Here

Contents

- 1 Femtozone Services
- 2 Interference
  - 2.1 Co-Layer Interference
  - 2.2 Cross-Layer Interference
  - 2.3 Interference mitigation techniques for femtocells
- 3 Femtocell Issues
  - 3.1 Security Solution
    - 3.1.1 IPsec
    - 3.1.2 Extensible Authentication Protocol
    - 3.1.3 Femtocell Secure Authentication
      - 3.1.3.1 X.509 Authentication
      - 3.1.3.2 SIM Card Authentication
  - 3.2 Femtocell Location Solution
  - 3.3 Need for New Applications
  - 3.4 Development of New Applications
    - 3.4.1 Femtozone Services
    - 3.4.2 Connected Home Services
    - 3.4.3 Femtocell API

Femtozone Services

- **Family Alert Service:** When a family member arrives home or leaves, the femtocell automatically sends an SMS message. For example, a parent at work can be notified that their child has arrived home from school.
- **Virtual Home Number:** A ?home? phone number that rings on all the handsets at home when a call comes in to that number.
- **Media Synchronization:** Ability to synchronize music tracks and video clips automatically between a mobile handset and a home PC.
- **Photo Upload:** Ability to upload photos automatically from the handset to a home PC when handset arrives home and display the photos to a digital picture frame.
- **Contact/Calendar Synchronization:** Ability to synchronize handset calendar/contacts with home personal and family calendars/contacts every time the handset arrives home.
- **Remote Control:** Ability of the mobile phone to function as a remote control for home devices (DVR, DVD, TV) when it is in the home.
- **Mobile Video:** Ability to stream videos from DVR/DVD player directly to your mobile phone.
- **Family Tablet:** Ability to enable a group of family communication features on an in-home display to show the geographic locations of household members, display household calendar and reminder messages, access voicemail and text messages, and store and display pictures from the mobile phone.
- **Point-of-Sale promotion:** Femtocells in retail spaces allow merchants to detect customers? presence and provide welcome messages, coupons, and store directory services.
- **Virtual PBX:** In an office setting, the femtocell combined with IP-PBX software on the corporate network can make mobile phones into virtual extensions on the office phone system.

Source:Femtozone Service Library

Interference

Co-Layer Interference

Co-layer interference is described as the unwanted signal received at a femtocell and sent from other femtocells, decreasing thus the quality of its communication. The name co-layer makes reference to the fact that all femtocells belong to the same network layer, unlike other elements like base stations, NodeBs and so on, which belong to the macrocell layer. Co-layer interference occurs mainly between inmediate neighbours due to low isolation between houses and appartments.

Cross-Layer Interference

In two-layer networks, an interfering signal is assumed to produce cross-layer interference if the aggressor and the victim systems belong to different layers of the network. For example, the distortion caused by an emitting FAP (member of the femtocell layer) at the downlink of one or several macrocells (members of the macrocell layer) is a clear case of cross-layer interference. Likewise, it can also be considered as cross-layer interference if the distortion is caused by a macrocell user (member of the macrocell layer) at the uplink of a nearby FAP (member of the femtocell layer). Cross-layer interference is a problem especially in CDMA co-channel deployed two-layer networks, due to the fact that both femtocells and macrocells use the same frequency band.

Interference mitigation techniques for femtocells

Mitigation technique	Explanation and usage
Channel assignment	The network assigns users who are not part of the femtocell subscriber group to the most appropriate channel. Users who are on the macrocell can avoid femtocell dead zones. Femtocell users can be assigned different channels to avoid interference in overlapping coverage areas
Downlink power management (i.e. automatic gain control)	The femtocell transmit power is adjusted to give an appropriate trade-off between coverage and interference at a given location. This may be done using direct measurements of both the uplink and downlink channels and using measurements taken by both femtocells and user equipments to provide enhanced accuracy. The levels may also be varied over time in response to changing conditions
Power capping of user maximum transmit power	The femtocell sends a broadcast message to mobiles in its coverage to ensure a given maximum transmit power is never exceeded. As users leave the femtocell coverage, they are thus prevented from causing excessive uplink interference to the macrocells and the coverage area
Dynamic receiver gain management	An adaptive attenuation level is included in the femtocell receiver to reduce its gain when a strong co-channel (or adjacent channel) mobile is nearby, keeping the receiver operating within its linear dynamic range and avoiding blocking while still providing sufficient sensitivity to detect mobile at the edge of femtocell coverage

Broad dynamic range specification and testing	Since mobiles can approach very close to femtocells, the strong signal-handling ability of the femtocell should be verified in conformance testing

Femtocell Issues

Security Solution

IPsec

IPsec is an Internet protocol, whose aim is to ensure security and authentication on the Internet. It operates on the third layer of the Open Systems Interconnection (OSI) model. The IPsec standard is defined by Internet Engineering Task Force (IETF). With IPsec, packets are divided into two parts: an IP header, and the data.

A security association protocol creates the security keys that will be used for encryption and to authenticate the two entities at the extremities of the tunnel. The creation of the keys is based on the secret shared concept, and a complex algorithm is responsible for sharing the secret between both entities.

Authentication Header (AH) is a protocol that provides authentication of the contents of the packet through the addition of a header that is calculated based on the content in the packet. It is based on checksums that depend on the keys defined by the security association. Which parts of the packet are used for the calculation, and the placement of the header depend on the mode (tunnel or transport) and the version of IP (v4 or v6). AH does not encrypt but only provides authentication.

Encapsulating Security Payload (ESP) ensures privacy by encrypting the data. This algorithm uses the key to combine the data in order to encrypt it. Only the security association users know the keys and are able to decrypt at the other side of the IPsec tunnel.

Extensible Authentication Protocol

EAP is a universal authentication framework frequently used in wireless networks. Many implementations have been proposed depending on the technologies. Few of them have been applied to femtocells and are implemented in the FGW to ensure security and authentication.

EAP-Transport Layer Security (TLS) is the most well known EAP, and is implemented by all wireless equipments. It is based on the use of a Public Key Infrastructure (PKI) to create and manage the digital certificates. EAP-TLS was formerly called EAP-Secure Socket Layer (SSL), and the last implementation is detailed in [9]. In this protocol, a certificate authority links the public keys with their respective users. The certificate can be established automatically by software or manually by the users themselves. The user, the keys, the certificates and their validity are managed by the PKI.

EAP-Subscriber Identity Module (SIM) is an implementation for GSM using a SIM card. It is defined in [10]. In this approach the shared information between the two entities is contained on the SIM card.

EAP-Authentication and Key Agreement (AKA) is used for UMTS combined with a Universal Subscriber Identity Module (USIM) card [11]. It is based upon symmetric keys and it includes optional user anonymity and reauthentication procedures.

EAP-Internet Key Exchange version 2 (IKEv2) is the improved version of EAP-Internet Key Exchange (IKE) proposed in 1998. It is a very secure solution that has the following options

Femtocell Secure Authentication

X.509 Authentication

X.509 certificates are usually used for authentication in IP-based networks. With such an approach, the sensitive information (i.e. the serial number) is stored in a specific hardware component called Trusted Platform Module (TPM). This element is a protected memory whose content can not be modified. With this approach, the identification of the FAP is defined at the manufacturing stage. When a customer purchases a FAP from an operator, the operator will associate this new customer to the serial number of the femtocell. The serial number information is given by the manufacturer directly to the operator, so that no other entity has access to this information. Later, when the customer uses his femtocell, its public key can only be used together with this serial number.

SIM Card Authentication

In this case the protected information to authenticate a user is stored in a SIM/USIM card, and this has to be installed inside the FAP (see Figure 9.6). In this approach, when a customer purchases a FAP from an operator, this operator will authenticate the user thanks to the information stored in both the SIM/USIM card and the Authentication, Authorization and Accounting (AAA) server.

Femtocell Location Solution

GPS positioning: some femtocell manufacturers have chosen to include a GPS receiver inside their equipment.GPS suffers low reception inside homes. However, the FAP is not expected to be moved often and so it could be possible for it to store the last received GPS coordinate in order to give a good estimation of the position of the FAP.

Cell sensing: the position could also be estimated using geolocalization methods. With such an approach the FAP senses the neighbouring macrocells, and uses triangulation methods, based on the received signal power or the time of arrival. With such information the FAP could estimate its position. However this solution is only possible if there are several macrocells in the surroundings of the femtocell.

TV signal: TV signals can be used not only for timing accuracy, but also to estimate the position of a FAP. The main advantage of such signals is that their levels are higher than GPS signals, and they use a wide range of frequencies, making them more efficient against fading. According to [15], it has been verified with measurements in the USA that using TV signals outperforms GPS, because of its cheaper price and higher accuracy. **Internet IP address:** it is possible to identify the location by the IP address of the Internet connection. However this information is not always reliable, unless the whole chain (Internet and mobile operator) work together to provide this information. In practice, IP addresses could be used when a unique operator offers a combined gateway incorporating the broadband router and the FAP.

Customer address: The last solution is to associate the home address of the subscriber to its FAP at the sale point. The advantage of this approach is that the exact address is located. The drawback is that the operator should be informed each time the subscriber moves to another location.

Need for New Applications

Indoor radio coverage: this was the initial goal of femtocells, i.e. ensuring a good radio coverage indoors, where the macrocell coverage was not sufficient. Cheap calls at home: for users already having a good indoor radio coverage, the concern is to have indoor calls at a lower price. It is also the main concern for enterprise femtocell deployment.

Mobile data: femtocells are not only aimed at voice, but also data services. Data services like video and web started to be widely used with UMA, which is why femtocells have to offer advanced data services.

Femtozone services: this kind of service is both voice/data, and is used automatically when the user is in the range of the femtocells. The operators are today very concerned about deploying such services.

Connected home services: a recent concern for customers is the concept of connected home. This is mainly the case with the scenario of gateway femtocells, were the services at home (like computer, phone, TV, printer, or camera) are all connected to the same box. In this case the phone can access mobile services via the femtocell.

Development of New Applications

Femtozone Services

Presence applications are based on the fact that customers always have their mobile phone with them. In such a case it is possible to initiate some automatic services each time the subscriber enters/leaves the range of their femtocells. For example, when a user enters his home, it could be possible to automatically upload all the new pictures in the mobile onto the home server. Another example could be for a mother to set up her child?s mobile, so that she will receive a Short Message Service (SMS) when the child arrives at home or leaves the house.

Virtual numbers can be added in the home. The calls would be managed only by the femtocell and not by the operator. Such numbers can be used to create groups of users inside the house. For example, a unique mobile number could be used to reach all the users inside the house.

Connected Home Services

The notion of connected home services aims at using the femtocell as a link between the mobile and the home network. Another idea would be to use the mobile to control some equipment like the TV. With connected home services, the mobile becomes a controller that helps to manage, via the FAP, all connected equipment inside the house. Such services could also help to diversify the role of the mobile, thus making more revenue for the operators.

Femtocell API

Femtocell applications can be implemented in different locations:

- in the FAP itself for most of the applications,
- in the handset that interacts with the FAP.

For those implemented in the FAP, the applications should be developed by the manufacturer. A good option could be that the operator provides an Application Programming Interface (API), in order to allow external companies easily to develop their software.