Journal of Universal Computer Science, vol. 21, no. 3 (2015), 406-418
submitted: 30/6/14, accepted: 28/2/15, appeared: 1/3/15

On the Security of a User Equipment Registration Procedure in Femtocell-Enabled Networks

Chien-Ming Chen
(Harbin Institute of Technology Shenzhen Graduate School, Shenzhen, China
and
Shenzhen Key Laboratory of Internet Information Collaboration
Shenzhen, China
dr.chien-ming.chen@ieee.org)

Tsu-Yang Wu
(Harbin Institute of Technology Shenzhen Graduate School, Shenzhen, China
wutsuyang@gmail.com)

Raylin Tso
(National Chengchi University, Taipei, Taiwan, R.O.C.
raylin@cs.nccu.edu.tw)

Masahiro Mambo
(Kanazawa University, Kanazawa, Japan
mambo@ec.t.kanazawa-u.ac.jp)

Mu-En Wu
Corresponding Author
(Soochow University, Taipei, Taiwan, R.O.C.
mnasia1@gmail.com)

Abstract: Mobile data traffic has been growing at an increasing rate with the popularity of smartphones, tablets, and other wireless devices. To reduce the load on the network, mobile network operators deploy femtocells to increase their coverage and performance and to eliminate wireless notspots. Femtocells are low-cost devices that connect a new femtocell network architecture to the core telecommunication network through a licensed spectrum and standardized interface protocols.

In this paper, we first note that the user equipment registration procedure, which is defined in the 3GPP (Third Generation Partnership Project) standard, in a femtocell-enabled network is vulnerable to denial-of-service attacks. We then propose a mechanism to defend against these attacks. For compatibility, the proposed mechanism makes use of the well-defined control message in the 3GPP standard and modifies the user equipment registration procedure as little as possible.

Key Words: Femtocell, denial-of-service attack, 3GPP standard, security
Category: H.2, H.3.7, H.5.4

1 Introduction

To eliminate wireless notspots, femtocell technologies have been proposed for broadband wireless networks [Guruacharya et al. (2013), Pantisano et al. (2013), López-Pérez et al. (2014)]. A femtocell is a small, low-cost base station that serves to provide improved indoor coverage to mobile devices with sufficient user data rates and stable bandwidth. In general, femtocells are expected to be cheap and widely distributed. Femtocells also provide the following two advantages: first, the base stations (also called Macrocells) can shift network loading to the femtocells; and second, the femtocells can be easily developed and placed in houses or offices [Chen et al. (2014)].

Recently, 3GPP (Third Generation Partnership Project) collaborated with Femto Forum and Broadband Forum to create a new standard for femtocells. In 2009, the first femtocell standard [3GPP (2010)] was announced and published. The purpose of this standard was to standardize femtocells to be produced in large volumes.

Although femtocell technologies have attracted widespread industry attention, they still have security issues. Normally, the security for a femtocell network contains two major parts, femtocell device authentication and encryption of control information across the untrusted Internet. To solve these problems, 3GPP UMTS Release 9 [3GPP (2010)] has been announced. All security specifications are complete.

However, we have observed that the user equipment (UE) registration procedure, which is defined in the 3GPP standard [3GPP (2010)], in a closed access mode is vulnerable to denial-of-service (DoS) attacks because the femtocells cannot release resources until they receive the verification results from the core network (CN). As a result, a mechanism to overcome this issue is necessary.

In this paper, we first demonstrate that the UE registration procedure is vulnerable to DoS attacks. We also propose a mechanism to defend against these DoS attacks. For compatibility, the proposed mechanism make uses of the well-defined control messages in the 3GPP standard and modifies the UE registration procedure as little as possible. A performance evaluation and security analysis demonstrate that the proposed mechanism is efficient and can effectively resist to DoS attack.

The remaining sections are organized as follows. [Section 2] introduces the relevant literature. In [Section 3], we briefly review the UE registration procedure proposed in 3GPP standard. In [Section 4], we show that this UE registration procedure is vulnerable to a DoS attack. We further propose an auto-reject mechanism in [Section 5]. The performance and security analysis are investigated in [Section 6], and finally, we give our conclusions in [Section 7].

2 Related Work

With the rapid growth of network technologies, security issues have been a matter of concern in various network environments such as cloud computing, wireless sensor networks, social networks, and the Internet of Things [Farash and Attari (2014), Mellado and Rosado (2012), Ajmal et al. (2014), Kong et al. (2013), Zhuang et al. (2013), Farash et al. (2015)]. In this section, we first introduce several related studies of femtocell-enabled networks. We also describe the closed subscriber group (CSG).

2.1 Security Issues of Femtocell-Enabled Networks

Bilogrevic *et al.* [Bilogrevic et al. (2010)] describe to need to consider the following three security vulnerabilities in femtocell-enabled networks: the air interface between mobile devices and the femtocells, the link between the femtocells and security gateways (SeGWs), and the femtocell itself. Segura *et al.* [Segura and Lahuerta (2010)] demonstrate the economic incentives of resisting DDoS attacks. Rajavelsamy *et al.* [Rajavelsamy et al. (2011)] analyze some possible security risks that can occur after the deployment of femtocells. Borgaonkar *et al.* [Borgaonkar et al. (2011)] demonstrate that attackers have the ability to gain root access and install malicious applications on femtocells. Golde *et al.* [Golde et al. (2012)] describe that femtocells involve the following aspects of security: the integrity of the device, the access control mechanisms, and the protection of the software update process. In 2013, a comprehensive analysis of the femtocell was proposed [Fabian and Schreur (2013)]. Chen *et al.* [Chen et al. (2014)] define two attacks, sinkhole and wormhole attacks, in femtocell-enabled networks. They also propose an approach based on a distance bounding protocol to defend against the above two types of attacks.

2.2 Closed Subscriber Group

A Closed Subscriber Group (CSG) is introduced in the 3G/WiMAX standards [3GPP (2008); Kim et al. (2009)]. It defines an identity, called Closed Subscriber Group Identity (CSG_id) that femtocells can use to authorize legitimate subscribers [Golaup et al. (2009)].

Fig. 1 depicts the access control strategy for subscribers based on CSG identities. Each subscriber can belong to one or more CSG_id; for example, Bob has two CSG_ids (1 and 2). In contrast to subscribers, each femtocell belongs to one or fewer CSG_id [3GPP (2009)]. Femtocells could restrict accesses for subscribers. They support three access modes: an open access mode, a hybrid mode, and a closed access mode [Golaup et al. (2009)].

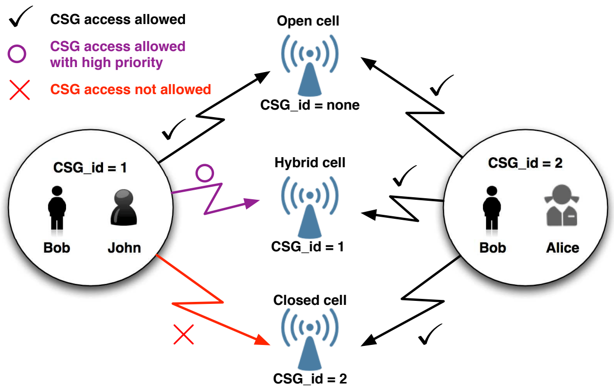

Figure 1: Access control strategy for subscribers based on CSG identity.

Open Mode The open mode allows any mobile device to access the femtocell without permission. For instance, John and Alice, whose mobile devices are carried with different CSG_ids are allowed to access the femtocell. Customarily, the open mode is designated for a public environment.

Hybrid Mode As with the open mode, all mobile devices with matched and unmatched CSG_id can access a femtocell in the hybrid mode; however the hybrid mode assigns a higher priority to devices that pass CSG_id verification.

Closed Mode In the closed mode, the femtocell allows only devices that hold the same identity as the connected femtocell to access the CN, and reject all others. For a closed mode femtocell, users should register their devices on a list (whitelist).

3 Review of the UE Registration Procedure

The 3GPP standard [3GPP (2010)] defines several kinds of UE registration procedures based on the access control mode of the femtocell. In our observation, only the UE registration of femtocells in the closed mode is vulnerable to DoS attacks.

Fig. 2 shows each step of the registration procedure when a UE attempts to access a closed mode femtocell. Note that the communication between the femtocell and the SeGW goes through an IPsec tunnel.

Step 1 to 4 From steps 1 to 3, an RRC (Radio Resource Control) connection is established between the UE and the femtocell. The UE then transmits an RRC Initial Direct Transfer message carrying a Location Updating Request message with its identity (e.g., IMSI(International Mobile Subscriber Identity) or TMSI(Temporary Mobile Subscriber Identity)) at step 4.

Step 5 to 9 In step 5, the femtocell checks the UE's capabilities. If the identity of this UE is unknown to the femtocell being accessed, the femtocell initiates UE registration toward the Femto-GW (steps 6-8).

In step 6, the femtocell sends the UE register request to Femto-GW for registration of the UE on the Femto-GW. After the Femto-GW checks the UE's capabilities(step 7), it responds with a UE Register Accept message back to the femtocell in step 8. The femtocell then transmits an RUA (RANAP User Adaption) Connect message containing the femtocell's access mode to the Femto-GW at step 9.

Step 10 to 17 The RUA Connect message triggers the setup of an SCCP (Signalling Connection Control Part) connection by the Femto-GW toward the CN at step 10. The CN then responds with an SCCP Connection Confirm message at step 11. Step 12 is an optional mobility management procedures, and the CN may perform an Authentication procedure. To this point, the access control of the UE is not performed. In other words, the femtocell has no information to determine whether it is legal for the UE to access the femtocell. Therefore, the femtocell cannot release its resource to the other UEs that also attempt to access the femtocell. At step 13, the CN performs access control to compare the UE's CSG_id with the femtocell's CSG_id. The CN then notifies the femtocell to accept or reject the UE's attempt (step 14). Steps 15-17 complete the rest of work.

4 DoS Attack on the UE Registration Procedure

In this section, we define the adversary model and demonstrate that the UE registration procedure described above is vulnerable to DoS attacks.

4.1 Problem Definition

As mentioned above, the access control verification of the UE registration procedure is executed in the CN. Connection to a wired network is an essential characteristic of a femtocell network. The transmitted data should pass through an insecure network, e.g., the Internet, and enter the CN. Hence, the transmission delay in femtocell networks is greater than in a 3G/WiMax network. It also means that a malicious subscriber can send a series of connect requests to the femtocell to launch a DoS attack. To solve this problem, we attempt to accelerate the access control verification.

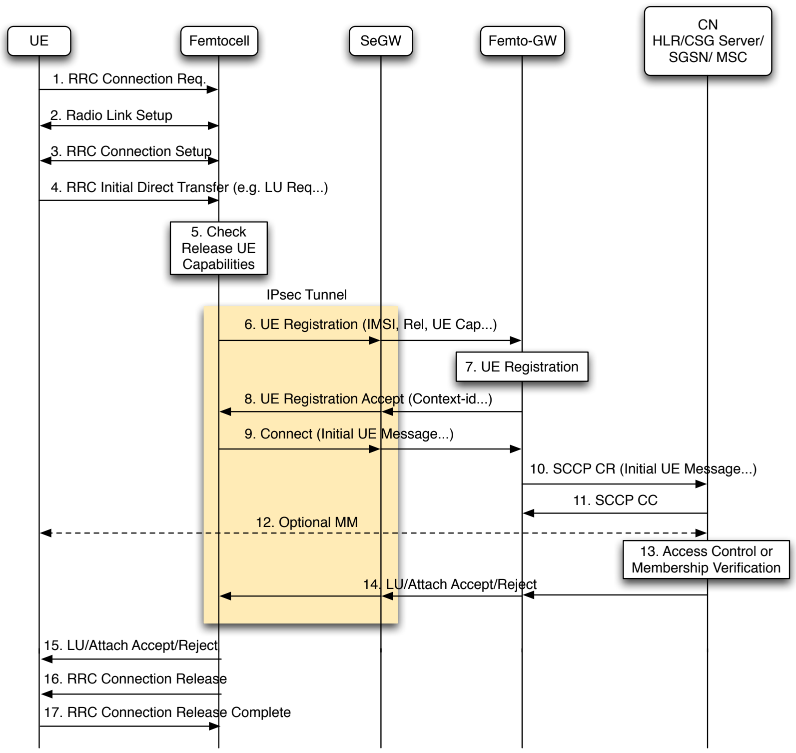

Figure 2: Procedure of UE registration

4.2 Adversary Model

Here we define an adversary model that depends on the capability of the UE. In general, the UE will hand over seamlessly from the base station (BS) to the femtocell once the femtocell signals are detected. In addition to automatic handover, the 3GPP standard provides a manual CSG selection property for the UE [3GPP (2009)]. The adversary can request the UE to perform a scan for available CSGs. The UE will display the available CSG identities and their femtocell names. Hence, the adversary can manually select a femtocell with which she prefers to connect. The abilities of adversary are as follows:

1. An adversary can arbitrarily connect to a femtocell.

2. An adversary can send a series of connect requests to a femtocell.

According to the adversary model, a DoS attack [Chang et al. (2010)] is defined as follows.

Table 1: The Notations

Notation	Description
CN	Core network
M_i	Subscriber i's device
ID_i	Subscriber i's device identity, e.g., IMSI
f_i	Femtocell i
L_i	Femtocell i's blacklist

4.3 Denial-of-Service Attack

The purpose of a DoS attack is to block legitimate users' system access by reducing system availability. Currently, a residential femtocell can support two to four mobile devices. This design demonstrates that femtocells can easily suffer from DoS attacks. If an adversary sends more than four connect requests to a femtocell simultaneously, the femtocell will be over-loaded. This attack works even if the target is a closed-mode femtocell because the femtocell cannot reject illegal users immediately. Based on the UE registration procedure, the femtocell must wait until it receives a response from the CN. The adversary can aim at a femtocell and begin sending a series of requests to it and the femtocell will have no extra resources to serve legitimate users.

As mentioned above, the UE registration is vulnerable to DoS attacks on femtocells. The messages transmitted between the femtocell and the SeGW may go through the Internet via the IPsec tunnel. Hence, the transmission time for messages in a femtocell network is much longer than in a normal 3G network; this will make DoS attacks more serious.

5 Auto-Reject Mechanism

In this section, we design an auto-reject mechanism to prevent these attacks. The notations used in this section are listed in Table 1.

Our auto-reject mechanism is designed for femtocells and consists of creation, blocking, and recovery phases. Each femtocell handles a blacklist to record which clients are malicious. When a client attempts to connect with a femtocell and is rejected by access control verification (see step 13 of Fig. 2), the femtocell records the client's identity, IMSI, which is contained in the reject message sent from the CN. The blocked client will be immediately rejected by the femtocell before its blocking time is expired.

Fig. 3 shows the details of auto-reject. In the beginning, f_i checks M_i to see whether ID_i exists in the blacklist L_i in the creation phase. If true, f_i checks whether M_i's block time has expired in the blocking phase. If so, f_i immediately rejects further requests from M_i to reduce the delay time of access

Creation		
1.	$M_i \to f_i$	: connect request
2.	f_i	: If $ID_i \in L_i$, go to blocking phase; otherwise, execute UE registration procedure.
3.	$CN \to f_i$	: Attach Reject message,
4.	f_i	: Retrieve ID_i from the message, and add ID_i into L_i.
5.	$f_i \to M_i$	: Attach Reject message.
Blocking		
1.	f_i	: Check the expiration of blocking time. If expired, go to recovery phase; otherwise, reset the expired time of blocking.
2.	$f_i \to M_i$	: Attach Reject message.
Recovery		
1.	f_i	: Remove ID_i from L_i, and go to step 2 of creation phase.

Figure 3: Auto-reject mechanism

control verification. To avoid false-positive or other unexpected errors, the auto-reject mechanism has a recovery mechanism to remove ID_i from L_i. After a period of time, M_i can again attempt to connect to f_i regularly.

With our auto-reject mechanism, the original procedure (see Fig. 2) is adjusted to another procedure (see Fig. 4).

6 Performance Evaluation and Security Analysis

In this section, we evaluate the performance of our mechanism by experimentation. We also provide a security analysis to show that our design can effectively resist DoS attacks.

6.1 Performance Evaluation

Experiment Setting We deploy a PicoChip femtocell device [picoChip Designs Ltd. (2010)] under the WiMAX network platform (Fig. 6.1). A SeGW is implemented on an Intel IXP465 network processor [Intel Corporation (2006)] and a backend CN is simulated on an emulator. An IPsec tunnel is also implemented between the SeGW and the femtocell. All network services are also performed by the emulator. The subscriber's device is a laptop equipped with WiMAX capabilities.

Estimated Results In the laboratory experiment, we measure the overhead of the transmission time between the components in the femtocell network. In

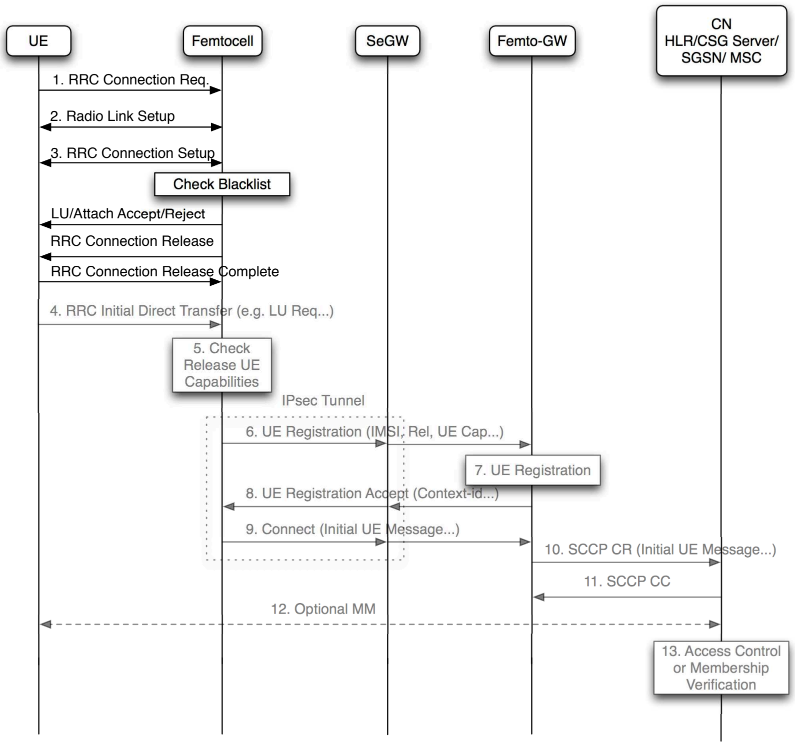

Figure 4: The benefit of auto-reject mechanism. Gray text signifies omitted steps.

Fig. 2, the section between the UE and the femtocell is referred to as A, and its overhead is approximately 10 ms. The section between the femtocell and the Femto-GW is referred to as B, and its overhead is approximately 110 ms. The section between the Femto-GW and the CN is referred to as C, and its overhead is approximately 30 ms. We use the notation N to represent the number of malicious connection requests. Therefore, the equation to estimate the overhead of the UE registration procedure with the traditional femtocell is derived as follows (optional step 12 is omitted):

$$(7A + 4B + 3C) * N \ (ms) \tag{1}$$

The femtocell should perform the full procedure to reject every request. According to Fig. 4, the equation becomes as follows:

$$(7A + 4B + 3C) + (N - 1) * (6A) \ (ms) \tag{2}$$

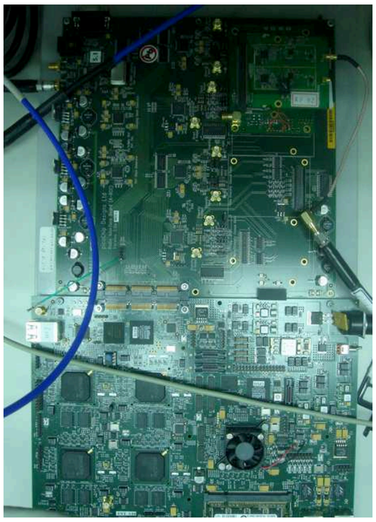

Figure 5: femtocell devices

To create the blacklist, the femtocell needs to perform the full procedure once. The rest of the requests only take $6A\ ms$ each. For example, if an attacker sends 10 requests to the femtocell, the total overhead of the auto-reject femtocell is 1140 ms; the total overhead of the traditional femtocell is 6000 ms. Fig. 6 illustrates that the total overhead of the auto-reject femtocell is much less than the total overhead of the traditional femtocell. Therefore, our proposed approach can prevent a femtocell from a DoS attack.

6.2 Security Analysis

Here we analyze the security of our auto-reject mechanism.

Secure against Dos attacks As mentioned above, the traditional UE registration is easily victimized by a DoS attack because the access control verification is executed by the CN. In the first step of our mechanism, the femtocell will check the connection request from the subscriber by checking the blacklist. If a malicious subscriber wants to send a series of requests to the femtocell, it will be rejected immediately. It is easy to see that our mechanism can efficiently reduce the effects of DoS attacks.

Message unforgeability Because the secure communication between the femtocell and CN is relied on IPSec, any malicious subscribers cannot attach forged reject messages to cheat the femtocell.

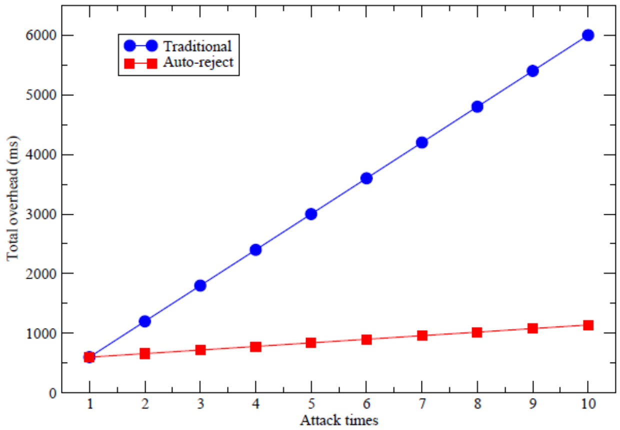

Figure 6: The estimated results of the auto-reject femtocell and the traditional femtocell.

7 Conclusion

In this paper, we demonstrate that the UE registration procedure defined in the 3GPP standard is vulnerable to DoS attack. These attacks can block legitimate users' system access, thus reducing the system availability. To eliminate this security problem, we propose an auto-reject mechanism that makes use of the well-defined control message in the 3GPP standard. Finally, a performance evaluation and security analysis showed that our design is efficient and can effectively resist DoS attacks.

In this paper, the performance evaluation is based on the transmission time between two devices. In future work, we attempt to carry out real implementation on a femtocell base station. We also plan to implement our mechanism on 3G femtocells environments. Consequently, we can perform a detailed theoretical performance analysis based on well-accepted traffic models.

Acknowledgment

The authors would like to thank anonymous reviewers for their valuable comments and suggestions, which certainly led to improvements of this paper. The work of Chien-Ming Chen was supported in part by the Project NSFC (National Natural Science Foundation of China) under Grant number 61402135 and in part by Shenzhen Strategic Emerging Industries Program under Grants No. ZDSY20120613125016389. The work of Raylin Tso was supported in part by the Ministry of Science and Technology, Taiwan, R.O.C., under Grant MOST 103-2221-E-004-009. The work of Mu-En Wu was supported in part by the Ministry of Science and Technology, Taiwan, R.O.C., under Grant MOST 103-2218-E-031-001. The corresponding author of this paper is Prof. Mu-En Wu.

References

3GPP: "TR-25.820-v8.2.0: 3G Home NodeB Study Item Technical Report (Release 8)"; (2008).

3GPP: "TS-22.220-v9.3.0: Service requirements for Home NodeBs and Home eNodeBs (Release 9)"; (2009).

3GPP: "TS-25.467-v9.3.0: UTRAN artitechture for 3G Home Node B (HNB) Stage 2 (Release 9)"; (2010).

Ajmal, S., Rasheed, A., Qayyum, A., Hasan, A.: "Classification of vanet mac, routing and approaches a detailed survey"; Journal of Universal Computer Science; 20 (2014), 4, 462–487.

Bilogrevic, I., Jadliwala, M., Hubaux, J.: "Security issues in next generation mobile networks: Lte and femtocells"; 2nd International Femtocell Workshop; 2010.

Borgaonkar, R., Redon, K., Seifert, J.: "Security analysis of a femtocell device"; Proceedings of the 4th International Conference on Security of Information and Networks; 95–102; 2011.

Chang, C.-C., Wu, C.-C., Lin, L.-C.: "3gpp sim-based authentication schemes for wireless local area networks"; International Journal of Innovative Computing Information and Control; 6 (2010), 2, 461–474.

Chen, C.-M., Chen, Y.-H., Lin, Y.-H., Sun, H.-M.: "Eliminating rouge femtocells based on distance bounding protocol and geographic information"; Expert Systems with Applications; 41 (2014), 2, 426–433.

Fabian, v. d. B., Schreur, R. W.: "Femtocell security in theory and practice"; Secure IT Systems; 183–198; Springer, 2013.

Farash, M. S., Attari, M. A.: "A provably secure and efficient authentication scheme for access control in mobile pay-tv systems"; Multimedia Tools and Applications; (2014), 1–20.

Farash, M. S., Kumari, S., Bakhtiari, M.: "Cryptanalysis and improvement of a robust smart card secured authentication scheme on sip using elliptic curve cryptography"; Multimedia Tools and Applications; (2015), 1–20.

Golaup, A., Mustapha, M., Patanapongpibul, L.: "Femtocell access control strategy in UMTS and LTE"; IEEE Communications Magazine; 47 (2009), 9, 117–123.

Golde, N., Redon, K., Borgaonkar, R.: "Weaponizing femtocells: The effect of rogue devices on mobile telecommunications"; Proceedings of the Symposium on Annual Network & Distributed System Security; 2012.

Guruacharya, S., Niyato, D., Kim, D. I., Hossain, E.: "Hierarchical competition for downlink power allocation in ofdma femtocell networks"; IEEE Transactions on Wireless Communications; 12 (2013), 4, 1543–1553.

Intel Corporation: "Intel IXP465 Network Processor"; http://www.intel.com/design/network/products/npfamily/ixp465.htm (2006).

Kim, R., Kwak, J., Etemad, K.: "WiMAX femtocell: requirements, challenges, and solutions"; IEEE Communications Magazine; 47 (2009), 9, 84–91.

Kong, Q., Li, P., Ma, Y.: "On the feasibility and security of image secret sharing scheme to identify cheaters"; Journal of Information Hiding and Multimedia Signal Processing; 4 (2013), 4, 2073–4212.

López-Pérez, D., Chu, X., Vasilakos, A. V., Claussen, H.: "Power minimization based resource allocation for interference mitigation in ofdma femtocell networks"; IEEE Journal on Selected Areas in Communications; 32 (2014), 2, 333–344.

Mellado, D., Rosado, D. G.: "An overview of current information systems security challenges and innovations j. ucs special issue"; Journal of Universal Computer Science; 18 (2012), 12, 1598–1607.

Pantisano, F., Bennis, M., Saad, W., Debbah, M., Latva-aho, M.: "Interference alignment for cooperative femtocell networks: A game-theoretic approach"; IEEE Transactions on Mobile Computing; 12 (2013), 11, 2233–2246.

picoChip Designs Ltd.: "PC203 Femtocell Multi-core DSP"; http://www.picochip.com/page/70/Multi-core-PC203 (2010).

Rajavelsamy, R., Lee, J., Choi, S.: "Towards security architecture for home (evolved) nodeb: challenges, requirements and solutions"; Security and Communication Networks; 4 (2011), 4, 471–481.

Segura, V., Lahuerta, J.: "Modeling the economic incentives of ddos attacks: Femtocell case study"; Economics of Information Security and Privacy; 107–119; Springer, 2010.

Zhuang, X., Wang, Z.-H., Chang, C.-C., Zhu, Y.: "Security analysis of a new ultra-lightweight rfid protocol and its improvement"; Journal of Information Hiding and Multimedia Signal Processing; 4 (2013), 3, 166–177.