On the Architecture of Authentication, Authorization, and Accounting for Real-Time Secondary Market Services

Yihong Zhou, Dapeng Wu, and Scott M. Nettles

***Abstract*— With the explosion of demand for wireless communication services, scarcity of spectrum poses a great challenge to wireless networking. However, recent field measurements show that a significant percentage of spectrum is under-utilized [1], [2], [3]. To address this problem, the research community introduced the concept of real-time secondary markets, where licensees are allowed to temporarily lease the spectrum unused by the primary users to secondary users. To support this new service, an Authentication, Authorization, and Accounting (AAA) mechanism must be in place to enable the licensees and secondary users to trade spectrum in a real-time manner. In this paper, we present an AAA system architecture, and propose a set of mechanisms to authenticate and authorize secondary users, synchronize multiple secondary devices, and manage real-time secondary market services. Furthermore, we address the accounting issue and examine the pricing strategies associated with accounting.**

***Index Terms*— Secondary market, authentication, authorization, accounting, pricing.**

I. Introduction

Radio spectrum is a limited resource. With the explosive growth of wireless communication technologies and increasing demand for wireless services, spectrum scarcity is becoming the most serious challenge facing the wireless industry. Demand is outstripping supply, especially in the most desirable range below three GHz [3], [4].

Ideally, spectrum scarcity should not be a barrier to the healthy growth of wireless businesses and technologies, and should not be a constraint on competition among commercial service providers. To address this issue, several technical solutions such as spectrum re-allocation, increasing spectrum efficiency, and spectrum sharing have been proposed [5]. Spectrum sharing is considered to be one of the key technologies in next generation communication systems [5] and it leads to the concept of a *secondary market*, where secondary spectrum users ask the license-holder for temporary access to the spectrum as needed, and the license-holder permits this sharing when and only when it determines that quality of service requirements can still be met for both the license holder and secondary users. Spectrum sharing will not only increase spectrum efficiency but also stimulate the licensees to adopt new technologies to improve spectrum efficiency.

In spectrum sharing, a primary market is represented by the initial distribution of a block of spectrum. A secondary market is represented by the trading of spectrum after the initial allocation [5]. A variation of this idea is the potential "lease" of under-utilized spectrum on a temporary basis to meet short or medium term demand for a particular service. In other words, spectrum resources could be traded just like wired bandwidth. Studies show that many frequency bands in the current distribution are rarely fully utilized [1], [2], [3]. This may be caused by a number of factors such as the licensee's business plan and service time (e.g., a TV station may not broadcast between 1 AM and 6 AM). By temporarily leasing the unused spectrum to those who need it (e.g., news reporters covering a sporting event or a political convention), more revenue can be generated for licensees. This motivates the Federal Communications Commission (FCC) to allow the development of the secondary market [3], [4].

Furthermore, Peha and Panichpapiboon [6] proposed a real-time secondary market, where secondary users are allowed to *temporarily* access the spectrum in a *real-time* manner, instead of going through a lengthy application to obtain the FCC's permission to trade the spectrum, a process that might take months. In this way, the secondary users can negotiate directly with the licensee, and use the available spectrum whenever they want. Without a doubt, such a short-cut procedure would greatly accelerate the application process, and promote the development of secondary markets.

To support this new service, an Authentication, Authorization, and Accounting (AAA) mechanism must be in place to enable the licensees and secondary users to trade spectrum in a real-time manner. However, the unique features of secondary market services pose new challenges in wireless network design. For example, the communications between secondary users are out of the control of the licensee's infrastructure. Thus, authentication and data communication needs a mechanism synchronizing all the secondary devices. We also need to develop a mechanism to manage the secondary services. Finally, we also have to address the issue of preventing unauthorized spectrum usage by secondary users.

In this paper, we explore this new area, propose an AAA system architecture, and present a set of schemes to tackle the aforementioned problems. In order to facilitate our descrip-

Yihong Zhou is with the Department of Electrical and Computer Engineering, The University of Texas at Austin, Austin, TX 78712, Email: zyihong@ece.utexas.edu

Please direct all correspondence to Prof. Dapeng Wu, University of Florida, Dept. of Electrical & Computer Engineering, P.O.Box 116130, Gainesville, FL 32611-6130, USA. Tel. (352) 392-4954, Fax (352) 392-0044, Email: wu@ece.ufl.edu. URL: http://www.wu.ece.ufl.edu

Prof. Scott M. Nettles is with the Department of Electrical and Computer Engineering, The University of Texas at Austin, Austin, TX 78712, Email:nettles@ece.utexas.edu. URL: http://www.ece.utexas.edu/~nettles

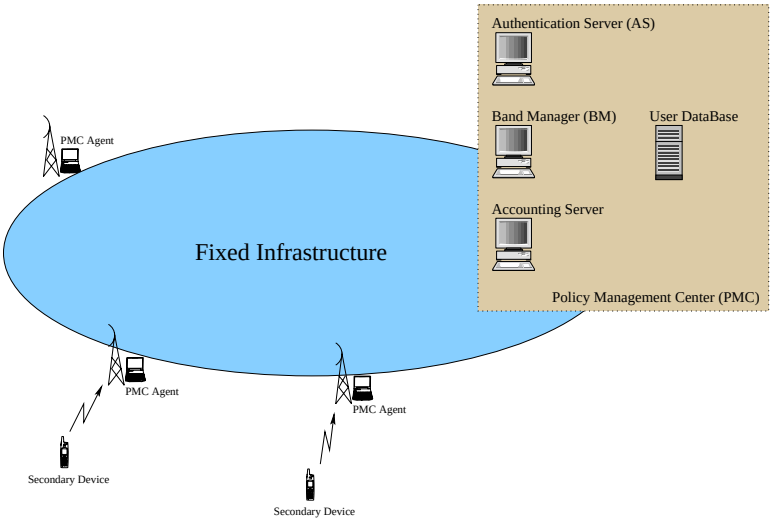

Fig. 1. AAA system architecture

tion, we use cellular networks as an example to present the mechanisms. However, our mechanisms can also be applied to other radio networks.

The rest of the paper is organized as follows. We present an AAA system architecture in Section II, and our authentication/authorization protocols in Section III. Service management mechanisms are discussed in Section IV. In Section V, we analyze the security issues associated with the proposed protocols. Accounting and pricing issues are addressed in Section VI. We conclude the paper in Section VII.

II. System Architecture

In this section, we first present an AAA system architecture, and then state several assumptions about the secondary market services. These form the basis of our further discussion.

A. System Architecture

Fig. 1 shows our AAA system architecture, which consists of a radio network infrastructure and a Policy Management Center (PMC). The PMC consists of an Authentication Server (AS), a user database, a Band Manager (BM), and an accounting server. The AS is responsible for authenticating legitimate users. The BM is in charge of spectrum management. Once a user is authenticated and its service requirement is determined to be acceptable, the BM authorizes the user by issuing a registration ticket, with which the user can communicate with others under the monitoring of the local PMC agents. The accounting server takes care of accounting and billing issues. Since different pricing strategies have different accounting requirements, we will discuss pricing issues in detail in Section VI.

The fixed infrastructure consists of base stations, mobile switching centers, etc. Moreover, a PMC agent is installed in each base station. The PMC agent forwards control messages between the secondary devices and the PMC, periodically broadcasts messages in its local area, and monitors spectrum usage.

In order to prevent the PMC from being overloaded, we assign most of the service management tasks, such as handoff management and monitoring, to PMC agents located in the base stations. Thus, a PMC agent is responsible for local secondary service management.

In the rest of this paper, we use the notations in table I.

B. Assumptions

We make three basic assumptions. First, as in [6], we assume that a wireless broadcast control channel exists between a secondary user and the licensee. Through this control channel, the secondary user can send authentication requests and receive replies whenever services are desired. It is not necessary for the licensee to deploy a widely covered network infrastructure just to provide the control channel. As an alternative, a licensee can lease wireless communication channels from a third party.

Second, we assume that all secondary devices follow the etiquette of “inquire before use” or “listen before use” [7]. Devices listen to the Channel Allocation Information (CAI), and transmit only after the channel has been allocated to them.

Finally, a key technology to the secondary market is Software Defined Radio (SDR) [8]. We assume that secondary devices are able to dynamically adjust radio waveforms according to the spectrum template required by the FCC.

In addition to our three basic assumptions, we assume that communication between the PMC components and the PMC agents is secure. The description of the secure communication mechanisms between those components is outside the scope of this paper.

Finally, we assume that a Certification Authority (CA) is available to serve the secondary market service. It issues public-key certificates to legitimate entities including the AS, the BM, the PMC agents, and the legitimate users. The certificate is an electronic document used to identify the entity and to associate that identity with a public key. Therefore, the public-key can be verified by any other entity at anytime.

TABLE I
NOTATIONS

Symbol	Meaning
P_x	public key of entity x
P_x^{-1}	private key of entity x
$K_x(m)$	encrypt m with entity x's secrete key k_x by using symmetric crypto-system
$E_x(m)$	encrypt m with entity x's public key P_x by using asymmetric crypto-system
$D_x(m)$	decrypt m with entity x's private key P_x^{-1} by using asymmetric crypto-system
$H(m)$	one way hash function with input m

III. Authentication and Authorization

In this section, we present the authentication and authorization protocols for the secondary service. A secondary user group may have multiple transceiver devices distributed in different areas. It is not necessary for all secondary devices to authenticate with the AS. Instead, a delegate device (DDev) can be elected and the DDev can negotiate with the AS as a representative of the secondary user group. Meanwhile, all the other secondary devices should listen to the control channel in their local areas. Once the service requirements are accepted, authorization information will be broadcasted through the control channel by the local PMC agents. After this, all the secondary devices are synchronized, and can begin transmission.

A. Authentication

Basically, the existing authentication schemes can be classified into four categories [9]:

1) Challenge/response interactive authentication.
2) Authentication using synchronized data such as time stamps or increasing counters.
3) One-way authentication using a password.
4) Authentication using asymmetric crypto-systems.

The first three schemes are symmetric crypto-system authentication techniques. They are widely used in today's telecommunication systems, including GSM and PCS [10], [11]. However, they also leave the system vulnerable to some easily launched security attacks [12], [13]. For example, the security level of a challenge/response scheme depends on the randomness of the challenges. If repeated challenges are used, replay attacks may occur. The second scheme requires synchronization between the user and the authenticator. This requirement is hard to achieve in some situations. The third authentication scheme is typically used for a user to log on a machine.

Asymmetric crypto-systems have advantages compared to symmetric crypto-system in terms of key management, even though their energy consumption is higher and their computation efficiency is lower. The advantage of asymmetric crypto-system authentication is that it eliminates the centralized maintenance of the shared secret keys between the authenticator and requestors, and thus eliminates a potential security threat. Furthermore, asymmetric crypto-systems facilitate the shared-key distribution process, which is applied in section III-C.

Our proposed authentication protocol is based on an asymmetric crypto-system. We assume each secondary user group has a pair of public/private keys, and that the private key is only known by the DDev. We also assume that a random number (or secret key) r_1 is delivered to all the secondary devices through a secure channel.

When a secondary user group needs to use spectrum, the DDev sends a message to the AS. We use the following notations to describe this procedure.

$$DDev \rightarrow AS: \quad UID, P_u, certificate, E_{as}(UID, sreq, H(r_1), nonce, Sign_u)$$

The left hand side of the above notation denotes the direction of the message flow, while the right hand side represents the message format. Specifically, the message consists of four fields: the user group's identifier UID, its public key P_u, the public key certificate, and an authentication request. The authentication request is an AS-public-key-encrypted message that contains the UID, the service requirement parameters sreq, the hashed r_1, a nonce and the user's digital signature $Sign_u$. The nonce could be a timestamp or a monotonically increasing number. The sreq should contain the following information:

- Desired bandwidth
- Current Locations for all secondary devices
- Maximal transmit power
- Maximum tolerable interference level
- Estimated service duration

The current location is not necessarily the geographical position. Instead, it could be the unique ID of each cell, which is broadcasted by the local PMC agent through the control channel. All of the above information is used by the BM to determine if the service requirement is acceptable and that accepting the service requirement would not severely degrade current users' service quality.

Upon receiving the request, the AS verifies the UID, P_u and the certificate. It decrypts the authentication request with its private key P_{as}^{-1}, checks the freshness of the nonce, and verifies the user's signature. In this way, the secondary user group is authenticated.

B. Authorization

Once the user group is authenticated, the PMC should authorize the user group by issuing a registration ticket. We use the following notation for this procedure:

$$\begin{aligned} AS \rightarrow BM: &\quad UID, sreq, H(r_1) \\ BM \rightarrow PA_i \text{ (where } i \in \mathcal{B}\text{)}: &\quad TK_r \\ PA_i \text{ (where } i \in \mathcal{B}\text{) broadcasts}: &\quad TK_r \end{aligned}$$

where $TK_r = D_{bm}(UID, ID_{channels}, H(r_1), T_1)$; PA_i denotes PMC agent i; and $\mathcal{B}$ is the set of the indices of all the

PMC agents that are in charge of the cells where the secondary devices of the user group are located. Note that each cell has one PMC agent and the secondary devices of a user group could be scattered over multiple cells.

The protocol uses three secure communications as follows:

1) The AS forwards a message consisting of UID, sreq and $H(r_1)$ to the BM.
2) The BM checks the current network status and accepts the service requirement if admitting the secondary user group would not degrade current users' quality of service. The BM then allocates channels and assigns a lifetime T_1 to the requested service, indicating the duration of the service. The BM then generates a registration ticket TK_r by decrypting the UID, the IDs of the allocated channels, $H(r_1)$ and T_1 with its private key P_{bm}^{-1}, i.e., $TK_r = D_{bm}(UID, ID_{channels}, H(r_1), T_1)$. The purpose of using the ticket TK_r is to allow verification that the service request has been granted by the BM. Finally, ticket TK_r is then transmitted to the PMC agents PA_i (where $i \in \mathcal{B}$).
3) Upon receiving TK_r, PMC agent PA_i (where $i \in \mathcal{B}$) broadcasts TK_r periodically through the control channel in its local area. The secondary devices, which are listening to the control channel, receive TK_r, and retrieve the IDs of the allocated channels as well as the lifetime T_1 by encrypting TK_r with the BM's public key P_{bm}. Note that $E_{bm}(m)$ is an inverse operation of $D_{bm}(m)$. We use $E_{bm}(TK_r)$ to verify if TK_r is issued by the BM. In this way, TK_r can be authenticated by the secondary devices. Thereafter, the secondary devices can register with its local PMC agent by presenting the TK_r, as described next.

C. Registration

Registering with the local PMC agent is the last step before the secondary devices can start communications. The purpose of registration is to prevent illegitimate use of the spectrum by illegal users (see Section IV-B for our prevention mechanism). Based on the authenticated Diffie-Hellman principle [14], we design a registration protocol, which is described by the following notations:

PA_i (where $i \in \mathcal{B}$) broadcasts : $P_{PA_i}, certificate$
$SDev \rightarrow PA_i : E_{PA_i}(UID, r_1, TK_r, nonce)$
PA_i (where $i \in \mathcal{B}$) broadcasts :
$$UID, ID_{channels}, TK_m, Sign_{PA_i}$$

where $TK_m = K_{r_1}(k^{'}, T^{'})$; SDev denotes a secondary device; PA_i denotes PMC agent i; and $\mathcal{B}$ is the set of the indices of all the PMC agents that are in charge of the cells where the secondary devices of the user group are located.

This protocol works as follows.

1) PMC agent PA_i (where $i \in \mathcal{B}$) periodically broadcasts its public key P_{PA_i} and the certificate issued by the CA through the control channel (the certificate was mentioned in Section II-B). In this way, the validity of P_{PA_i} can be verified by the secondary devices.
2) A secondary sends a registration request to the local PMC agent PA_i; the registration request is a PA_i-public-key-encrypted message that contains the UID, r_1, TK_r and a nonce; here TK_r is the registration ticket obtained through the authorization protocol.
3) PMC agent PA_i decrypts the registration request message with its private key $P_{PA_i}^{-1}$, checks the freshness of the nonce, and retrieves r_1 and TK_r. It encrypts TK_r with the BM's public key P_{bm}, and compares $H(r_1)$ with the one contained in TK_r. If the two match, the PMC agent further checks the ticket lifetime T_1 and IDs of the allocated channels. If the PMC agent is able to allocate those channels specified by the IDs, it accepts this registration request, assigns a service lifetime $T^{'}$, generates a temporary session $k^{'}$, and creates a monitoring ticket $TK_m = K_{r1}(k^{'}, T^{'})$. Thereafter, PA_i broadcasts the Channel Allocation Information (CAI) packet through the control channel in its local area. The CAI consists of UID, IDs of the allocated channels, TK_m and the signature of PA_i.
4) the secondary devices, which are listening to the control channel, receive the CAI packet, verify the CAI packet through the signature $Sign_{PA_i}$, retrieve TK_m from the packet, decrypt TK_m with secret key r_1, and store $k^{'}$ for future use. From now on, PMC agent PA_i and the local secondary devices have a shared temporary session key $k^{'}$, and the secondary devices can start communicating over the allocated channels.

It is worth mentioning that a session key is valid only in a local cell. Different local cells may have different session keys. A secondary device needs to update its local session key when it enters another cell. Since TK_m is periodically broadcasted by a local PMC agent, a secondary device can receive a new TK_m when it moves into a new area.

IV. Service Management

To support quality of service and security for real-time secondary markets in cellular networks, service management is needed. In this section, we discuss three service management issues, namely, handoff, monitoring, and ticket renewal.

A. Handoff

A secondary device may move over multiple cells in cellular networks. When a secondary device enters a new cell, it should first search for the CAI information broadcasted by the local PMC agent. If the CAI packet is detected, the secondary device can use the allocated channels; otherwise, it needs to request permission for channel access from the local PMC agent through a handoff protocol.

The handoff protocol is the same as the registration protocol presented in Section III-C. That is, the secondary device requests a handoff by presenting its registration ticket TK_r and r1. The local PMC agent checks the ticket, and determines whether the specified channel can be allocated. If the local PMC agent accepts the handoff request, it will broadcast the CAI through the control channel; otherwise, it sends a message indicating rejection of the request, and the secondary device cannot access the licensed channel.

B. Monitoring

Monitoring the channel use of secondary users is necessary for the following reasons. First, unlike traditional telecommunication services, communication between secondary devices does not require the participation of the licensee's base stations or other network infrastructure. Hence, the licensee is unable to control channel access and prevent illegal use of the spectrum. So, a monitoring mechanism is needed to make sure that all the secondary users are authorized and that they use the specified channels only for a specified duration. Second, in order to increase spectrum efficiency, a cell needs to recycle the allocated channels when all the secondary devices handoff to other cells. To achieve this, the monitoring mechanism, actually a PMC agent, can periodically scan the channels, and recycle channels that have been idle for a certain amount of time.

In our monitoring mechanism, the session key $k^{'}$ exchanged during the registration/handoff process is used for monitoring purpose. The monitoring mechanism can be employed in two ways, namely, passive listening and active inquiring.

1) Passive Listening: For passive listening, we assume that a PMC agent is able to correctly decode the signal transmitted by the secondary devices.

Each message, sent by the secondary devices, should have a token appended. The token is the value of an one-way hash function H(x), the argument of which consists of the message, the UID, IDs of the allocated channels, and the session key $k^{'}$. It can be described by the following notation:

$$SDev: \qquad \{message, token\}$$

where $token = H(message, UID, ID_{channels}, k^{'})$ and $k^{'}$ is a temporary session key.

The PMC agent scans the channels and randomly selects some transmitted packets for decoding. It applies the decoded information to the same hash function H(x), and verifies the result with the token sent by the secondary device. If the two match, the secondary user is regarded as legal; otherwise, it is illegal. If an illegal user is detected, the PMC agent may send an alarm signal to the network administrator, and the administrator may search for the illegal user and punish it accordingly.

2) Active Inquiring: In active inquiring, the PMC agent challenges the secondary devices occasionally. One of the secondary devices replies with a response and proves its legality. If no response is received for a certain amount of time, the spectrum is regarded as idle and can be recycled. The protocol can be described by the following notation:

$$\begin{aligned} PA_i(\text{where } i \in \mathcal{B}): &\qquad P_{PA_i}, certificate \\ SDev: &\qquad E_{PA_i}(UID, r_1, TK_r, nonce) \end{aligned}$$

Here, PA_i denotes PMC agent i; and $\mathcal{B}$ is the set of the indices of all the PMC agents that are in charge of the cells where the secondary devices of the user group are located.

Now, we explain the protocol. First, the PMC agent broadcasts its public key P_{PA_i} as well as the certificate. Then, a secondary device replies with a response which is a PA_i-public-key-encrypted message that contains the UID, r_1, TK_r and a nonce. The PMC agent decrypts the response with its private key $P_{PA_i}^{-1}$, checks the freshness of the nonce, and checks TK_r. If $H(r_1)$ matches the one contained in TK_r, the secondary device is regarded as legal; otherwise, the secondary device is regarded as illegal and an alarm signal will be sent out to the administrator.

C. Renewal of Registration Tickets and Session Keys

A mechanism is needed to renew registration tickets and temporary session keys, since their lifetimes may expire or the network administrator may want to revoke registration tickets and session keys for security reasons. Next, we describe our schemes for renewing registration tickets and session keys.

1) Registration Ticket Renewal: We propose two ways to renew a registration ticket. In the first method, the BM revokes its public key/private key. Then, all the issued registration tickets become invalid. Therefore, all the secondary user groups must re-authenticate with the AS (using the protocols in Sections III-A and III-B) to obtain registration tickets.

In the second method, a secondary user initiates a ticket renewal. The protocol is described by the following notation:

$$\begin{aligned} &DDev \rightarrow BM: E_{bm}(UID, sreq, r_1, TK_r, H(r_2), nonce) \\ &BM \rightarrow PA_i \text{ (where } i \in \mathcal{B}): TK_r^{'} \\ &PA_i \text{ (where } i \in \mathcal{B}) \text{ broadcasts}: TK_r^{'} \end{aligned}$$

where $TK_r^{'} = D_{bm}(UID, ID_{channels}, H(r_2), T_2)$.

Now, we explain the protocol.

1) First, the delegate device DDev chooses a new random number r_2 and notifies all devices in a secure way such as face-to-face meeting or a secure mechanism for distributing a group key. With the BM's public key P_{bm}, the DDev then encrypts a message that consists of the UID, the sreq, the old random number r_1 and old TK_r, the hashed new random number $H(r_2)$ and a nonce.
2) Upon receiving the message from the DDev, the BM decrypts the message with its private key P_{bm}^{-1}, checks the freshness of the nonce, and verifies the user's legitimacy by checking r_1 and TK_r. Thereafter, it generates a new registration ticket $TK_r^{'}$ by encrypting the UID, the IDs of the allocated channels, $H(r_2)$ and a new lifetime T_2 with its private key, and sends the new ticket to the local PMC agents, which are indicated in sreq.
3) Finally, PMC agent PA_i (where $i \in \mathcal{B}$) broadcasts $TK_r^{'}$ through the control channel so that all the local secondary devices can receive and update the registration ticket.

2) Session Key Renewal: We propose two ways to renew a session key. In the first method, the BM revokes its public key/private key. Then, all the issued registration tickets become invalid. If a registration ticket is revoked, the subsequence registration and handoff cannot proceed. Therefore, all the secondary user groups have to re-authenticate with the AS (using the protocol in Section III-B) to obtain registration tickets, and re-register with the local PMC agents (using the protocol in Section III-C) to obtain session keys.

In the second method, a secondary user initiates a session key renewal. It can renew the session key through the registration protocol. Then, a new monitoring ticket $TK_m^{'}$ is broadcast

periodically by the local PMC agent. Finally, all the local secondary devices update their session keys by decrypting the $TK_m^{'}$ with the group key r_1.

V. Security Analysis

Since some of our protocols are based on asymmetric cryptography, it is extremely important for the requester to correctly recognize the authenticator's public key, which can be verified by the certificate issued by the Certification Authority (CA). To achieve this, each PMC agent needs to periodically broadcast its public key and the certificate signed by the CA through the control channel, so that all the secondary devices in the local area can receive and verify the public key. Moreover, secondary devices can also verify the public keys of the AS and BM through the CA.

To counter replay attacks, we introduce a nonce into each protocol. The nonce monotonically increases, and it could be a time-stamp or a counter so that every request packet is unique. Therefore, adversaries have no way to eavesdrop on the previous packet and successfully replay it later.

VI. Accounting and Pricing Issues

Accounting mechanisms in real-time secondary markets are closely related to the pricing strategy of the service provider since different pricing strategies have different accounting requirements. There are two types of pricing, namely, usage-based and flat-rate pricing.

Under usage based pricing, a user is charged based on how much resource it actually consumes. Studies have shown that this kind of pricing is good for improving service quality [15]. However, the accounting overhead incurred is substantial, especially for the secondary market services. This is because not only the start time and the end time, but also the consumed bandwidth and the affected area have to be recorded. Since communications between secondary devices are out of the control of the licensee's network infrastructure, it is difficult to capture the end time accurately.

At present, most service providers prefer flat-rate pricing, under which a user is charged with a flat (generally monthly) fee. Although this pricing scheme leads to problems such as unfairness, which causes light users to subsidize heavy users [15], it eliminates accounting overhead and reduces operational cost and accounting-equipment investment. For this reason, flat-rate pricing is favored by most service providers.

In this section, we briefly discuss two flat-rate pricing models based on two different assumptions. First, if the licensee allocates spectrum from a band that carries primary services, the charge for the secondary service should at least compensate for the lost profit from primary services. Second, as we mentioned in Section I, if the spectrum is allocated from a band that carries no primary services (e.g., the licensee has not been able to deploy primary services due to business plans or shortage of funds), the price should be calculated in a way that maximizes the profit for service providers and maximizes the utility for secondary users.

A. Flat Rate Pricing Model 1

If the licensee allocates spectrum from a band that carries primary services, the lost profits should be compensated by the profits from secondary services. We assume R_s is the monthly fee for a secondary user, and R_p (\$/month) is the monthly fee for a primary user.

Assume A_0 and A_1 are the admissible traffic before and after allocating the spectrum to a secondary user. Given the blocking rate B and the total number of channels C_0, A_0 can be calculated with the Erlang B equation [16]. Also, A_1 can be calculated with the Erlang B equation, given B and the number of channels allocated to secondary users.

Assume A_u is the average traffic generated by a primary user. The monthly fee for the secondary users should be at least:

$$R_s = \frac{A_0 - A_1}{A_u} \times R_p(\$/cell/month) \tag{1}$$

R_s is the even point of profit compensation, because the secondary user group is served by blocking $\frac{A_0 - A_1}{A_u}$ number of primary users. Here, the unit of R_s is \$/cell/month. Therefore, the actual charge for the secondary user depends on the maximum number of cells it may use at one time.

B. Flat Rate Pricing Model 2

In most cases, licensees are reluctant to trade spectrum that has been deployed for primary services. They are more likely to lease spectrum in which primary services have not been deployed. In this scenario, we should use optimization theory to address the pricing issue as mentioned in [17].

Basically, the benefits of the service provider and the benefits of the user are conflicting. The service provider wants to provide low quality service with high price, whereas the user wants to choose a high quality service with low price. Therefore, the price and service quality should be carefully chosen to strike the best trade-off between the profits of service provider and the user's satisfaction. We describe our derivation for the best operating point in the trade-off as below.

Assume there are multiple competitive secondary service providers. All of them have spectrum resources in the same area. For cellular networks, we use the blocking rate B to measure the service quality. If, in a certain area (one cell), a service provider has a total of K channels and n registered secondary user groups. If each secondary user group needs x_i channels, the service provider can sell a total number of $X = \sum_{i=1}^{n} x_i$ channels. Assume the average traffic load generated in one channel is A_c. The total traffic load that the service provider needs to support is $A = XA_c$. Given A_c, the blocking rate B is a function of X (i.e. A) and K, denoted by $B(X, K)$, which satisfies the Erlang B equation [16].

Let R_s (\$/channel/cell/month) be the monthly charge to a secondary user for using one channel in one cell at a time. If different quality of service results in a different charge, R_s is a function of the blocking rate B, denoted by $p(B)$.

Let $c(K)$ be the average cost of maintaining K channels in a cell. We assume the service provider's profit function is:

$$\Gamma_{profit} = p(B)X - c(K) \quad (2)$$

This is the monthly profit of one cell with K channels. To maximize the profit, we set the derivative of Γ_{profit} w.r.t. X equal to zero, i.e.,

$$\frac{\partial \Gamma_{profit}}{\partial X} = p(B) + p'(B)\frac{\partial B(X,K)}{\partial X}X = 0 \quad (3)$$

So, we have

$$p(B) = -p'(B)\frac{\partial B(X,K)}{\partial X}X \quad (4)$$

Now, let's consider the user's concern. Denote n the total number of secondary users in the cell. Let x_i be the number of channels that a secondary user i ($i \in \{1, 2, \cdots, n\}$) is using in the cell. We assume the user's utility function U is given by:

$$U = u(x_i) - \gamma B - p(B)x_i \quad (5)$$

where $u(x_i)$ is the utility created by x_i channels; γ is the conversion factor that converts the blocking probability B to a cost in the same unit of utility; and $p(B)x_i$ is the cost incurred by using x_i channels. A user can switch to a different service provider, which results in a different blocking rate B. To maximize the utility function, we set the derivative of U w.r.t. B equal to zero, i.e.,

$$\frac{\partial U}{\partial B} = -\gamma - p'(B)x_i = 0 \quad (6)$$

So, we have

$$p'(B)x_i = -\gamma, \quad \forall i \in \{1, 2, \cdots, n\}. \quad (7)$$

Since $X = \sum_{i=1}^{n} x_i$, adding up equation (7) over all the users, we have:

$$p'(B)X = -n\gamma \quad (8)$$

That is,

$$p'(B) = -\frac{n\gamma}{X} \quad (9)$$

Plugging the above equation into equation (4), we obtain

$$R_s = p(B) = n\gamma\frac{\partial B(X,K)}{\partial X}(\$/channel/cell/month) \quad (10)$$

The value R_s obtained in (10) is the optimal price that best trades off the blocking probability with the price from a user perspective. Finally, the actual charge to a secondary user depends on the maximal number of channels and cells they use at one time.

VII. Conclusions

In this paper, we presented an AAA system architecture, and proposed a set of security mechanisms for real-time secondary market services. We addressed the issues of authenticating and authorizing secondary users, synchronizing a group of secondary devices, managing handoff, and detecting unauthorized spectrum usage. Furthermore, we studied pricing strategies and accounting issues, and proposed two flat-rate pricing strategies based on two different assumptions.

Although all of our discussions in this paper are based on the cellular network environment, we believe the proposed schemes are also applicable to other types of radio networks.

Since real-time secondary market services is a new area, many open issues such as location privacy and electronic payment methods, need to be addressed, and we leave these for future studies.

References

[1] FCC discusses secondary markets for wireless spectrum. [Online]. Available: http://www.techlawjournal.com/telecom/20001110a.asp

[2] FCC takes steps to make more spectrum available through the developement of secondary markets. [Online]. Available: http://www.fcc.gov/Bureaus/Engineering_Technology/News_Releases /2000/nret0012.html

[3] F. C. Commission, "Secondary markets spectrum initiative policy statement," *Policy Statement (FCC 00-401)*, 2000.

[4] ——, "Promoting efficient use of spectrum through elimination of barriers to the developement of secondary markets," *Notice of Proposed Rule Making (FCC 00-402)*, 2000.

[5] D. N. Hatfield, "Perspectives on the next generation of communications," in *Opening Plenary Session of VTS*, Sept. 2000. [Online]. Available: www.fcc.gov/oet/speeches/perspec_next_generation.doc

[6] J. M. Peha and S. Panichpapiboon, "Real-time secondary markets for spectrum," in *Proceedings of the 31st Telecommunications Policy Research Conference (TPRC)*, Sept. 2003.

[7] D. P. Satapathy and J. M. Peha, "Etiquette modification for unlicensed spectrum: Approach and impact," in *Proceedings of the IEEE Vehicular Technology Conference*, vol. 1, May 1998.

[8] Improving spectrum usage through cognitive radio technology. [Online]. Available: www.ieeeusa.com/policy/positions/cognitiveradio.asp

[9] S. Suzuki and K. Nakada, "An authentication technique based on distributed security management for the global mobility network," *IEEE Journal on Selected Areas in Communications*, vol. 15, no. 3, Oct. 1997.

[10] ETSI, *Recommendation GSM 03.20: Security related network functions*.

[11] TSB51, *Cellular Radio Telecommunications Intersystem Operations: Authentication, Signaling Message Encryption and Voice Privacy*, May 1993.

[12] C.-C. Lee, M.-S. Hwang, and W.-P. Yang, "Extension of authentication protocol for GSM," *Proceedings of Communications, IEEE*, vol. 150, no. 2, Apr. 2003.

[13] S. Patel, "Weaknesses of north american wireless authentication protocol," *IEEE Wireless Communications*, vol. 4, no. 3, June 1997.

[14] C. Kaufman, R. Perlma, and M. Speciner, *Network security: private communication in a public world, 2nd Edition*. Prentice-Hall, 2002.

[15] R. Edell and P. Varaiya, "Providing internet access: What we learn from index," *Network, IEEE*, vol. 13, no. 5, Sept. 1999.

[16] T. S. Rappaport, *Wireless Communications, Principles and Practice, 2nd Edition*. Prentice Hall, 2002.

[17] J. K. MacKie-Mason and H. R. Varian, "Pricing the internet," WUSTL, Tech. Rep., 1994.

PLACE PHOTO HERE

Yihong Zhou is a PhD student in the department of Electrical and Computer Engineering at The University of Texas at Austin. She also received her ME and BE degree in the Department of Computer Engineering from Beijing University of Posts and Telecommunications in 1993 and 1998 respectively. Her current research interests are spatial usage and power control in multi-hop wireless networks. She is also interested in wireless network security.

PLACE PHOTO HERE

Dapeng Wu received B.E. in Electrical Engineering from Huazhong University of Science and Technology, Wuhan, China, in 1990, M.E. in Electrical Engineering from Beijing University of Posts and Telecommunications, Beijing, China, in 1997, and Ph.D. in Electrical and Computer Engineering from Carnegie Mellon University, Pittsburgh, PA, in 2003. From July 1997 to December 1999, he conducted graduate research at Polytechnic University, Brooklyn, New York. During the summers of 1998, 1999 and 2000, he conducted research at Fujitsu Laboratories of America, Sunnyvale, California, on architectures and traffic management algorithms in the Internet and wireless networks for multimedia applications.

Since August 2003, he has been with Electrical and Computer Engineering Department at University of Florida, Gainesville, FL, as an Assistant Professor. His research interests are in the areas of networking, communications, multimedia, signal processing, and information and network security. He received the IEEE Circuits and Systems for Video Technology (CSVT) Transactions Best Paper Award for Year 2001.

Currently, he is an Associate Editor for the IEEE Transactions on Vehicular Technology and Associate Editor for International Journal of Ad Hoc and Ubiquitous Computing. He served as Program Chair for IEEE/ACM First International Workshop on Broadband Wireless Services and Applications (BroadWISE 2004); and as TPC member of over 20 conferences such as IEEE INFOCOM'05, IEEE ICC'05, IEEE WCNC'05, and IEEE Globecom'04. He is Vice Chair of Mobile and wireless multimedia Interest Group (MobIG), Technical Committee on Multimedia Communications, IEEE Communications Society. He is a member of the Award Committee, Technical Committee on Multimedia Communications, IEEE Communications Society. He is also Director of Communications, IEEE Gainesville Section.

PLACE PHOTO HERE

Scott Nettles is an Assistant Professor in the Department of Electrical and Computer Engineering at The University of Texas at Austin. He received his B.S. in Chemistry from Michigan State University in 1981. He received his M.S. in 1992 and his Ph.D. in 1996 both in Computer Science from Carnegie Mellon University. His research interests include persistence, high-performance garbage collection, highly programmable "active" networks, and wireless networking. His most recent focus has been on the design and implementation of wireless MAC's.