Security aspects of home base station management

Pronkin Leonid,
Pudalev Timofey,
Grigorieva Olga,
Yavnoshanov Dmitriy
students of Siberian Federal University,
Krasnoyarsk, Russia,
E-mail: pudalev@gmail.com

This article discusses the main aspects of the safety of home base stations LTE's functioning. There are different ways to protect communications between system components and security features in the initial launch of base stations.

Keywords: mobile network, LTE, femtocells, HeNB, IPSec, TLS.

HeNB (Home e-Node Base) – the house base station in the LTE technology representing the low-power and miniature station to cellular communication (femtocell) intended for service of the small territory (one office or the apartment). HeNB are the first mobile network elements which operators tear in locations of the client. HeNBs connect to a network of mobile network operator through the communication link brought to the user. This channel services usually no more than several phones.

Femtocells, picocells, metrocells, and microcells belong to the category small cells — the low-power wireless access points working in the licensed frequency range and controlled by the operator.

When using of femtocells, the covering of a cellular network sharply improves in those points where it is necessary. Femtocells the same functions, as a "big" cellular cell, but in one convenient container provide. Until recently, main attention was paid to development UMTS-femtocells, however they can be created and for other standards, including for LTE.

For mobile network operator it gives the chance to improve a covering and capacity of a network, especially in buildings. There is an opportunity to provide supplementary services at reduced prices and to save on the equipment.

However, in view of many reasons, for HeNB the safety issue of data transfer is of special importance. In this regard for the first time in 3GPP of the specification of the characteristic of safety for network element management are considered so in details. Being guided by waiting on mass demand in deployment of HeNB, the management interface was completely standardized that management systems of HeNB and HeNB from different vendors could interact beyond all bounds with each other [1].

The architecture of safety of control of HeNB is based on specification 3GPP. These specifications describe the Type 1 interface, which is the interface between managing directors and managed controls of a network. This protocol provides real-time communication between HeMS (Home e-Management System) and HeNB, and defines commands and the data formats, which will be used. Besides, this protocol allows using the file transfer mechanism for loading of the software, the general configuration data, and different statistical data.

In a figure 1, the foundation architecture of control for HeNB is shown. HeMS can be located both on the operator's network, and on the Internet. If HeMS is located in the domain of the operator, the traffic of control goes through SeGW as the traffic from the Internet shan't have access to the domain of safety of the operator directly. If HeMS is located on the Internet, then direct connection via the Internet between HeNB and HeMS is realized [2].

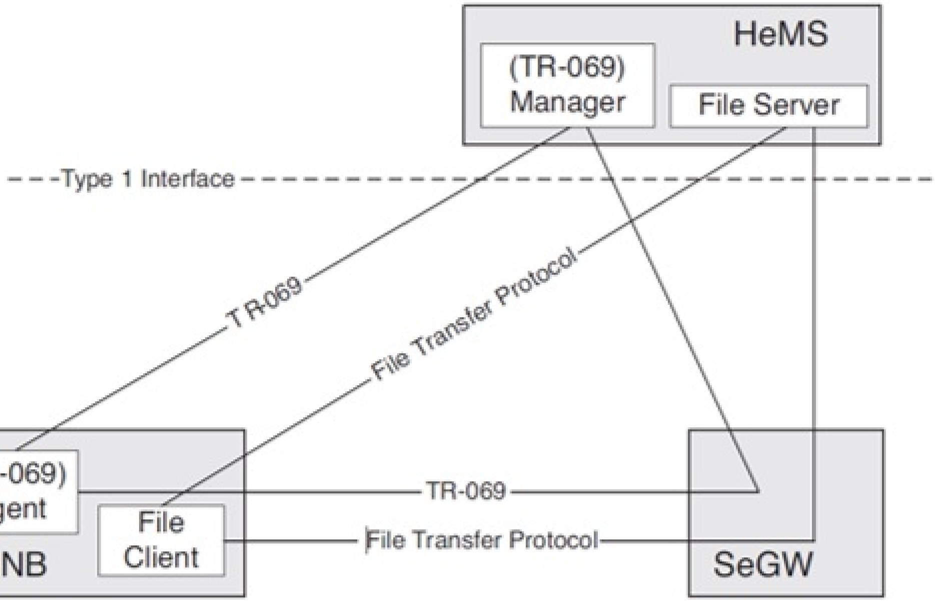

Figure 1 – Architecture of control of HeNB and HeMS

Depending on layout of HeMS different mechanisms of safety are required. It must be kept in mind that HeMS can be geographically distributed system; for example, the server of an automatic configuration and a file server can be physically partitioned [3]. It can occur if the existing infrastructure of a file server, which is generally available via the Internet, is used for support of the existing gateways; for example, HeNB and a file server DSL are partitioned by a router.

When HeMS are located in the domain of safety of the operator, the traffic of control is tunneled via the same IPsec tunnel, which is used for a signaling and the user traffic between HeNB and a basic network. Besides, if open safety between HeNB and HeMS is required, the operator can tear in addition certain mechanisms of safety for access to HeMS located in a generally available segment of the Internet.

When HeMS is available via the Internet, HeNB shall set the protected tunnel to this HeMS for traffic of control. Such protected tunnel, with use of the TLS protocol, isn't mandatory.

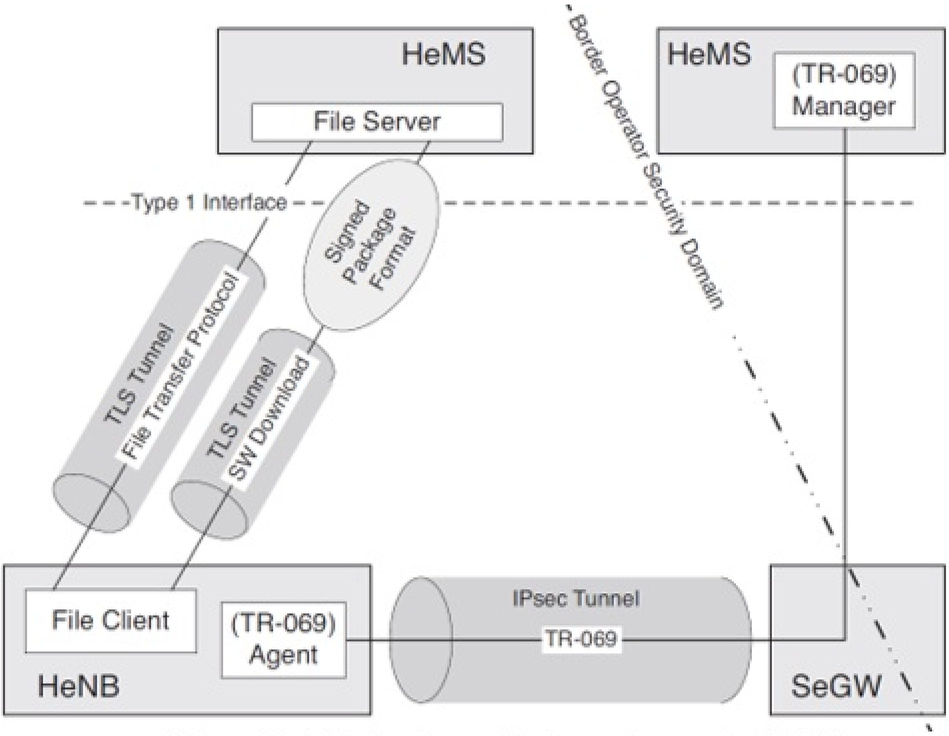

Figure 2 – Mechanisms of safety of control of HeNBs

In a figure 2 the architecture of control in a case from the distributed HeMS is shown. Also in figure mechanisms of safety and the main types of connections, mandatory for this case, are marked. The IPsec tunnel protects traffic of control between the client of HeNB and the server of HeMS. According to a policy of the operator, the interface between SeGW and HeMS and other internal network interfaces can be protected by means of the integrated means of the Zb interface. For loading of the software or any other file transfer, HeNB shall set the TLS tunnel with a file manager in HeMS before any data are loaded or downloaded.

Important aspect of safety is support of initialization of the equipment HeNB. HeMS is the general manager an element for HeNB after the first switching on of a supply, or after reset of HeNB to factory defaults. The URL address for access to these HeMS can be stored in the ciphered look in HeNB. 3GPP of the specification do not define whether belongs an initial address of HeMS to the vendor of HeNB, provider or the third party. On this network, there is a flexible procedure of connection of HeNB to the operator's networks, which is not requiring setup by the operator of certain parameters in HeNB for all HeNBs during production or delivery from manufacturing enterprises. Initial HeMS will settle down in a generally available segment of the Internet as otherwise the address SeGW shall be programmed also beforehand in HeNB.

HeMS provides to HeNB operational addresses and parameters for the subsequent net surfing of a certain operator. The choice of addresses and parameters can be based on geographical layout, which are defined in HeNB, or according to global unique identification data. Besides, primary loading of the software can be made if initial HeMS finds the outdated or inappropriate version of the software of HeNB. The safety mechanisms used for protection of HeNB are used as well to the original HeMS setup [4]. If primary HeMS is located on the operator's network to SeGW, this SeGW cause "initial SeGW", and the address of this SeGW shall be also predetermined in HeNB.

Thus, we considered only the highlights to which it would be necessary to pay attention in case of safety of control of HeNB LTE. However even short-listing potentially of weak spots of technology gives a reason seriously to think of safety of this technology of access. It is necessary to mark that eventually distribution of networks of fourth generation and growth of number of subscribers will only increase relevance of use of low-power wireless access points. Respectively will become tougher requirements to support of their safety.

Bibliography

1. Tikhvinskiy V., Terentyev S., Networks of mobile communication of LTE: technologies and architecture. – 224 pp.
2. Gelgor A., LTE technology of mobile data transfer: studies. manual. – 204 pp.
3. Hassanein H. LTE, LTE-Advanced and WiMAX. Chichester, UK: John Wiley & Sons, 2012, – 275 pp.
4. Forsberg D., Günther H., LTE Security. Chichester, UK: John Wiley & Sons, 2010, – 284 pp.