i.e. a hacker may intercept communication between the MT and the AP and exchange Diffie-Hellman keys with both ends. This way, both the MT and the AP think they are talking with each other with a secure communication channel but in fact they both talk to the hacker in the middle. Thus a rogue AP can take advantage of the weakness in this solution and snoop user traffic with potentially secret infor-

mation. Another problem is that the secure channel establishment procedure (but not the Diffie-Hellman algorithm) is Lucent proprietary. Most of the wireless LAN cards from other vendors do not support such a solution. Given all these problems, Agere has since adopted the IEEE 802.1x standard in their new access point products.

III.C. Nokia

Nokia also has a series of WLAN products based on IEEE 802.11b. From the beginning, Nokia has targeted their products for network access in public "hot spots". Their "public access zone" solution [6], for example, provides a complete set of wireless LAN equipment to support WLAN for airports, hotels and railroad stations. Each set contains a number of access points and a gateway router connecting these access points to the Internet. However, judging from the available technical information about the "public access zone" solution, virtual operator support is not carefully considered. Only one way authentication is performed by the access point to ensure that mobile users have the permission to access the WLAN. Recently, Nokia announced their "operator wireless LAN"[7] solution. It consists of wireless LAN cards for the terminals, wireless access points, a public access controller and a GSM authentication and billing gateway. Each wireless LAN card has an integrated SIM card reader. It can thus be used for user authentication with GSM networks. The public access controller serves as a control point between the wireless LAN and the Internet. It is also responsible for relaying the authentication messages between the mobile terminals and the GSM gateway. RADIUS protocol is used between the public access controller and the GSM authentication and billing gateway. Each wireless operator LAN belongs to a single mobile operator, but global roaming can be achieved in a similar fashion as in the GSM network. Currently, Nokia only offers a conceptual description of this technology. Many technical details, especially those related to the AAA aspect, are quite unclear. For example, it does not specify

- Whether mutual authentication between the mobile terminal and the public access controller is performed.
- How the mobile terminal communicates with the public access controller before successful authentication and how the controller prevents users with fake identity from accessing the network

Given Nokia's market focus, it came as no surprise that their Operator LAN solution only targets cellular network based virtual operators. One particular requirement in their solution is that the MT be equipped with a SIM card so that the user can be properly authenticated by the cellular network. For this purpose, Nokia makes a wireless LAN card with a built-in SIM module. However, given the diversity of WLAN cards on the market, such a requirement is not very easy to be satisfied. We believe that the virtual operator concept should be applicable to a much wider range of entities including cellular operators, ISPs and any other third party operators willing to provide user AAA services.

III.D. Boingo

As one of the most popular public wireless LAN service providers, Boingo (http://www.boingo.com) is actually a service aggregator that uses existing wireless LAN hot spots to provide wireless services to its subscribers. Hot spot operators can join the Boingo program by installing Boingo's "hot spot in a box" package or individual access server components. Wireless users need to subscribe to the Boingo service and create accounts with Boingo. A client software from Boingo helps a user locate potential Boingo compatible access points and start the login process with the user name and password. The AAA scheme is based on IP. After successful login by the user through the Boingo client, an IPSEC tunnel is built between the client and a Boingo specific AAA server, such as "vpn.boingo.com". It is possible that this domain name may be resolved according to load balancing and location considerations, similar to what Akamai (http://www.akamai.com) does with web server redirection. It is unclear whether Boingo employs such a scheme, but it may seem inevitable: if all Boingo wireless accesses had to pass through the same IPSEC end point, the routing paths would be very inefficient and the end point could become overloaded.

The Boingo AAA scheme and the scheme that we will describe shortly are similar in terms of the IP based approach. However, in our solution, the IPSEC tunnel ends in the WLAN, which only performs access control and relies on the virtual operators for actual user authentication. In the Boingo approach, the tunnel ends in the Boingo authentication server, both authentication and access control are performed in the Boingo server. This difference is dictated by the support (or lack of support) of virtual operators in these two approaches. As a service aggregator, Boingo's "hot spot in a box" solution does not and would not provide virtual operator support. Boingo would be the only AAA service provider.

III.E. Web Browser based approach

Among the current public wireless LAN service providers, a majority of them use a web browser based approach for user authentication. Some of these service providers include Wayport (http://www.wayport.com), Nomadix (http://www.nomadix.com), NetNearU (http://www.netnearu.com), HereUare (http://www.hereuare.com) and joltage (http://www.joltage.com), to name a few. In this approach, the wireless users are not required to download any client software. Instead, the authentication processes are carried out in the web browsers on the client machines using the secure HTTPS protocol. One significant benefit of this approach is the so-called "zero configuration" on client machines: Web browsers with HTTPS support are universally available on nearly all client machines. A user is passive during the authentication process: when the user launches his/her web browser in a wireless LAN hot spot, any HTTP request will be redirected by the wireless LAN to a default authentication server web page. The user just

follows the instructions given on the page and inputs the user name and password accordingly. The HTTPS protocol is based on strong encryption and proven technology, thus the user authentication process is very secure.

However, the access control mechanism in such an approach is not secure at all. This is because the browser cannot perform any key configuration on the client machine after the authentication. Most of these browser based solutions thus have to rely on MAC address or IP address based access control, which are obviously quite vulnerable given that MAC addresses and IP addresses can be easily faked. Hacking and getting unauthorized access in such solutions are thus relatively easy.

III.F. Mobile IP

In [8], Perkins presented a framework in which AAA functions are integrated into mobile IP. Trust relationships among home AAA servers, local AAA servers, home agents, foreign agents and mobile stations are examined and an authentication model is proposed based on these relationships. Although the model is designed specifically for mobile IP, it is applicable to authentication in wireless LAN public access. In fact, all of the solutions discussed in the previous sections follow either part or all of such a trust model.

It should be noted that the focus of this paper is different from [8]. Whilst [8] mainly concerns with a general trust model and AAA framework, this paper concentrates on the technical methods in implementing a particular framework. This requires that both framework correctness and implementation efficiency be evaluated in a public access wireless LAN context. Additionally, some of the issues that are not addressed in [8] are taken into consideration and resolved in our solution. These include, among other things, mutual authentication between mobile stations and access points, and, proper accounting dispute handling.

III.G. MeshNetworks

Meshnetworks' (http://www.meshnetworks.com) mobile broadband technology utilizes peer-to-peer routing to create robust meshed networks with low cost and extensive coverage. A mesh network consists of four types of network elements: Subscriber devices, Wireless Routers, Intelligent Access Points (IAP), and Mobile Internet Switching Controller (MiSC). Subscriber devices are equivalent to the MTs in this document. They could be either an off-the-shelf laptop/PDA running Meshnetworks proprietary routing software, or a MeshNetworks' transceiver in the form of a PC card. These subscriber devices not only can access the fixed infrastructure through other network elements, but can serve as routers themselves to extend the mesh network coverage and increase the number of alternative paths that subscribers may utilize.IAPs are just like wireless LAN access points and act as the transition points between the wireless network and wired core network. The wireless routers are fixed network elements which are primarily deployed to extend the range of the IAPs and increase the network's spectral efficiency.

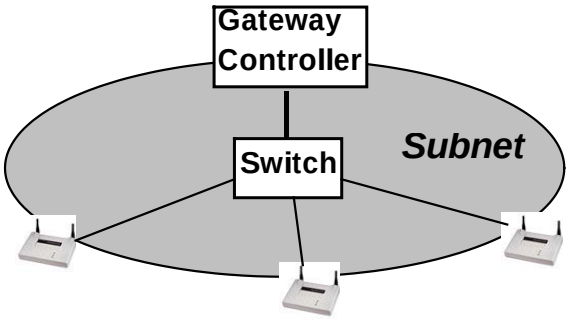

Figure 3: External gateway controller configuration in a wireless LAN

The MeshNetworks architecture has been generating substantial interests in the wireless industry. The company has been deploying experimental networks to demonstrate the feasibility and advantages of commercial ad-hoc networks. We believe that such an architecture is of great value to the wireless access industry. However, to make it feasible, good schemes must be designed to give subscriber devices motivation to forward other subscribers' traffic. Simply assuming a collaborative environment is apparently not sufficient. After all, packet forwarding is not for free as most mobile devices are concerned about, among other things, power consumption. At this point, it is still unclear how MeshNetworks addresses this issue judging from the available literature and press releases. In this paper, we shall discuss some of the possible incentive mechanisms that address the above concern in the context of wireless LAN hot spots.

IV. Our solution

In our solution, the entire AAA process is carried out over the IP layer. What differentiates us from other schemes (and all other schemes from each other) is the way AP controls the authentication, which includes the establishment of the authentication channel, the controlling mechanism on the AP and the session key assignment and management mechanisms. The scheme requires that a router-based controller be employed between the MT and the virtual operator for controlling MT access and relaying AAA messages. Such a controller can be either implemented in the AP (e.g. as in PamLAN [9]), or in an external entity (e.g. a gateway router the APs attached to). Figure 3 illustrates a possible set-up when the controller is an external entity. Since our scheme works essentially the same way in both cases, we shall use the router based AP scenario in our discussion thereafter. Because of the IP based solution, our AAA scheme has at least the following benefits:

1. It works over different air interfaces (e.g. IEEE 802.11[1], Bluetooth[10], HiperLAN2[11],

homeRF[12]) and across wireless LAN cards from different vendors.

2. It does not require modification to layer 2 protocols (e.g. 802.11, 802.1x)

3. It does not require that the AP support layer 2 session keys since encryption can be done at the IP layer using IPSEC[13]. If the AP supports 802.11 per session key, our scheme can take advantage of such support easily.

4. It supports ad-hoc networking for service coverage extension without any protocol change as the ad-hoc network is treated as a transparent IP transport cloud.

IV.A. Authentication and Authorization

In terms of the authentication scheme, our solution is similar in nature to the Cisco solution. However, there is one notable difference. In the Cisco solution, the session keys between APs and MTs are assigned by the authentication server. Since session keys are used between an AP and its associated MTs, they should be local to the AP. The Cisco solution could be problematic when multiple virtual operators are involved. Coordination among these virtual operators to generate unique keys can be a difficult task. We provide a mechanism that allows APs to determine session keys and communicate them securely to the associated MTs. We also designed the authentication procedure to be less vulnerable to denial of service attack at the step when the mobile user tries to authenticate itself with the virtual operator. A hacker may pretend to be the user and send a wrong response to the AP which in turn relays it to the authentication server. The authentication server will immediately close the authentication session by rejecting the user. Our solution alleviates this problem by letting the AP make more intelligent decision when relaying user authentication response.

Central to our solution is a filtering function installed on every AP. It is similar to the firewall function and filters all mobile traffic and determines whether they should be let through (authenticated user traffic with the session key), sent to the authentication engine (login session traffic), or blocked (unauthorized traffic). Besides security control, the filtering function is also used for traffic classification where multi-layer packet header information may be extracted through deep packet processing. IPSEC can be used to ensure data integrity as well as to prevent unauthorized users from pretending to be authorized ones. Each authenticated user (from a specific IP address) has a shared session key with the AP. If somebody fakes the source IP address in the packet without knowing the shared key, the IP packet headers will not be correctly decrypted and the packet will be discarded.

IV.A.1. The authentication procedure

In our solution, each mobile user has two keys, a private key and a public key. The private key is also used as a single shared secret key between the user and the virtual operator. We also refer to it as the user's password. The public key is stored at the virtual operator as part of the user's profile. This public key will be sent to the AP after user authentication. In other words, the user and the virtual operator authenticate each other using symmetric-key encryption with the user's password. After a successful authentication, the session key between the AP and the user is encrypted by the AP using public-key encryption and the result is sent to the user. With this session, the AP and the MT establish a trust relationship with respect to the service provider agreement. For ease of presentation, we shall assume that the AP and the virtual operators communicate with each other using RADIUS protocol. Thus we shall use the terms "RADIUS server" and "virtual operator" interchangeably in the rest of the paper.

When a mobile user moves into the coverage area of an AP, his mobile terminal (MT) first establishes a layer 2 connection with the AP. In the IEEE 802.11 term, this is called "association". Since we are going to use the virtual operator authentication process, this association step does not require any layer 2 authentication. The following procedure describes one possible authentication sequence after the association. Note that the AP has a list of virtual operators with which the AP has partnership agreements. The AP and each RADIUS server share a secret and all RADIUS packets exchanged between them are authenticated using this secret together with a random authenticator. Any sensitive information, such as plain text passwords, are encrypted using this shared secret.

1. The AP assigns the MT a dynamic IP address with the help of a DHCP [14] server. The AP also installs a filter for the IP address. At this stage, all IP traffic from this address is filtered and terminated by the AP and assumed to be authentication packets.

2. The user initiates a login session with his virtual operator. The virtual operator id and the user id are sent to the AP.

3. The AP sends the user's virtual operator RADIUS server an "Access-Request" packet with the user id.

4. The RADIUS server checks if the user id is valid. If so, it generates a random string S_1 and encrypts it using the user's password into string SS^1. It then sends back the AP an "Access-Challenge" packet with S_1 and SS^1. SS^1 is encrypted using its shared secret with the AP.

5. The AP forwards S_1 to the MT and saves SS^1 locally.

6. The MT encrypts S_1 using its password with the virtual operator. This encrypted string, SS_1, together with another randomly generated string, S_2, are sent to the AP.

7. If SS^1 and SS_1 do not match, the message received from the MT in step 6 is simply ignored. The AP waits until it receives another encrypted S_1 or times out. As

we will explain in more details, this extra checking is done to prevent the denial of service attack we mentioned earlier. If SS^1 and SS_1 match, the AP sends another "Access-Request" to the RADIUS server with the user id, SS_1 and S_2.

8. The RADIUS server uses the user's password to decrypt SS_1 and compares the result with S_1, if they match, it encrypts S_2 with the user's password (denotes the result as SS_2) and sends the AP an "Access-Accept" packet with both SS_2 and the user's public key PK encrypted using its shared secret with the AP. If the decrypted result does not match with S_1, it sends back an "Access-Reject" packet.

9. If the AP receives an "Access-Reject", it denies the user access. Otherwise, it notifies the user of successful login and forwards the user SS_2, the user's session key and the WEP broadcast key, all encrypted with PK using public key encryption. When the MT receives this encryption result, it first decrypts it with the user's password using private key decryption and obtains SS_2, the session key and the WEP key. It then decrypts SS_2 with the user's password using symmetric decryption and compares the result with S_2. If they match, it knows that the virtual operator and the AP can be trusted and may start using the AP, which has already changed the filter to let through all traffic from the MT's IP address.

Note that at step 4, the RADIUS server sends the AP both S_1 and SS^1. This is designed to solve the denial of service attack vulnerability in which only S_1 is sent to the AP. To see how the attack is possible, consider the following scenario: at step 5, a hacker may notice that the AP asks the MT to reply to the virtual operator's challenge. He can pretend to be the MT and sends the AP some garbage string. The AP then dutifully forwards this string to the RADIUS server thinking it is the MT's reply to the challenge. However, since it is the wrong response, the RADIUS server will immediately reject the request and close the authentication session. In our solution, since the AP knows the encryption result for S_1, if someone fakes a reply, the reply will be immediately discarded at the AP without affecting the actual authentication session. Of course, if the original authenticating user is a fake, the AP allows the authentication session to live longer than necessary and terminates the authentication session with timeout. Compared to the more serious problem of being denied of services, we feel that this is a small price to pay. The timeout value can be properly set to limit the problem.

Figure 4 illustrates the message exchanges among the MT, the AP and the virtual operator RADIUS server for a successful authentication.

Note that the above sequence can be simplified into only one round trip message exchange, i.e. only the mobile challenges the RADIUS server. This is possible because all mobile packets will be subsequently authenticated based on the shared key. The RADIUS server thus need not authenticate the mobile user in the first step. This simplified authentication procedure is apparently faster, but is also subject to easier denial-of-service attacks, i.e. a malicious user may constantly challenge the RADIUS server. Even with the addition of some user credentials, replay attacks are still possible. These two mechanisms can be used according to the level of security requirement in an actual system.

MTAP	Mobile Terminal Access Procedure
NAS/RC	Network Access Server/RADIUS Client
RS	RADIUS Server
UID	User identifier
S_1	Random string generated by RS
S_2	Random string generated by Mobile Terminal
E(M,K)	M is encrypted with key K using symmetric-key encryption
EP(M,K)	M is encrypted with key K using public-key encryption
A(M,K)	M is encrypted for authentication with key K using MD5
Kmu	Shared secret between the mobile user and RS
Krc	Shared secret between RC and RS
SK	Session key between mobile user and RC
Pkmu	Mobile user's public key

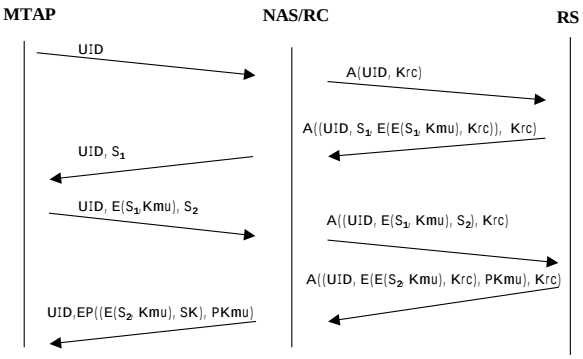

Figure 4: Message exchange sequence for user authentication

IV.A.2. Authorization Profile

Once a user is properly authenticated, the RADIUS server forwards the user profile to the access point. Such a profile contains the information regarding the user's service subscription with the virtual operator. Such subscription information may include, among other things, the following:

- The QoS parameters associated with the user access, e.g. the sustained rate and the peak rate for the wireless access.
- The types of user traffic that are allowed to pass through, e.g. any types of IP traffic, only HTTP traffic, or all traffic except RealVideo streaming.
- The type of services that are accessible to the user, e.g. whether the user is allowed to access local services provided in the wireless LAN.

Such subscription information is translated into filtering rules which are installed on the access point. Proper access control can then be carried out by filtering user packets based on these rules.

IV.A.3. Fast AAA handoff

When the user moves to a different AP, it is possible to perform a fast handoff such that the user does not have to go through the authentication process all over again. In most cases, such a fast handoff can be achieved based on the trust relationship between the new and the old APs. Given that both APs reside in the same public access LAN, such a trust relationship should not be a problem. In case two APs cannot trust each other, they can use the virtual operator as the relay point for the following fast handoff procedure:

After the reassociation, the new AP contacts the old AP, notifies the old AP about the reassociation and fetches the user profile (including the user's public key and the session key) from the old AP. The new AP then encrypts the new session key it shares with the user together with the old session key using the user's public key. The user then decrypts these keys and compares the old session key with the one he/she has. If the two matches, the user establishes a new session with the new AP. The reason the new AP does not use the old session key to encrypt the new session is because the session keys are local to each AP. Thus there is certain possibility (albeit remote) that the old session key may be already used in the new AP.

IV.A.4. Potential Problems

In this section, we discuss some potential problems in our proposed authentication scheme and techniques that directly address some of the problems.

- Fake IP attack: Because of the initial DHCP process happens in a non-secure channel, a hacker may easily learn the authorized user's IP address and MAC address. He can then fake to have the same IP address. Since the filter for that IP address has been changed to allow all traffic through, the hacker can gain unauthorized wireless access. This actually is a common problem with all access solutions without per session keys. Since we have individual session keys in our solution, we can easily avoid this problem through packet encryption either at layer 3 (IPSec) or layer 2 (802.11 encryption). IPSec is more generic and does not require per session key support from 802.11 (AP has to dynamically determine which key to use for different packets). However, it most likely will be done in software and cannot take advantage of the hardware encryption built in the 802.11 MAC layer (albeit optional). Thus we should use 802.11 per session key if it's supported. To use layer 2 encryption, the filter at the AP needs to check the mapping between the mobile's IP address and MAC address. If a hacker fakes the same IP address and the same MAC address, encryption by the 802.11 protocol would render his effort useless. The only possibility is then to fake the same IP address but a different MAC address, but this can be detected by the filter.
- Denial of DHCP service: Because DHCP request occurs before authentication, a hacker may constantly initiate the login session with fake MAC addresses. He may then occupy some IP addresses and may slow down others in gaining DHCP service. This can be partly mitigated by properly setting time out value for user's login session. Because the attacker cannot successfully authenticate himself, he will be kicked out quickly. Note that this problem is no more serious than the "air jamming" attack which can not be effectively prevented.

IV.B. Accounting

Proper accounting is of paramount importance to both the virtual operators and the wireless LAN operators since they directly affect revenue generation and sharing. We discuss two key issues related to accounting in this section: 1) how a virtual operator prevents potential accounting dispute between the wireless LAN and the user, and 2) how the intermediate forwarding nodes in an ad-hoc network get proper service credits.

IV.B.1. Mutual Proof Accounting

The virtual operator model we discussed in this paper dictates that the virtual operators and the wireless LAN operators are likely not in the same administrative domains. This may cause potential problems, especially in terms of accounting, between these operators. For example, a wireless LAN operator may overcharge a mobile user by mistake, or a dishonest mobile user may deny some reported usage. One way to avoid such potential dispute, as employed by some solutions, is to route all mobile user traffic through a central entity, which then routes the traffic to the Internet. This solution, however, is highly inefficient since it would create unnecessarily complicated routing paths and considerably slow down mobile user access.

We provide an effective accounting solution without requiring all mobile traffic to be routed through a central virtual operator server. We achieve this by using mutual accounting proof from both the mobile users and the wireless LAN operators. To avoid possible dispute, the virtual operator must have proof that the user and the AP both report the same traffic usage history. This can be done as follows:

On the MT, a traffic monitoring module monitors wireless LAN traffic after the user login and periodically compiles a traffic usage profile. It then signs this profile with a digital signature using the mobile user's shared secret with the virtual operator and sends the signed profile to the AP. The AP checks the profile against the stats for the MT collected by its filter. If the two match (with a tolerable error margin), the profile is forwarded to the virtual operator. Since all communication between the AP and the virtual operator is authenticated, the virtual operator can prove that both the MT and the AP agree on a usage profile. If the two

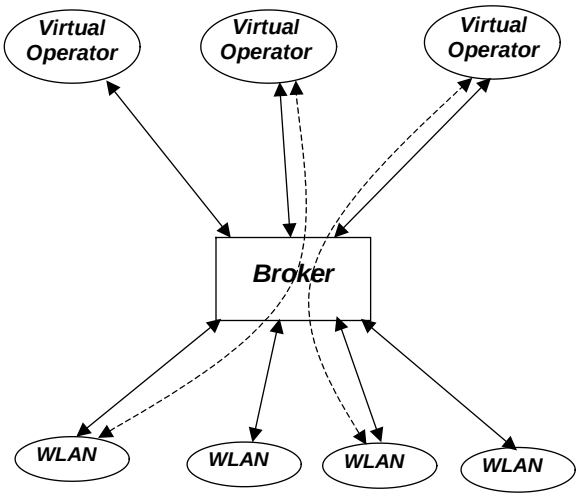

Figure 5: Business relationship establishment with a broker

do not match, the AP may simply terminate the service or ask the MT to readjust its stats.

IV.B.2. Ad-hoc Network Accounting

With ad-hoc networking support, a wireless LAN operator may extend wireless service at a hot spot using other mobile terminals. However, in order for these terminals to willingly provide such relay services, certain incentives must be given. In other words, the access points must be able to determine which MTs helped an MT reach the AP and reward these MTs accordingly, e.g. through service credits. Given the transient nature of ad-hoc networking, it is unlikely that the relay network configuration for an MT would remain the same for a reasonably long period of time. The routing table of any of these MTs may change at any time depending on the MT availability and signal strength variation. This makes it difficult to perform service credit accounting for the intermediate MTs on a time basis. Packet based accounting may thus be needed to properly identify the contributions of intermediate MTs. It should be noted that in order for these MTs to get service credits, they should have certain AAA association with an AP at the time they provide the relay services. They therefore should have already obtained an IP address and a session key shared with the AP. The simplest way for the intermediate MTs to be recognized at the AP is to use the "IP Record Route Option" [15] on the MTs along the routing path. This is an option field in the IP packet header to allow a router that processes an IP packet to record its IP address. This solution, although simple, is effective. One may suspect that it is vulnerable to cheating: any MT may put its IP address in a packet. However, we should note that the packet must reach the AP in order for the relay MT to get service credits. Thus in effect, even an MT not in the optimal routing path modifies an IP packet, the MT has to actually route the packet. There is thus not much incentive for the MT to do so. After all, why should it cheat when it can get the same result serving as a real relay MT? Such a simple method, however, does not prevent collaborative cheating in which an intermediate MT may record another MT's address in the IP packet header.

A more effective way in ensuring proper accounting in an ad-hoc set-up is through secure network configuration. This is similar to the network path set up in a switched Ethernet [16]. A Minimum Spanning Tree rooted at the AP may be constructed based on the reachability information flooded into the network from all the involved MTs. Such a tree is constructed in a secure manner such that the distance of each MT from the AP is verified. The verification can be carried out during the tree construction in a hierarchical fashion: The AP first determines all the MTs that can be directly reached. These MTs are then included as trusted MTs and in turn determine the other MTs that can be directly reached from them. Such a process is repeated until all MTs are included. Once the tree is determined, the subsequent packet forwarding no longer needs route recording because the AP already knows the branches and can thus figure out who are on the routing path for any specific MT. When there are any changes that warrant a new spanning tree topology, the spanning tree algorithm is re-run by the AP and a new tree is constructed. The collaborative cheating problem mentioned earlier is no longer a problem here: if a tree is constructed through cheating, some of the paths may be invalid, i.e. cannot reach the intended MTs. Since service credits can only be obtained when an MT transmits or receives a packet through the path, the path set up through cheating is useless for the cheating MTs.

IV.C. Broker

One particular difficulty with virtual operator set-up is that each wireless LAN operator and virtual operator pair with a business agreement need to establish a trust relationship. Given the diverse nature of the wireless LAN operators and different types of virtual operators, it would be quite impractical, if at all possible, to build such trust relationships on an operator-by-operator basis. To deal with this problem, a broker model can be employed. Figure 5 illustrates such a model. All the wireless LAN operators that provide virtual operator support only need to establish business agreements with this broker. Similarly, all the virtual operators just set up agreements with the broker in order to reach all the potential wireless LAN operators. The broker then bridges between the wireless LAN operators and the virtual operators for trust relationship establishment. There are two possible ways to achieve such bridging: AAA proxying and dynamic relationship set-up. In AAA proxying, the broker serves as a simple proxy and forwards all AAA traffic between the wireless LANs and the virtual operators. There is no explicit trust relationship between a communicating wireless LAN and a virtual operator. Instead, the relationship is implicitly set up through the concatenation of the trust relationships between the wireless LAN and the broker, and between the broker and the virtual operator. In dynamic relationship set-up, the broker helps a wireless LAN and a virtual operator build a direct trust relation-

ship and communication channel. Once such a relationship is established, all the subsequent AAA transaction will be carried out through the direct communication channel between the wireless LAN and the virtual operator without the involvement of the broker. Multiple brokers may exist for fault tolerance and competition purposes. Even if a wireless LAN operator and a virtual operator may have to establish business agreement with more than one broker, it is still far simpler than the case where a virtual operator has to establish business relationship with each and every potential wireless LAN operators.

V. Conclusion

"Virtual Operator" is a very useful concept in providing public Internet access with wireless LAN technologies. Mobile users can use their service providers for Authentication, Authorization and Accounting (AAA) and conveniently access the Internet through wireless LANs at hot spots such as airports and hotels. We presented an IP-based Virtual Operator AAA scheme in this paper. Compared with existing solutions, our scheme is simple and flexible. It is independent of the layer 2 wireless protocols and is interoperable with wireless LAN cards from different vendors. It also supports the scenario where ad-hoc networks formed by individual MT are used to extend the service coverage of access points. In a public access LAN environment, multiple wireless access technologies, a diverse set of wireless products and different types of wireless operators may coexist to provide mobile users with convenient and comprehensive wireless access solutions. Our scheme is thus particularly suitable for such an environment.

VI. Acknowledgement

The authors would like to express their gratitude to Kumar Ramaswamy, Charles Wang, Guillaume Bichot, Sachin Mody and Saurabh Mathur of Thomson Multimedia for the valuable discussions and ideas that greatly enrich the content of this paper.

References

[1] IEEE standard, "Information technology - Telecommunication and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications".

[2] Jesse Walker, "Unsafe at any key size: an analysis of the WEP encapsulation", IEEE 802.11 standard draft document, document number 802.11-00/362.

[3] IEEE Draft Standard, "Standards for Local and Metropolitan Area Networks: Standard for Port Based Network Access Control", IEEE Draft P802.1X/D11.

[4] L. Blunk and J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP)", IETF RFC 2284.

[5] C. Rigney et. al., "Remote Authentication Dial-In User Service", IETF RFC 2138.

[6] Nokia Corporation, "The Nokia Public Access Zone Solution", http://www.nokia.com/serviceproviders/pdfs/paz_brochure.pdf

[7] Nokia Corporation, "The Nokia Operator Wireless LAN", http://nokia.com/press/background/pdf/OWLAN.pdf

[8] Charles Perkins, "Mobile IP Joins Forces with AAA", IEEE Personal Communications, Aug. 2000.

[9] Jun Li, Stephen Weinstein, Junbiao Zhang, Nan Tu, "Public Access Mobility LAN: Extending the Wireless Internet into the LAN Environment", IEEE Personal Communications Magazine, Special Issue on Mobile and Wireless Internet: Architectures and Protocols, June, 2002.

[10] Bluetooth Special Interest Group, "The Bluetooth Specification", http://www.bluetooth.com/developer/specification/core_10_b.pdf

[11] HiperLAN2 Global Forum, "HiperLAN/2 - The Broadband Radio Transmission Technology Operating in the 5 GHz Frequency Band", http://www.hiperlan2.com/web/pdf/whitepaper.pdf

[12] HomeRF Working Group, "HomeRF Technical Overview Presentation", http://www.homerf.org/data/tech/techpres.pdf

[13] IP Security Protocol Charter, "IP Security Protocol", http://www.ietf.org/html.charters/ipsec-charter.html

[14] R. Droms, "Dynamic Host Configuration Protocl", IETF RFC 2131.

[15] W. Richard Stevens, "TCP/IP Illustrated, Volume 1", Addison-Wesley Professional Computing Series.

[16] IEEE Standard, "1998 Edition (ISO/IEC 15802-3:1998), IEEE Standard for Information technology–Telecommunications and information exchange between systems–IEEE standard for local and metropolitan area networks–Common specifications–Media access control (MAC) Bridges", IEEE standard 802.1D.

Biographies

Junbiao Zhang is currently a senior member of technical staff in the Thomson Multimedia Corporate Research, Princeton, New Jersey. Prior to joining Thomson, he was with the C&C Research Laboratories of NEC USA as a research staff member. He obtained his Ph.D and M.S.degrees, both in computer science, from Rutgers

University and his B.S. degree in computer science from the University of Science and Technology of China. His major research interests include 3G wireless/WLAN interworking, wireless LAN solutions,mobile applications, and content delivery networks.

Jun Li received his B.S. and M.S. degrees from Xidian University and Ph.D. degree from WINLAB, Rutgers University, respectively, all in electrical engineering. Since January 1986 he has worked for various R&D labs and industrial companies in China, Japan, and the United States. He is now with Corporate Research of Thomson Multimedia Inc., Princeton, New Jersey, working on wireless communication systems for high-value high-quality digital content delivery.

Stephen B. Weinstein served as President (1996-97) of the IEEE Communications Society. He received his B.S., M.S., and Ph.D. degrees in electrical engineering from MIT, the University of Michigan, and the University of California at Berkeley, respectively. He invented the echo cancellation technique used in telephone channel modems and was a pioneer in OFDM/DMT modulation. He is the author of several technical books on communication technologies and data networking. He is currently editor in chief of Journal of Communications and Networks (JCN).

Nan Tu is a research associate in the Computer and Communication Research Laboratories of NEC USA. He received his B.S. in computer science and mechanical engineering from Tsinghua University, China in 1996, and his M.S. in computer science from Rutgers University in 2001. His current research interests are high-speed networks, optical networks, and mobile networks.