Int. J. Communications, Network and System Sciences, 2015, 8, 70-78
Published Online April 2015 in SciRes. http://www.scirp.org/journal/ijcns
http://dx.doi.org/10.4236/ijcns.2015.84009

Local Gateway Assisted Handover Key Derivation in Enterprise Femtocell Network

Peng Wang[1], Xiaojuan Zhang[2]

[1]Bell Labs, Shanghai, China
[2]School of Computer Science, Qinghai Normal University, Xining, China
Email: wp3891@seu.edu.cn, zhxj@qhnu.edu.cn

Received March 2015

Abstract

With the dense deployment of femtocells in enterprise femtocell network and the small coverage of femtocells, handover in enterprise femtocell network will be frequent. The general handover key derivation method which is used in handover procedures in LTE is not suitable for handover in this scenario because of its long time cost and the weak security. To solve this problem, this paper has proposed a new local gateway assisted handover key derivation schema in enterprise femtocell network. It can meet the fast derivation and good forward/backward key secrecy requirement of handover key derivation in enterprise femtocell network. The simulation result has verified that the proposed handover key derivation schema works better than the existing method.

Keywords

Femtocell Network, Key Derivation, Mobility Management, Handover, Local Gateway

1. Introduction

Enterprise Femtocell Network (EFN) is a novel and very promising application concept of femtocells [1]-[4]. It is defined as a group of femtocells that are able to form a partially autonomous network under the administration of a Local Network Operator (LNO). EFN is conceived as a complementary solution to existing macrocell deployments in order to improve network coverage and capacity, offload traffic from the Evolved Packet Core (EPC), and provide new services to mobile subscribers. EFN can be deployed for many scenarios, such as shopping malls, corporate environments, convention centers, or university campuses.

The handover key derivation method used in EFN is the same with the general one used in handover procedures in LTE [5]-[7]. There is no specific handover key derivation methods for Enterprise Femtocell Network (EFN). In recent years, a lot of researches on handover authentication for eNBs have been proposed [8]-[13]. But this general handover key derivation methods in LTE is not suitable for EFN. There are two different key derivation ways for X2-based handover and S1-based handover in LTE. In X2-based handover situation, the new key for target HeNB K^*_{eNB} is generated from the old communication key K_{eNB} between UE and source HeNBs. The source HeNB may derive K^*_{eNB} by K_{eNB}. So K^*_{eNB} is not forward secure. In S1-based handover situation, the key K^*_{eNB} is derived from the K_{ASME} by MME. This provides good key backward/forward secrecy.

How to cite this paper: Wang, P. and Zhang, X.J. (2015) Local Gateway Assisted Handover Key Derivation in Enterprise Femtocell Network. *Int. J. Communications, Network and System Sciences*, **8**, 70-78.
http://dx.doi.org/10.4236/ijcns.2015.84009

But because MME is far away from HeNB of EFN, this method will take a lot of time. With the dense deployment of HeNB in EFN and the small coverage of HeNB, handover in EFN will be frequent. S1-based key derivation method will not be efficient enough for EFN.

This paper is to solve the handover key derivation problem in EFN. To meet the fast derivation and good forward/backward key secrecy requirement of handover key derivation in EFN, a local key derivation device, named Local Key Distributor (LKD), is added into Enterprise Femtocell Gateway (EFGW). When UE hands its connection over to EFN, the MME (Mobility Management Entity) issues delegation power to the LKD. Then LKD uses a key K_{LKD}, which is derived from K_{ASME} by MME, to generate new keys for target HeNBs in handover process in EFN. This helps to reduce the time of key derivation greatly. Meanwhile, it provides good key forward/backward secrecy, because the source HeNB can't derive the new key for target eNB without knowing the key K_{LKD}.

The rest of this paper is organized as follows: In Section 2, we will introduce how to deploy a local key distributor into EFN. In Section 3, we will detail the local gateway assisted handover key derivation schema in EFN. And the performance analysis will be presented in Section 4.

2. The Deployment of Local Key Distributor into EFN

In order to provide EPC functionalities within the EFN and to keep data and signalling traffic within the local network, there was a new element introduced in the network architecture: Enterprise Femtocell Gateway (EFGW). In the literatures [1]-[4]. From the logical point of view, the EFGW is located in the edge of the EFN and acts as a network manager for local mobility, traffic management, access control, authentication, power management, and fault management. And it can also provide Local IP Access (LIPA) or Selected IP Traffic Offload (SIPTO) services, which are particularly relevant in femtocell networks [5].

Local Key Distributor (LKD) can be deployed separately or integrated into EFGW. **Figure 1** presents the evolved system architecture with the deployment of the LKD integrated into EFGW. LKD will use the standard S1 interface to communicate with entities in EPC (Evolved Packet Core). The LKD behaves towards the EPC (Evolved Packet Core) like a standard eNB. And LKD communicates with HeNB in EFN with enhanced S1 interface. The details of the enhancement will be explained later in this proposal.

3. The Proposed Local Gateway Assisted Handover Key Derivation Schema

Handover key derivation problem in EFN has three sub problems, including how to generate new keys during hand-in process (handover process from an eNB/HeNB out of EFN to a HeNB in EFN), how to generate new keys during inter-HeNB handover process in EFN, and how to generate new keys during hand-out process (handover process from a HeNB in EFN to an eNB/HeNB out of EFN. The key derivation procedures in these three scenarios are as follows:

3.1. Key Derivation Procedure in Hand-In Process

Except generating new key for target HeNB, the other propose of this procedure is to derive a delegation key for LKD, which LKD will use to generate new keys for target HeNBs in place of MME in later intra-HeNB handover in EFN. The key derivation process is shown as **Figure 2**.

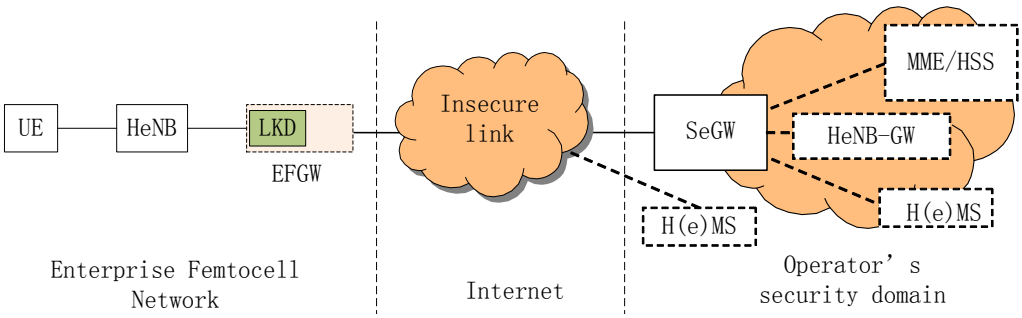

Figure 1. Evolved system architecture of enterprise Femtocell network with addition of LKD.

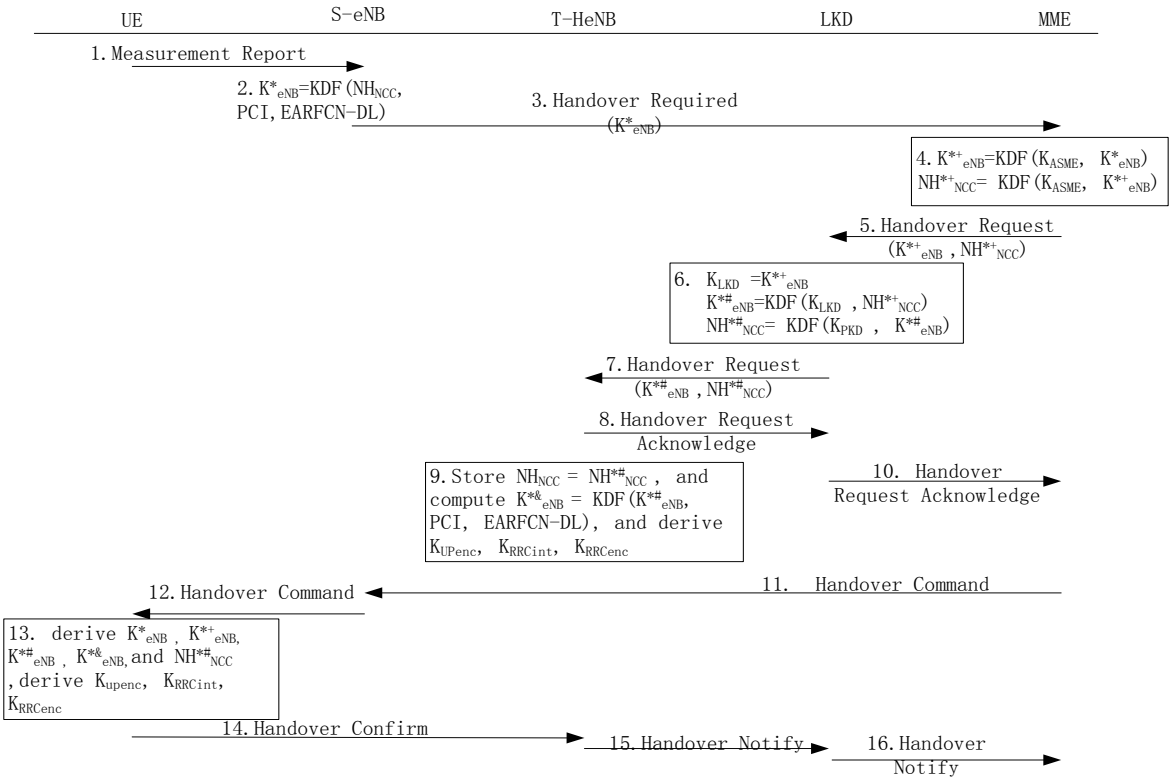

Figure 2. Key Derivation during Hand-in process.

The message sequence of key derivation during hand-in procedure into EFN is as follows:

1. UE sends Measurement Report message to the source eNB (S-eNB) in macrocell network.
2. S-eNB computes K^{*}_{eNB} with Key Derivation Function (KDF).
3. S-eNB sends Handover Required to MME
   K^{*}_{eNB} will be included in the Handover Required message.
4. MME computes K^{*+}_{eNB} and NH^{*+}_{NCC}
5. MME sends Handover Request message to LKD
   K^{*+}_{eNB} and NH^{*+}_{NCC} are included in the Handover Request message. K^{*+}_{eNB} will be sent to LKD, and used as the key K_{LKD}.
6. When LKD receives K^{*+}_{eNB} and NH^{*+}_{NCC} from MME, it sets $K_{LKD} = K^{*+}_{eNB}$, and then computes $K^{*\#}_{eNB}$ and $NH^{*\#}_{NCC}$ by $K^{*\#}_{eNB} = KDF(K_{LKD}, NH^{*+}_{NCC})$ and $NH^{*\#}_{NCC} = KDF(K_{LKD}, K^{*\#}_{eNB})$.
7. LKD sends Handover Request message to T-HeNB
8. If T-HeNB can accept this handover, it sends Handover Request Acknowledge message to LKD
9. T-HeNB stores $NH^{*\#}_{NCC}$ and computes $K^{*\&}_{eNB} = KDF(K^{*\#}_{eNB}, PCI, EARFCN\text{-}DL)$, and derive K_{UPenc}, K_{RRCint}, K_{RRCenc}
10. LKD sends Handover Request Acknowledge message to MME
11. MME sends Handover Command message to S-eNB
12. S-eNB sends Handover Command message to UE
13. UE derives new keys for communication with T-HeNB, and then derive K_{upenc}, K_{RRCint}, K_{RRCenc}
14. UE sends Handover Confirm message to T-HeNB.
15. T-HeNB sends Handover Notify message to LKD.
16. LKD relays the Handover Notify message to MME.

3.2. Key Derivation Procedure of Inter-HeNB Handover in the EFN

In the inter-HeNB handover process in EFN, the new keys for target HeNB are generated by LKD in this paper. The handover key derivation functionality of MME under the control of the EPC is transferred to LKD in the

EFN. This helps to reduce the time for generating new keys for target HeNB. The inter-HeNB handover key derivation process in EFN is shown as **Figure 3**.

The concrete procedures are as follow:

1. UE sends Measurement Report message to the source HeNB (S-HeNB) in macrocell network.
2. S-HeNB computes K^{*}_{eNB} with Key Derivation Function (KDF).

K^{*}_{eNB} = KDF (NH_{NCC}, PCI, EARFCN-DL), K^{*}_{eNB} is a material for generating new key of target HeNB, KDF must be a one-way function (e.g. a hash function like SHA256).

3. S-eNB sends Handover Required message to LKD

K^{*}_{eNB} is included in the Handover Required message.

4. LKD computes $K^{*\#}_{eNB}$ and $NH^{*\#}_{NCC}$ by $K^{*\#}_{eNB}$ = KDF (K_{LKD}, K^{*}_{eNB}) and $NH^{*\#}_{NCC}$ = KDF (K_{LKD}, $K^{*\#}_{eNB}$).

In this step, LKD acts as a proxy MME using K_{LKD} to generate new key $K^{*\#}_{eNB}$ for target HeNBs. And $NH^{*\#}_{NCC}$ is a parameter used for next handover.

5. LKD sends Handover Request message to T-HeNB

$K^{*\#}_{eNB}$ and $NH^{*\#}_{NCC}$ are included in the Handover Request message.

6. If T-HeNB can accept this handover, it sends Handover Request Acknowledge message to LKD
7. T-HeNB stores $NH^{*\#}_{NCC}$ and computes $K^{*\&}_{eNB}$ = KDF ($K^{*\#}_{eNB}$, PCI, EARFCN-DL), and derive K_{UPenc}, K_{RRCint}, K_{RRCenc}

$NH^{*\#}_{NCC}$ will be used in next handover key derivation. K_{UPenc}, K_{RRCint}, K_{RRCenc} are generated from $K^{*\&}_{eNB}$, and the algorithms are presented in 3GPP TS 33.401.

8. LKD sends Handover Command message to S-HeNB
9. S-eNB sends Handover Command message to UE
10. UE derives new keys for communication with T-HeNB, and then derives K_{UPenc}, K_{RRCint}, K_{RRCenc}

UE generates new keys by K^{*}_{eNB} = KDF (NH_{NCC}, PCI, EARFCN-DL), $K^{*\#}_{eNB}$ = KDF (K_{LKD}, K^{*}_{eNB}), $NH^{*\#}_{NCC}$

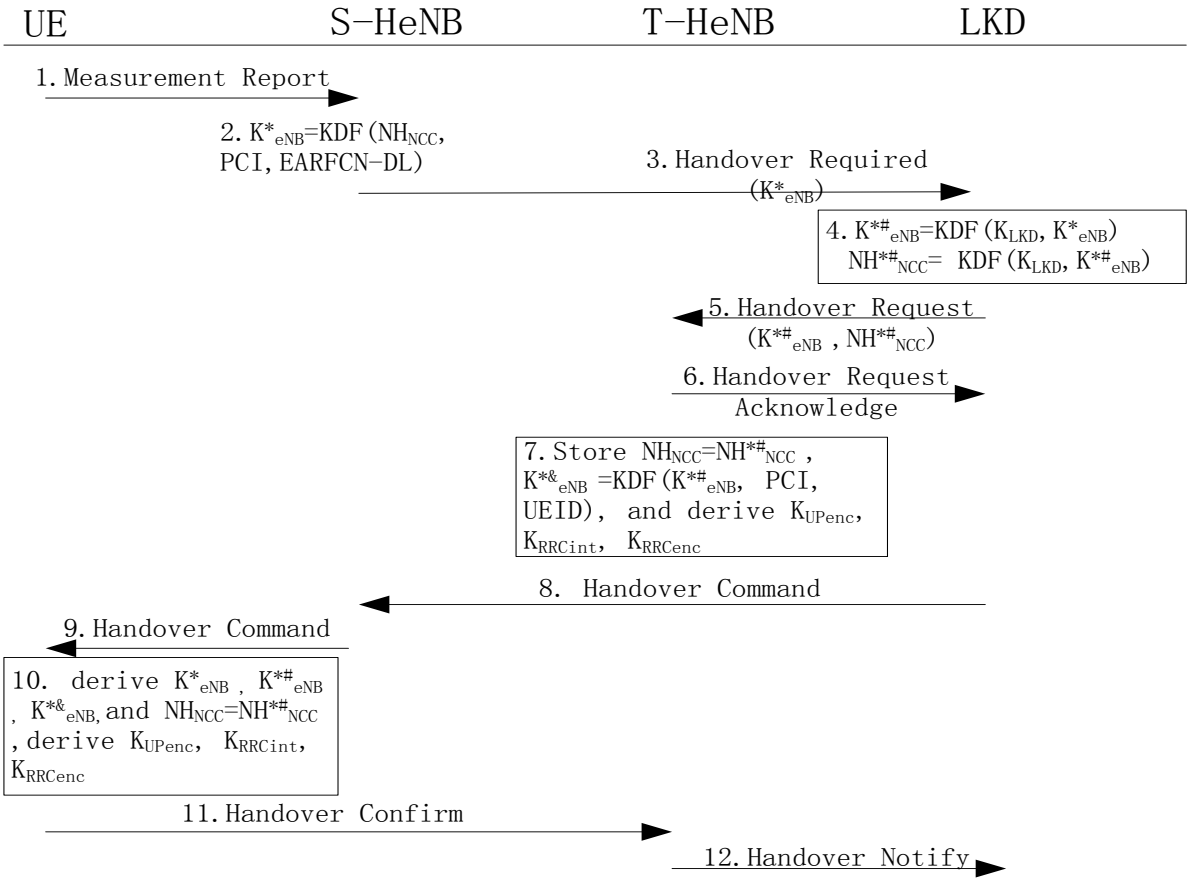

Figure 3. Key Derivation during Inter-HeNB Handover in EFN.

= KDF (K_{LKD}, $K^{*\#}_{eNB}$), $K^{*\&}_{eNB}$ = KDF($K^{*\#}_{eNB}$,PCI,EARFCN-DL), and derive K_{UPenc}, K_{RRCint}, K_{RRCenc} from $K^{*\&}_{eNB}$, and the algorithms are presented in 3GPP TS 33.401.

11. UE sends Handover Confirm message to T-HeNB
12. T-HeNB sends Handover Notify message to LKD

3.3. Key Derivation Procedure of Hand-Out Process

The key derivation procedure of hand-out process is almost the same with that in handover between eNBs in LTE, as shown in **Figure 4**. The LKD just acts as a relayer to transmit messages between source HeNB (S-HeNB) and MME when LKD finds the target eNB (T-eNB) is not in EFN. The concrete procedures are as follows:

1. UE sends Measurement Report message to the source HeNB (S-HeNB) in macrocell network.
2. S-HeNB computes K^{*}_{eNB} with Key Derivation Function (KDF).
   K^{*}_{eNB} = KDF (NH_{NCC}, PCI, EARFCN-DL), K^{*}_{eNB} is a material for generating new key of target HeNB, KDF must be a one-way function (e.g. a hash function like SHA256).
3. S-HeNB sends Handover Required message to LKD
   K^{*}_{eNB} will be included in the Handover Required message.
4. LKD relays this Handover Required message to MME
5. MME computes K^{*+}_{eNB} and NH^{*+}_{NCC}
   K^{*+}_{eNB} = KDF (K_{ASME}, K^{*}_{eNB}), NH^{*+}_{NCC}= KDF (K_{ASME}, K^{*+}_{eNB}). K^{*+}_{eNB} and NH^{*+}_{NCC} will be transferred to target eNB directly, and NH^{*+}_{NCC} will be used for generating K^{*}_{eNB} in next handover.
6. MME sends Handover Request message to T-eNB
   K^{*+}_{eNB} and NH^{*+}_{NCC} are included in the Handover Request message.
7. If T-eNB can accept this handover, it sends Handover Request Acknowledge message to MME
8. T-eNB stores $NH^{*\#}$NCC, $K^{*\#}_{eNB}$ = K^{*+}_{eNB}, and computes $K^{*\&}_{eNB}$ = KDF($K^{*\#}_{eNB}$, PCI, EARFCN-DL), and derive K_{UPenc}, K_{RRCint}, K_{RRCenc}
   $NH^{*\#}_{NCC}$ will be used in next handover key derivation. And K_{UPenc}, K_{RRCint}, K_{RRCenc} are generated from $K^{*\&}_{eNB}$,

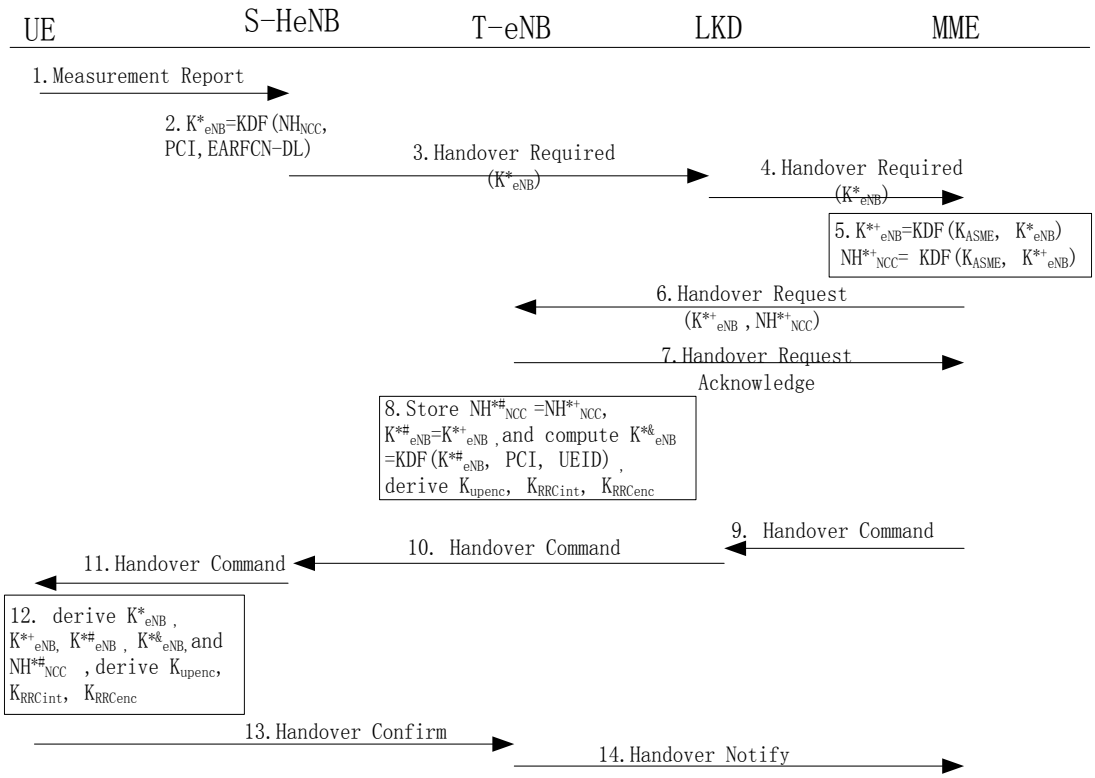

Figure 4. Key derivation during hand-out process.

and the algorithm is presented in 3GPP TS 33.401.

9. MME sends Handover Command message to LKD
   EFN-Flag = 0 is included in Handover Command message.
10. LKD relays the Handover Command message to S-eNB
11. S-eNB sends Handover Command message to UE
12. UE derives new keys for communication with T-eNB, and then derive Kupenc, KRRCint, KRRCenc
    UE generates new keys by K^{*}_{eNB} = KDF (NH_{NCC}, PCI, EARFCN-DL),
13. UE sends Handover Confirm message to T-eNB
14. LKD relays the Handover Notify message to MME.

4. Performance Analysis

In the following parts, the performance of this paper is analyzed in terms of communication time cost and computational time cost, by comparing it with previous LTE methods in 3GPP TS 33.401. And the forward/backward secrecy of this solution is analyzed theoretically.

4.1. Key Derivation Cost Analysis

There are two parts of key derivation cost, computation cost and communication cost. The communication cost includes the delay of delivery between the eNB/HeNB and the MME λ, the communication cost between the UE and the eNB δ, the cost between eNB/HeNB ε, the communication cost between HeNB and LKD α, the communication cost between LKD and MME β. Since MME is far away from eNB/HeNB, δ is range in $0 < \delta < \lambda$. And because LKD and HeNBs are connected with each other in the same way (like Ethernet) in EFN, ε and α can be considered to be equal $\varepsilon = \alpha$. With the deployment of LKD in EFN, the HeNB communicates with MME through LKD, then $\lambda = \alpha + \beta$. Since LKD is far away from MME, and it communicates with MME by an Internet link, β is always far bigger than $10 * \alpha$. **Table 1** presents the communication costs of different method in different handover process. **Table 1** shows that comparing with the previous key derivation method in LTE, LKD-based method reduces the key derivation time greatly in inter-HeNB handover in EFN without introducing extra communication cost in hand-in and hand-out process.

To test the computation cost of key derivation, the time used for the primitive cryptography operations has been measured by using C/C++ OPENSSL library tested on an Celeron 1.1 GHz processor as an UE, Dual-Core 2.6 GHz as an eNB, a LKD and a MME. The computation cost of generating a key of UE is 0.0356 ms, and computation cost of generating a key of LKD, eNB or MME is 0.0121 ms.

To show the performance of this paper visually, we gives a simulation example of communication cost as follows: The one-way latency of the LTE radio access is modelled to fit normal distribution $\delta \sim \mathrm{N}(5,1)$. The broadband link transmission delay in EFN is modelled to fit normal distribution $\alpha \sim \mathrm{N}(1,1)$. The communication delay of Internet backhaul and mobile operator networks is modelled to fit normal distribution $\beta \sim \mathrm{N}(10,20)$. And the load-dependent queuing delay is modelled as an M/D/1 system. **Figures 5-7** presents the performance of different method in inter-HeNB handover, hand-in and hand-out process in EFN.

Table 1. Compare of Communication Cost in inter-HeNB handover in EFN.

Inter-HeNB handover key derivation in EFN	Previous X2-based method of LTE	$3\delta + 2\varepsilon + 2\lambda = 3\delta + 2\alpha + 2*(\alpha + \beta)$ $> 3\delta + 24\alpha$
	Previous S1-based method of LTE	$3\delta + 5\lambda = 3\delta + 5*(\alpha + \beta)$ $> 3\delta + 55\alpha$
	LKD-based method of this paper	$3\delta + 5\alpha$
Hand-in key derivation of EFN	Previous S1-based method of LTE	$3\delta + 5\lambda$
	LKD-based method of this paper	$3\delta + 5\lambda$
Hand-out key derivation of EFN	Previous S1-based method of LTE	$3\delta + 5\lambda$
	LKD-based method of this paper	$3\delta + 5\lambda$

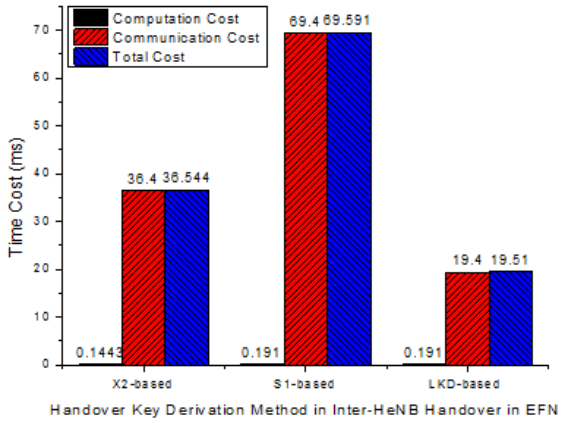

Figure 5. The Time Cost of Handover Key Derivation Methods in Inter-HeNB Handover Process in EFN.

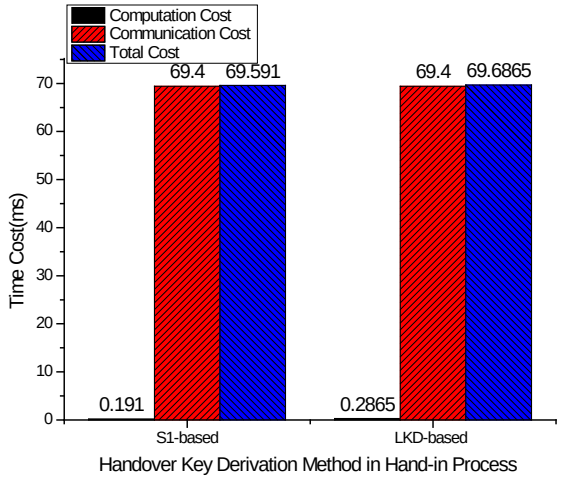

Figure 6. Time cost of handover key derivation methods in hand-in process.

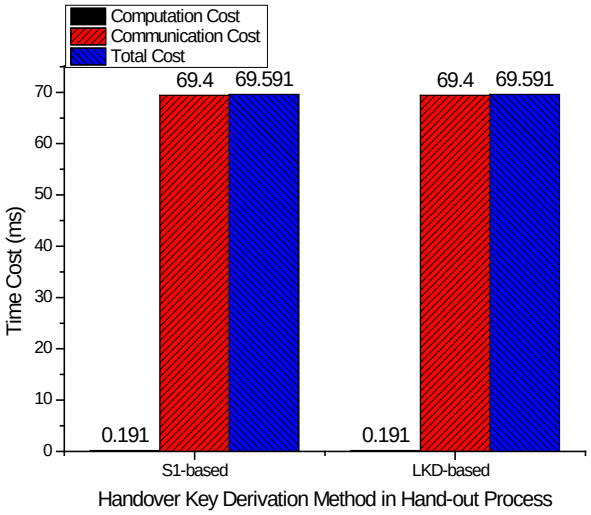

Figure 7. The time cost of handover key derivation methods in hand-out process.

Figure 5 presents the inter-HeNB handover key derivation time cost of the previous LTE X2-based method, previous LTE S1-based method and our LKD-based method (this paper). **Figure 5** shows that computation cost is nearly zero, and the communication cost accounts for the main parts of total cost. And it shows that this paper greatly reduces the communication cost, comparing to the previous X2-based method and S1-based method in LTE. This is because LKD localizes the key derivation signaling in EFN, not like the previous S1-based or X2-based method in LTE.

Figure 6 presents the handover key derivation time cost of previous S1-based method and LKD-based method (this paper) in hand-in process. **Figure 6** shows that this paper only increases 0.0955 ms in total. This is because LKD-based method only adds one step to the process of previous S1-based method to compute keys for target HeNBs. This result shows that LKD-based key derivation method generates keys for the target HeNB in EFN, with almost the same performance of previous S1-based method, meanwhile it helps the LKD get its proxy key K_{LKD} from MME. This is very meaningful because this paper introduces very little cost to allocate proxy key for LKD, which will reduce the communication cost in later inter-HeNB handover in EFN.

Figure 7 presents the handover key derivation time cost of previous S1-based method and LKD-based method (this paper) in hand-out process. The results show that the costs of the two methods are the same. This is because LKD only acts as a relay for the delivery of key derivation signaling messages.

4.2. Forward/Backward Secrecy Analysis

Based on the knowledge of forward/backward secrecy of S1-based handover key derivation, the forward/backward secrecy of the LKD-based handover key derivation method (this paper) is analyzed as follows:

In the hand-in case, the MME generates K_{LKD} and $NH^{*+}{}_{NCC}$ ($K_{LKD} = K^{*+}{}_{eNB} = KDF(K_{ASME}, K^{*}{}_{eNB})$, $NH^{*+}{}_{NCC} = KDF(K_{ASME}, K^{*+}{}_{eNB})$) for LKD by K_{AMSE}, so K_{LKD} and $NH^{*+}{}_{NCC}$ are not known to both the source eNB and the target HeNB, and then LKD uses the K_{LKD} and $NH^{*+}{}_{NCC}$ to generate new keys $K^{*\#}{}_{eNB}$ and $NH^{*\#}{}_{NCC}$ ($K^{*\#}{}_{eNB} = KDF(K_{LKD}, NH^{*+}{}_{NCC})$, $NH^{*\#}{}_{NCC} = KDF(K_{LKD}, K^{*\#}{}_{eNB})$) for target HeNB, so the keys $K^{*\#}{}_{eNB}$ and $NH^{*\#}{}_{NCC}$ are also not known to source eNB. Then the target HeNB computes $K^{*\&}{}_{eNB} = KDF(K^{*\#}{}_{eNB}, PCI, EARFCN\text{-}DL)$. So $K^{*\&}{}_{eNB}$ can't be derived from the known parameters by the source eNB. The key forward secrecy is provided in hand-in case.In the inter-HeNB handover case, the LKD generates new keys $K^{*\#}{}_{eNB}$ and $NH^{*\#}{}_{NCC}$ ($K^{*\#}{}_{eNB} = KDF(K_{LKD}, K^{*}{}_{eNB})$, $NH^{*\#}{}_{NCC} = KDF(K_{LKD}, K^{*\#}{}_{eNB})$) for target HeNB. Because source HeNB don't know K_{LKD}, $K^{*\#}{}_{eNB}$ and $NH^{*\#}{}_{NCC}$ are not known to source HeNB. Then target derives its new key $K^{*\&}{}_{eNB} = KDF(K^{*\#}{}_{eNB}, PCI, UEID)$ by which is also not known to source HeNB. So the key forward secrecy is provided in inter-HeNB handover case. In the hand-out case, the new key derivation process in LKD-based method is similar with that in S1-based handover in LTE. So the key forward secrecy is provided in hand-out case. Besides, the target HeNB knows nothing about the key materials and the key of source eNB (HeNB) in all the process, so the key backward secrecy is provided in LKD-based handover key derivation method in this paper. In conclusion, good key forward/backward secrecy is provided in LKD-based handover key derivation method in this paper.

Acknowledgements

This work is supported by China Scholarship Council (CSC) and by National Natural Science Foundation of China (No.6126104) and by the Science and Technology Project Foundation of Qinghai Province (No. 2013-Z-605 and No.2011-Z-719).

References

[1] Jaime, F., Josep, M.B., José, N.M. and Frank, Z. (2012) Traffic and Mobility Management in Networks of Femtocells. *Mobile Networks and Applications*, **17**, 662-673. http://dx.doi.org/10.1007/s11036-012-0396-9

[2] Broadband Evolved FEMTO Networks (BeFEMTO) Project (2011) The BeFEMTO System Architecture. http://www.ict-befemto.eu/publications/deliverables.html

[3] Zdarsky, F., Maeder, A., Al-Sabea, S. and Schmid, S. (2011) Localization of Data and Control Plane Traffic in Enterprise Femtocell Networks. *Proceedings of IEEE* 73*rd Vehicular Technology Conference* (*VTC Spring* 2011), Budapest, 15-18 May 2011. http://dx.doi.org/10.1109/VETECS.2011.5956622

[4] 3rd Generation Partnership Project (2012) Technical Specification Group Service and System Aspects; 3GPP System Architecture Evolution (SAE); Security Architecture (Rel 12) 3GPP TS 33.401 V12.6.0.

[5] 3rd Generation Partnership Project (2011) Technical Specification Group Services and System Aspects; General Pack-

et Radio Service (GPRS) Enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) Access (Rel 10), 3GPP TS 23.401 V10.5.0.

[6] 3rd Generation Partnership Project (2011) Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; (Rel 10), 3GPP TS 36.300 V10.4.0.

[7] Forsberg, D. (2010) LTE Key Management Analysis with Session Keys Context. *Computer Communications*, **33**, 1907-1915. http://dx.doi.org/10.1016/j.comcom.2010.07.002

[8] Bohk, A., Buttyn, L. and Dra, L. (2007) An Authentication Scheme for Fast Handover between WiFi Access Points. *Proceeding of ACM Wireless Internet Conference* (*WICON* 2007), October, 22-24. http://dx.doi.org/10.4108/wicon.2007.2282

[9] Cai, L., Machiraju, S. and Chen, H. (2010) CapAuth: A Capability-Based Handover Scheme. *Proceedings of IEEE INFOCOM* 2010, USA, March, 1-5. http://dx.doi.org/10.1109/INFCOM.2010.5462208

[10] Jin, C., Hui, L., Maode, M., Yueyu, Z. and Chengzhe, L. (2012) A Simple and Robust Handover Authentication between HeNB and eNB in LTE Networks. *Computer Networks*, **56**, 2119-2131. http://dx.doi.org/10.1016/j.comnet.2012.02.012

[11] Choi, J. and Jung, S. (2010) A Handover Authentication Using Credentials Based on Chameleon Hashing. *IEEE Communications Letters*, **14**, 54-56. http://dx.doi.org/10.1109/LCOMM.2010.01.091607

[12] Roh, H. and Jung, S. (2010) RSA-Based Proxy Signature for Media Independent Handover. *Proceeding of the First International Conference on Smart IT Applications* (*SITA* 2010), September.

[13] Qi, J., Zhang, Y., Fu, A. and Liu, X. (2011) A Privacy Preserving Handover Authentication Scheme for EAP-Based Wireless Networks. *Proceeding of GLOBECOM* 2011, December, 1-6.