Journal of Information & Communication Technology
Vol. 6, No. 2, (Fall 2012) 27-32

Brief Overview on Femtocell Architecture & its Threats

Faisal Bin Ubaid *
GSAS Department, Baharia University, Islamabad, Pakistan

Adil Yasin *
GSAS Department, Baharia University, Islamabad, Pakistan

ABSTRACT

In cellular world new technology is being adopted namely Femtocell for simplification of network architecture to provide better coverage and increase performance. Femtocell is a small seamless integrated base station which is to be installed on user premises in order to connect user with network of his service provider by means of existing broadband connection. This enables service providers to have load balancing. But femtocells are also facing various potential security threats. The objective of this paper is to provide a comprehensive overview of femtocell architecture & its threats.

INSPEC Classification : B6250F, D4045, B6210, C5620

Keywords : Femtocell, HNB, Architecture, Threats.

1. INTRODUCTION

During recent years cellular network companies face numerous challenges when it comes to provide an effective coverage with high speed data rates to indoor users. Traditional macro base stations (BTS) provide limited coverage to indoor subscribers because they operate on high frequencies which reduce their ability to penetrate walls of those users who reside in deep urban environment. To overcome this problem femtocell can be installed in user home premises replacing traditional BTS. Just like any other plug and play device femtocell once installed in user's premises, it will provide high QOS services to users located in its surroundings meeting end user satisfaction and ultimately large revenue.

Due to more than two times the increase in data traffic (CNN Money. 2011) femtocells can also help network service provider by load balancing the traffic. Femtocell uses user internet broadband connection, which can be fiber optic, digital subscriber line (DSL) or

*The material presented by the authors does not necessarily portray the viewpoint of the editors and the management of the Institute of Business and Technology (IBT) or GSAS Department, Baharia University, Islamabad, Pakistan.

* Faisal Bin Ubaid : faisalubaid@mcs.edu.pk
* Adil Yasin : adeel_yasin1@yahoo.com

any other, as backhaul to connect user to its network provider. By doing so, network operator achieve load balancing which otherwise would be directly on the core network macro layer. Another added advantage of using femtocell compare to traditional BTS is that it minimizes the on air data traffic cost.

The 3rd Generation Partnership Project (3GPP) has following characteristics/considerations for femtocells:

- As femtocell will be installed on user premises so its size should be compact and its operating power must be small which should not affect user in term of electricity bill.
- Femtocells have small transmitting power ranging from 10 to 100 mW which is also lesser than Wifi whose transmitting power is approximately 1W. Moreover user's cellphone will also operate on lesser power levels for uplink as compare to traditional BTS scenario.
- Femtocell can support up to six users simultaneously maintaining high QOS.
- Femtocell installation procedure will be user friendly. It will help network operators to eliminate the need of sending installation team whenever new Femtocell is installed by user.
- Femtocell will operate on same license plan as on which network service provider operates.
- Cell phone which is going to be served by femtocell will be completely identical to the one serviced by traditional BTS.

As femtocell is providing high QOS so user can use his cellular phone for all communication requirements irrespective of his location. Where femtocells provide so many advantages, it also involves security threats.

This paper is divided into two parts. First part will describe architecture of femtocell while later part will throw light on its threats and in the end we conclude the paper along with countermeasures of threats.

2. Related Work

3GPP have named femtocell as an Home Node B or HNB. 3GPP and GSM association have worked on HNB deployment and also have worked on its security issues significantly (GSM Association, 2008), (C.-K.Han, H.K.Choi, I.H.Kim, 2009). Unfortunately there considerations regarding deployment issues and security threats are abstract.

3. Architecture

HNB architecture is illustrated in figure 1. Components of HNB architecture along with their functionality is explained below.

UE: UE (User Equipment) is nothing but a standard 3G communication device which interacts with HNB on air interface through mechanism namely AKA, Authentication and Key Agreement .

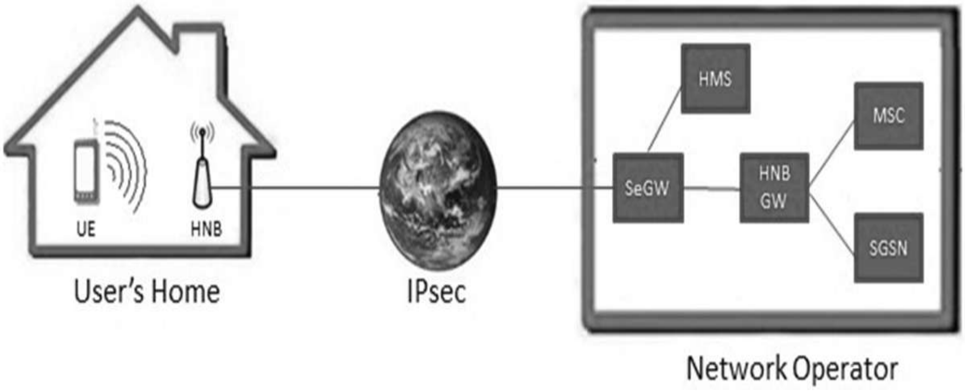
HNB: It acts as a BTS which interconnect user equipment to its service provider core network through radio/air interface. Like any other base station major features of HNB include Radio resource management, Firewall, Signaling, QOS, NAT, auto configuration and IP transport function.

SeGW: SeGW (Security Gateway) function is to have secure tunnel between HNB and core network with help of mutual authentication. After authentication HNB is registered in SeGW. Mutual Authentication can be carried out through by combination of Extensible Authentication Protocol, EAP-SIM certificates. It can also be authenticated by EAP-AKA.

HMS: HMS (HNB Management System) is a management module. Its function is to provide and configure the user data in compliance with the policies of network service provider. HMS module also includes AAA server (Authentication, Authorization and Accounting). It is important to note that HMS is deployed in network service provider core network.

HNB GW: HNB GW (HNB Gateway) perform access control functions on signaling, (includes mobile phone traffic), originating from the HNB. Major protocols which are used in this module are IPsec, TLS/SRTP and GAN (Transport Layer Security/Secure Real-time Transport Protocols, Generic Access Network)

Fig 1
HNB Architecture



4. Threats

The possible threats and there impacts which can be faced in real environment to HNB are summarized in this section. However there details can be find in (3rd Generation Partnership Project; 2009), with complete parameters like consequences of each threat to various assets or there impact level.

"Compromise of HNB Authentication Token"

HNB authentication token can be compromised by brute force attack or by reading authentication credentials through local physical intrusion. Afterwards this token can be used by attacker to pretend legit HNB to user cell phone or launch more attacks which can involve eavesdropping user data.

"Configuration attacks on HNB"

HNB will be needing software updates with passage of time for optimization and other factors. If software distribution is compromised there is a chance that HNBs will receive and upgraded to fraud software whose consequences will be non-optimized functioning of HNB, DOS attacks, eavesdropping or spoofing.

Attacker can also change the access list if HNB is misconfigured or having access to authentication token afterwards resulting in not allowing legit users to access HNB.

"Attacks on OAM & its Traffic"

OAM, Operation & maintenance center despite having very secure protocols, they are still open because of open ports through which attacker can access link between HNB and OAM. This threat can have adverse impacts like Men in middle attack or attacks described earlier like DOS attack, fraud software update and misconfiguration of HNB.

"Men in Middle Attack during HNB first network access"

When HNB make very first time contact to service provider core network, there is a possibility that attacker can intercept the communication between them and later it can masquerade HNB. This threat involves impact like sending data on behalf of any party or eavesdropping.

"Threats of HNB network access"

Rouge HNB can be setup (Nico Golde, Kevin Redon and Ravishankar Borgaonkar, 2012), and it can gain network accessibility. Afterwards this rouge HNB can spoof or eavesdrop of those users who are registered with it. This can be mitigated to some extent by HNB SeGW to check access rights of HNB.

"Changing HNB location without reporting"

Buyer of HNB can vary the position of its HNB making its provisioned location information invalid. This can impact on frequency planning of other operator in newly displaced position of HNB. In various countries it also violates frequency allocations requirements. The most worth mentioning impact is that HNB can no longer be used for emergency call because it can't be reliably relocated.

"Eavesdropping of the other user's E-UTRAN user data"

HNB configured in "open access" mode intentionally by attacker results in eavesdropping of user communication with its core network. Eavesdropping is carried out by reading data, which is neither available unprotected on air-interface, nor with IP-interface security. Impact of this threat depends upon confidentiality and sensitivity of data communicated.

"Masquerade as other users"

This threat is similar in a manner to threat described earlier i.e. Masquerade as other users. The only difference is that in "Masquerade as other users", attacker not only eavesdropping but also spoofing the data.

"Masquerade as a valid HNB"

Attacker can configure its HNB in a complete similar manner as target HNB to which it want to impersonate. Afterward attacker can have access to user keys or attacker can change HNB configuration to integrity level or no encryption at all.

Table 1
A table is illustrated with threats discussed above and their countermeasure is given below.

Security threats	Countermeasure
Compromise HNB authentication token	Authentication credentials of the HNB shall be stored inside trusted platform module
User cloning the HNB authentication token	The users could be required to obviously confirm their acceptance before being joined to HNB
Fraud software update/ configuration changes	All software and configuration changes shall be cryptographically signed by OAM
Mis-configuration and compromise of ACL	Secure means of creation, maintenance and storage of Acl and software distribution is required.
Men in the middle attacks on HNB first network access	HNB's credentials shall be recognized at the core network operator's side
Attack on OAM and its traffic	The communication between the HNB and the OAM should be secured
Threat of HNB network access	SeGW in core network should have the related profile information of HNB to check whether a HNB can access the network
Changing of the HNB location without reporting	Location locking mechanism shall be designed and implemented
Eavesdropping of the other user's E-UTRAN user data	The user could be notified when the UE camps on a closed or open access type HNB
Masquerade as other users	Same as above threat
Masquerade as a valid HNB	Related configuration should be hidden

5. Conclusion & Future work

In this paper we have briefly overviewed femtocell architecture and threats involved to it. There is no doubt that it is an emerging technology which not only offer high data rate but also provide load balancing for network service providers. In present deployed 3G femtocells are larger than traditional base transceiver stations. However femtocells are facing various threats when placed in unworthy hands. It is impossible for network service provider to prevent users from being attacked as all communication occurs outside the space of network service provider. Future work can be carried out on additional security mechanisms to increase performance of femtocells against threats.

6. References

CNN Money. 2011 "4G won't solve 3G's problems". [Online] Available: http://money.cnn.com/2011/03/29/technology/4g_lte/index.htm

The Femto Forum, 2010, "Wireless in Home & Offce", [Online] Available: www.femtoforum.org

GSM Association, 2008, Security Issues in HNB Deployment. Technical report, July (2008)

C.-K.Han, H.-K.Choi,I.H.Kim, 2009, Building femtocell more secure with improved proxy signature. In Global \Telecommunications Conference, 2009

3rd Generation Partnership Project; 2009, Technical Specification Group Services and System Aspects; Security of H(e)NB (Rel.8), 3GPP TR 33.820 v1.3.0, Jan. (2009)

Nico Golde, Kevin Redon and Ravishankar Borgaonkar, 2012, "Weaponizing Femtocells: The Effect of Rogue Devices on Mobile Telecommunications" In the Proceedings of the 19th Annual Network and Distributed System Security Symposium, (NDSS 2012), San Diego, February (2012)