Indian Journal of Science and Technology, *Vol 7(S4), 46–51, April 2014*

ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Securing the Femtocells: Anonymity and Location Privacy

Marc del Valle[1*], B. Manikandan[2] and V. S. Shankar Sriram[2]

[1]ETSETB, Universitat Politècnica de Catalunya, Barcelona, Spain; mrofthevalley@gmail.com
[2]School of Computing, SASTRA University, Thanjavur, India ;
manik.balki@gmail.com, sriram@it.sastra.edu

Abstract

Femtocells have been proposed as solution for high-speed mobile network (i.e. LTE) bandwidth requirements. Research work in the field of securing femtocells is still in its infant stage. In this research contribution an attempt has been done to identify and mitigate a possible attack in the femtocells where locational information about a femtocell user is disclosed. The proposed mechanism notifies the femto entity under threat about the attack. Also a novel Multi-hop algorithm has been proposed to hide the details of the communicating parties from the attacker.

Keywords: Femtocell, Mobile Cellular Network, Mobile User Location, Multi-hops Algorithm, Security, Small Cells

1. Introduction

Nowadays users are expecting for more features in their devices. More and more users and de- vices are being introduced into the network every day. Carriers have the responsibility to pro- vide better throughput and bandwidth to the users of the wireless network. The implementation of femtocells into the network is also pro-posed as a better solution, since this technique is able to recycle the frequency slots used by macro cell users in a specified range and transferring the data through the Internet to the Mobile Core Network (MCN), which results in achieving high bandwidth at low cost, satisfying the network users. Further details about mechanisms and architecture can be found in 3GPP Technical Report 3rd Generation Partnership Project[1].

Femtocells Access Points (FAP) are designed for indoor deployments. Recent research extends the deployment to outdoor as well[2]. Generally the implementation is owned by users who want to increase throughput in their office or home and by users who have low coverage in their buildings.

Different kinds of femtocell network approaches are possible. They are closed femtocell, open femtocell and hybrid femtocell. The differences are basically in the kind of users who can join the femtocells. In closed femtocells only a group of authorized users are able to join the FAP, and authentication process is required in this kind of closed femtocells. Although the fact that any person, malicious or not, is able to get an authorization from the operator, malicious users can also appear in these femtocells. On the other hand there are open femtocells that let every user join the network, which does not demand authentication. This kind of scenario will be commonly used when the femtocells are deployed in public places, where everyone should be able to access the network. The hybrid femtocells appear in order to maximize the spectrum usage. In this approach registered users have the preference to access FAP and there is possibility for non-registered users as well, to join the network if there still resources available. The methodologies addressed in this paper can work on all the three scenarios, since the practical femtocell network will include in it all different kind of femtocells access points.

**Author for correspondence*

Researchers mainly have focused on interferences between macrocells and femtocell network users. Other different scenarios have been proposed and various solutions are also available in the literature, regarding spectrum sharing techniques, misbehaving femtocells, user interferences, etc. In the security domain only a few concrete contributions have come from the research community. Malone et al.[3] demonstrated how an attacker can trace the packets in different femtocell, and then find correlation between femtocells traffic flows. One other contribution from DePerry et al.[4] had demonstrated how to hack a FAP.

This paper attempts to address security issues in femtocells from a different perspective. The security concerns addressed in this paper mainly focus on user location privacy and non disclosure of user identity.

The rest of the article is structured as follows; Section 2 summarizes the security issues identified in femtocells and introduces the possibility of new ones. Section 3 proposes mitigation mechanisms against those security issues in the form of two novel algorithms. After discussing about solutions we provide simulation results in Section 4. Section 5 concludes this paper and points out avenues for future work.

2. Security Threats in Femtocells

2.1 Data Interception

DePerry et al.[4] demonstrated an idea of obtaining data from femtocell users, by joining the FAP and getting all the packets on transit. The authors give a practical approach of how to record a voice call and read SMS going on in a femtocell. Furthermore researchers were able to clone a device by using the information given to the femtocell by the device. In their work authors conclude that femtocells have many security issues and are not recommended for deployment in the current scenario.

2.2 Packets Correlation

A new security leak-age in femtocells network is presented by Malone et al.[3]. Rouge femtocells appear in this scenario, authors were able to identify each type of packet in the network by using these misbehaving FAP. With this knowledge an approach for correlating the packets in different femtocells is discussed. Both edges of a data transfer can be pointed out by the knowledge of ingoing and outgoing data in different femtocells correlation. In the same work three different solutions are proposed: dummy traffic, IMEI/IMSI verification and requesting the user for the decision to join the network. The requesting process was figured as the better solution since the user had the choice for the decision-making. The other securing approach proposed is addressed to the user identity; the transmitting user information is disclosed by correlating the on-going packets. In Section 3.2 collaborative work of the femtocell users is proposed to provide anonymity by using a novel algorithm.

2.3 Location Acknowledgment

User location privacy is ensured in the mobile network by using IMSI, which allows users identity to be secure. Using femtocell deployment, attackers could find a way of tracking the user since, Terayama et al.[5] location notification service is one of the new applications that FAPs are able to run. It is considered as a clear opportunity for attacker, who can disclose the user location to the attacker, by control-ling a single FAP. Furthermore by controlling geographically separated FAPs, attackers can be able to track user movement path by tracking the user joining along different femtocells. These scenarios represent a newfangled security issues for this devices. In Section 3.1 a countermeasure algorithm is proposed to mitigate these attacks.

Figure 1 presents the architecture which forms the basis of this investigation. As shown in the figure the attackers have gone one step forward and are able to hack femtocells remotely by using a backdoor entrance through internet network. An attacker might get access to the FAP, once accessed can be able to modify some lines of the FAP controller code. This modification would be able to reveal the backhaul traffic information to the attacker, which clearly represents security vulnerability in the FAP.

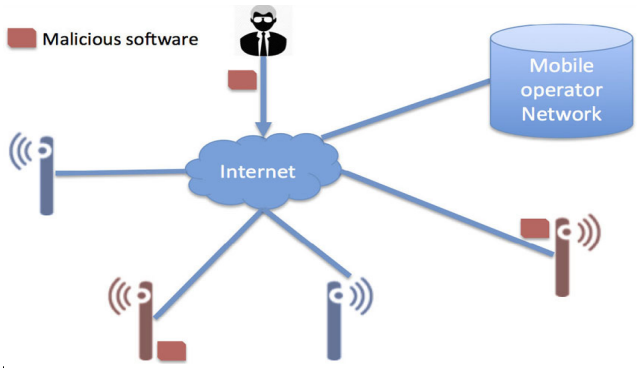

Figure 1. Remote femtocell attacking.

3. Two Tiers of Security

The two-tier security mechanism proposed are tracking notification which informs the user under threat about the attackers tracking move and a multi-hop algorithm that randomizes the packet flow thereby the origin of the packet is hidden.

3.1 Tracking Notification

A traffic monitoring device in the backhaul connection is needed to analyze the packet flow between the device and the internet network. The analysis of the traffic has to be done by the FAP at same time it is computing new joining requests, and also all the data transfers. Since the amount of users in a femtocell is typically between 1 and 16 users, this increase of computational operations can be afforded by the FAP. In Figure 2 the algorithm block diagram is presented. Once handover process is over, by monitoring backhaul interface FAP can decide about if user should join again. If after user rejoins same kind of packets appear in backhaul link, a pop-up message appears in the users device advising that its location might be compromised. Application like proposed by iSEC partners[4], which attempts to refuse femtocell connection, can be run after that notification appears.

Attacker can use dynamic algorithm to reformat the data that is updated, packet will be forwarded to malicious users. The implementation of a learning algorithm as a part of discussed algorithm helps to trace malicious user packets. Papageorgiou[6] discusses about cognitive learning, an opportunity for FAP to learn from known attacks and point out new ones, appears if applying this algorithm. Further work is needed to adapt this algorithm to the proposal made in this article.

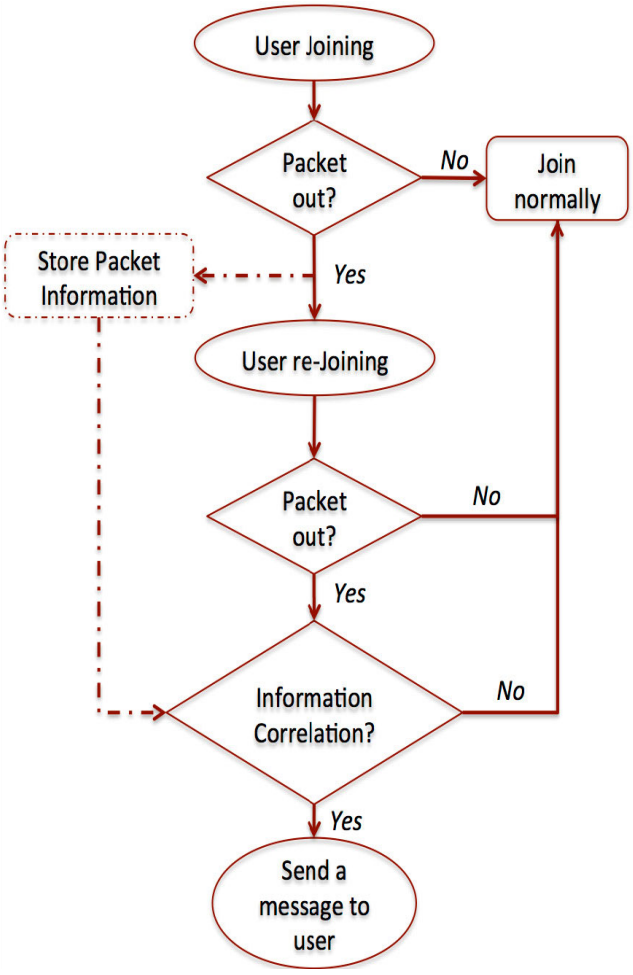

Figure 2. Tracking detection flow algorithm.

3.2 Multihops Algorithm (MhA)

To provide privacy to the sender this algorithm ensures that each packet sent is scheduled to travel in between the same femtocell users before going out to the Internet. These operations will be made totally in random; FAP is in charge of calculating next destination node by using a random function. In Figure 3 pseudocode approach for developing this algorithm is proposed, there is no need for any extra hardware to run this algorithm.

Tstamp value has to be generated in random by the sender attending to the bounds fixed by Tmax and Tmin. These parameters are defined as the maximum and minimum timestamp values, and they vary according to the packets supported on the network, and its performance. Possible values are given in Section 4 on this article. The FAP which has the responsibility for the synchronization of all users, and listing the available users connected

```
1|    #Define Tmax
2|    #Define Tmin
3|    Tstamp=rand(Tmin, Tmax);
4|    while(Tstamp!=0){
5|          list[]=Listing all users;
6|          i =rand(0,length(li st));
7|          Send packet to list [i];
8|          wait(Same packet Rx);
9|          Refresh Tstamp;
10|   }
11|   Send packet to Internet;
```

Figure 3. MhA pseudo-code.

to the femtocell. Further this non disclosed table will be stored in the FAP. Other users in the network only have to send back the packets to the FAP in order it can go on with the algorithm.

4. MhA Simulation

NetSimTMv.[7] is the software tool used to evaluate the performance of the proposed algorithm. All the configuration parameters described below can be modified with this software. For performance evaluation, the packet average number of reflections and average time spent in the femtocell are measured for different Tstamp values. At the end of this section discussion about the results is provided.

4.1 Simulation Settings

4.1.1 Network Parameters

Only one femtocell is considered for the simulation. Alcatel-Lucent 9361 home cell v2 is used as model for the FAP. The femtocell includes 15 users inside its radius coverage, which is 25 meters. During the simulation period all users remain inside the femtocell since when staying at home or office users will not move out for long time periods. GSM is proposed as the cellular standard protocol. No indoor path-loss model is proposed since in real time traffic a packet retransmission might not be feasible. A summary of the simulation parameters is presented in Table 1.

4.1.2 Packet Transmission

Channels are created by distributing all the available bandwidth in same-width slots. In order to reduce the delay on account of channels set-up a preallocating channel method is proposed. Therefore the FAP is in charge to previously assign each user a channel for sending the reflected packets.

4.1.3 Time Stamp Ranges

According to literature a phone call can handle a delay time up to 400ms. As presented by Rath[7] time spent for a packet to travel through internet is 200ms. Since the packet has to travel throughout the MCN some guard time should be kept. With these considerations two different time stamp ranges are proposed and simulated. First Tstamp is randomly selected between 10 and 30 milliseconds, then an extended range up to 60 milliseconds is used.

4.2 Simulation Results

Simulation results are presented in this section, in Table 2 and Table 3 direct results obtained from the simulations are presented. Probability density functions (p.d.f) are graphed in Figure 4 and Figure 5. Sim1 and Sim2 are used to refer Tstamp=(10,30) and Tstamp=(10,60) simulations respectively.

4.2.1 Average Number of Reflections

The mean number of reflections in Sim1 is 4 and in Sim2 7. This means that by doubling the Tstamp we can achieve a little bit less than the double of reflections. Furthermore in Figure 4 can be appreciate that in Sim2 the probability density function is flatter, which means that the number of reflections is more random than in Sim1.

In Figure 4 can be seen how for Sim1 the probability to have more than 5 reflections decreases really fast. While for Sim2 the probability decreases softly, providing higher values for more than 8 reflections. As expected, in terms of number of reflections, best choice will be the

Table 1. Simulation parameters summary

Network Parameters		**Demand Generation Parameters**	
Cellular Protocol	GSM	Voice packet size	300 bytes
Number of users	15	Voice packet generation	20 ms
Mobility Parameters		Voice data rate	13.3 kbps
Restricted inside femtocell coverage	25 m	Underlying data rate	270 kbps
User speed	0.5 m/s	Ongoing calls	4
		Tranmission Parameters	
		Listening bands	1900 MHz 850 MHz

Table 2. Number of reflections

Tstamp = (10,30)		Tstamp = (10,60)	
Records	8919	Records	6067
Mean Std	4.0189	Mean Std	7.6949
Std. Dev.	2.3289	Std. Dev.	5.2575
Minimum	1	Minimum	1
Maximum	13	Maximum	26
Median	4	Median	7

Table 3. Time inside the femtocell

Tstamp = (10,30)		Tstamp = (10,60)	
Records	8919	Records	6067
Mean Std	12.9382	Mean Std	22.8935
Std. Dev.	5.9170	Std. Dev.	13.7755
Minimum	0.5200	Minimum	0.5400
Maximum	28.1800	Maximum	57.2900
Median	12.3800	Median	20.3100

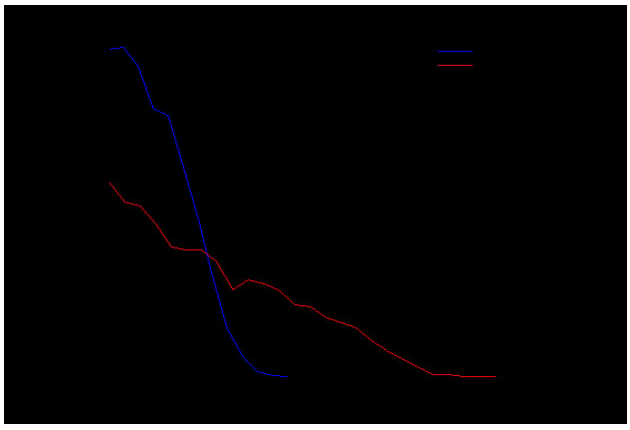

Figure 4. Number of Reflections p.d.f

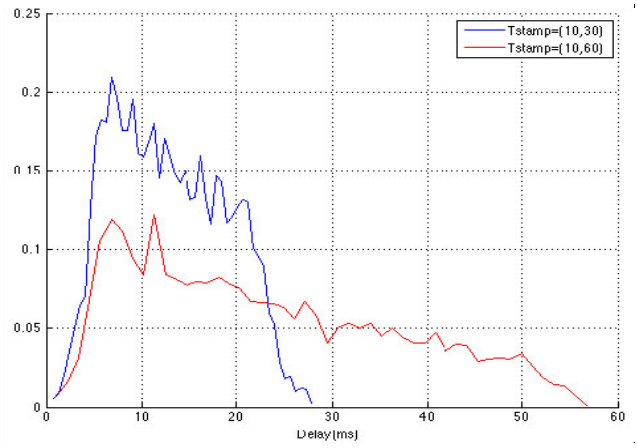

Figure 5. Introduced delay p.d.f

largest range for Tstamp values. Further work is need to find out which is the number of hops needed to ensure that an attacker can not point out the sender user.

4.2.2 Average Time Spent in the Femtocell

As discussed above in terms of number of reflections scenario of Sim2 is better. In this section we analyse the delay introduced since it is the main drawback of the proposed algorithm.

By observing the mean it is clear than by doubling the Tstamp range we are not doubling the time inside the femtocell. In Figure 5 can be seen graphically how the probability of getting low delays in Sim2 is not so distant to the obtained in Sim1. If we analyse the delay obtained in Sim2 it can be calculated than in 90% of the cases a delay under 43.7 ms is introduced. This delay could be afforded by the proposed network architecture.

With the obtained results it can be concluded that the largest Tstamp range is a better choice. Moreover the algorithm will become more robust if the delay is increased, but the relation of this increase is not lineal since the robustness rises faster.

5. Conclusions

In this article we have proposed a new attack scenario, where attackers are able to control more than one femtocell. We have analysed the different existing problems and proposed new attack which disclose user location. Alerting the user who is under treat has mitigated this attack. Algorithm for providing femtocells users anonymity is proposed as a new way for fighting this already discussed, security issue. The values for the variables in this algorithm have been proposed, simulated and discussed in a friendly environment.

Implementing both proposed solutions in a real network seems to be the next step in the path of securing femtocells. Also, as commented, further work is needed in tracking algorithm to make it learning-capable, which allows following attackers improvements.

6. References

1. 3GPP Technical Report 3rd Generation Partnership Project; Technical Specification Group Service and System Aspects; Security of H(e)NB; 3GPP TR 33.820 V8.2.0; 2009 Oct.

2. Tyrrell A, Zdarsky F, Mino E, Lopez M. Use cases, enablers and requirements for evolved femtocells. IEEE 73rd Vehicular Technology Conference (VTC Spring); 2011 May 15–18; Yokohama. p. 1–5.
3. Malone D, Kavanagh DF, Murphy NR, Femtocell R. How mallory can monitor my devices. 5th IEEE International Traffic Monitoring and Analysis Workshop; 2013 Apr 14–19; Turin. p. 429–34.
4. DePerry D, Ritter T, Rahimi A, iSEC Partners. Traffic interception and remote mobile phone cloning with a compromised CDMA femtocell. Black Hat Conference; 2013 Aug ; Las Vegas.
5. Terayama T, Ohyane H, Sato G, Takimoto T. Femtocell technologies for providing new services at home. NTT DOCOMO Technical Journal. 2011 Mar; 11(4).
6. Papageorgiou EI. Learning algorithms for fuzzy cognitive Maps—a review study. IEEE Trans Syst Man Cybern C Appl Rev. 2013; 42(2) :150–53.
7. Rath A, Panwar S. Fast handover in cellular networks with femtocells. IEEE International Conference on Communications (ICC); 2012 Jun 10–15; Ottawa. p. 2752–57.