Self-Configuration in LTE Self Organizing Networks

Florian Kreitmair
Advisor: Tsvetko Tsvetkov
Autonomous Communication Networks 2013
Chair for Network Architectures and Services
Department of Informatics, Technische Universität München
Email: florian.kreitmair@in.tum.de

ABSTRACT

This paper describes and reviews the mechanics of self configuration in Long Term Evolution (LTE) mobile networks. In particular I examine the process of auto connectivity and auto commissioning in detail, with an extra look at the security setup. Furthermore I describe the dynamic radio configuration framework for configuration of parameters that depend on neighboring cells. Finally, I survey the possibilities and current status of adoption in practice.

Keywords

Cellular Networks, Long Term Evolution, Self-Organizing Networks, Self-Configuration, Dynamic Radio Configuration, Femto Cells, Cell Allocation

1. INTRODUCTION

Due to the increase of mobile communication in the last decade, mobile networks become more and more heterogeneous. This process is still going on. Meanwhile, mobile network traffic is expected to rise dramatically, pushing existing infrastructure to its limit [9] and forcing network providers to introduce more but smaller base stations to allow higher throughput per area. In consequence base stations are not only deployed by network operators any more, but also by private users to increase the coverage and capacity indoor by installing very small home base stations, called femto cells [7]. Applying changes to such complex structures, e.g. deploying a new base station, comes with a high pre-operational planning and configuration effort. LTE self configuration technology is aimed towards reducing this effort by replacing steps that had to be done manually with automatic procedures.

With LTE, several aspects of self organization were introduced for mobile communication: Apart from deployment issues, there are also ways to automatically enhance operation performance (self-optimization) and to maintain operation in case of failures (self-healing).

Traditionally, in second and third generation networks the configuration of Network Elements (NEs) was done manually. This process consumed several days to weeks and had to be done regularly to adapt the configuration to modified requirements [16]. Furthermore, base stations are usually installed at locations where manual configuration is physically difficult as they are often located outside and exposed for a better coverage (e.g. on top of masts or under the roof of a congress hall).

The main idea of self configuration is to apply changes to the hardware infrastructure without much configuration effort to reduce the operators Operation Expenditures (OPEX). In practice, the goal is just to buy a mobile network base station from a vendor and connecting it to the Internet. All the configuration is supposed to be set up automatically.

2. THE SELF CONFIGURATION PROCESS

As already mentioned in the introduction, self configuration comes as a set of distinctive steps that take place before the operation of the new NE. The complete process consists of three logical parts:

1. *Auto Connectivity*: Establishment of a secure connection to the Auto-Connection Server (ACS)
2. *Auto Commissioning*: The configuration of pre-planned parameters and installation of required software
3. *Dynamic Radio Configuration*: Configuration of parameters that need to be assign dynamically

But before this process can be executed, some preparations have to be made.

2.1 Manifacturer Pre-deployment Activities

For identification purposes, the new NE is assigned a unique identification number, called Hardware ID (HW-ID). This is a serial number for purchasing and service purposes [14].

Furthermore the device is delivered with a basic software and configuration setup, supporting all self-configuration steps before a connection to the ACS is established, thus allowing Plug&Play deployment.

Finally, a public/private key is installed to be used for initialization of a secure connection. Details of the security setup will be illustrated in Section 4.

2.2 Operator Pre-deployment Activities

The operator still has to set up the physical equipment involved such as antenna and backhaul network connectivity. But furthermore he has to provide adequate server software that supports the evolved NodeB (eNB) during self-configuration and supplies appropriate configuration parameters. More precisely, it consists of a Dynamic Host Configuration Protocol (DHCP) server to provide initial network

doi: 10.2313/NET-2013-08-1_19

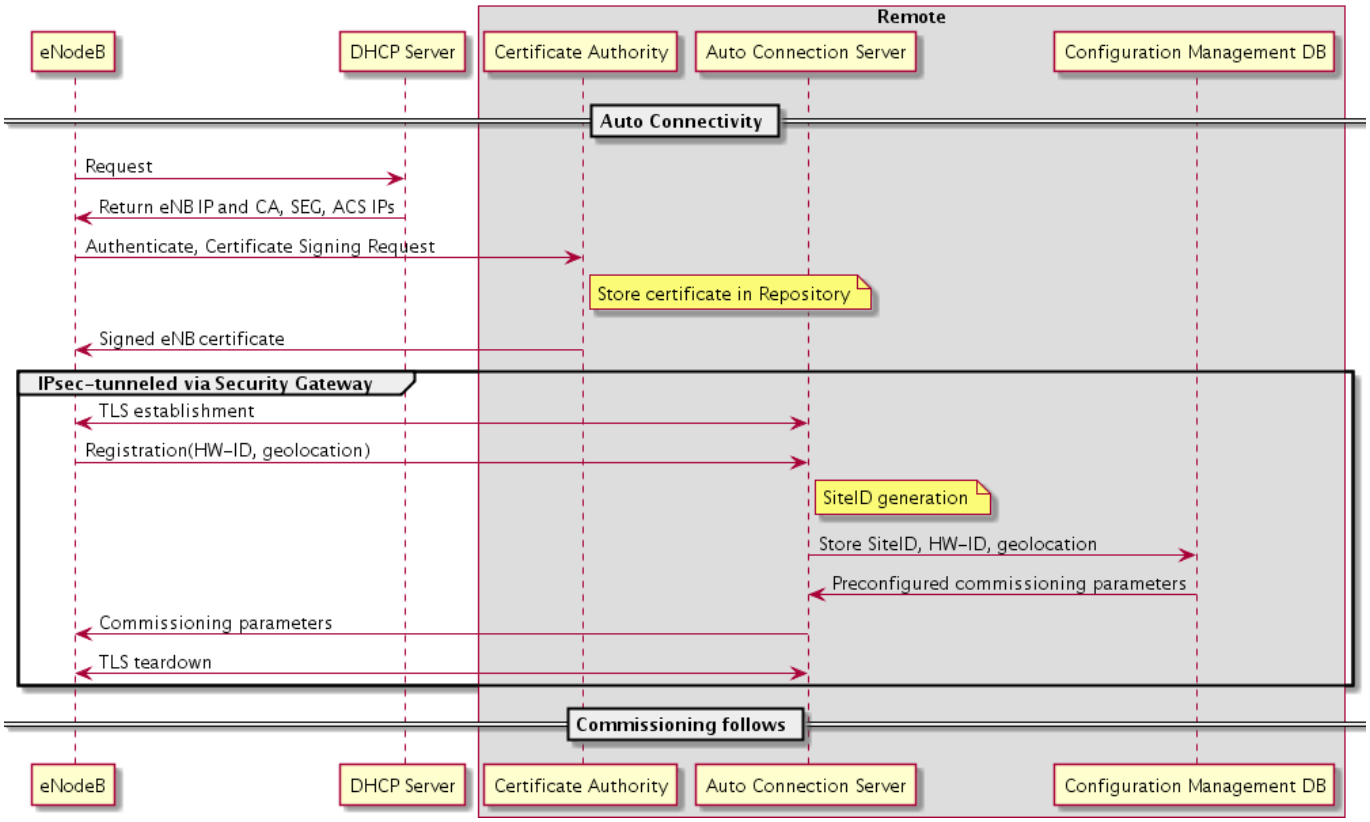


Figure 1: The Auto Connectivity Process [14]

configuration, an ACS server that provides all further configuration and a Certificate Authority (CA) infrastructure to secure the process.

The main task is, of course, the planning of new bases station sites. This is a process on its own and not a use case for self configuration. However, it must be ensured, that the configuration planned specifically for a NE gets on exactly this device. This is accomplished by a unique identification key referred to as SiteID. Usually it contains information about the location the new base station is planned for.

2.3 Self-Configuration Process

The tasks for the installer are very limited. He just has to mount the antenna, transport network, power supply and the eNB itself, connect them physically and power on the NE. The preceding steps are executed automatically. See Figure 1 for a schematic overview. In cases when the automatic configuration process fails, the installer has the possibility to phone a remote commissioner who can solve the problem manually [14].

2.3.1 Connectivity setup

The actual process beginns with a self-test procedure, to assure hardware integrity. Thereafter, a basic connection on layer 1 and 2 is set up. Typically this is done by using DHCP. Additionally to a free IP address, the DHCP-Server also replies the addresses of the ACS, CA and optionally the Security Gateway (SEG) [14]. According to [10], Bootstrap Protocol (BOOTP) and Internet Group Management Protocol (IGMP) are also feasible for this task. There are also cases in which the NE does not have connectivity to a server providing the information. Such a NE is called a Relay Node (RN) and it uses other eNBs' connectivity for establishing a connection. It acts as a regular User Equipment (UE) at configuration time and is configured with a Donor evolved NodeB (DeNB) via which all operation traffic will be routed [14].

Secondly, a connection to the ACS has to be set up because all further configuration steps need information from the operator. This connection has to be secured properly. The details about this process are covered in Section 4.

2.3.2 Commissioning & Localization

After a secure connection has been set up, it can be used to download the required software and operational configuration parameters from the ACS [10]. To determine which planned configuration is designated to be installed on the new device, the NE has to be identified via its SiteID. This can either be accomplished manually or automatically using geolocation technology or by a combination of both [15].

Former requires the installer to provide the SiteID as input to the process who reads it from a sticker or a list. The usage of bar codes or Radio Frequency Identification (RFID) tags is also possible. Alternatively, the installer provides the HW-ID which is then matched to the SiteID by the Configuration Management Database (CMDB). However, the manual option is easier to implement, but time-consuming

doi: 10.2313/NET-2013-08-1_19

and error-prone [6].

An option that tries to circumvent this drawback is to have the SiteID automatically be determined. This is done by the usage of geolocation technology, such as satellite based positioning using NAVSTAR GPS, GLONASS or Galileo infrastructure. It is important to mention that this just works if the sky is not screened what implies it is not suitable for indoor deployments. Alternatively, the position can be determined using radio beacons or by intensity measurements of WiFi networks nearby [6]. Latter works as following: If the possitions of nearby radio signal senders are known, measurements of the insity of their signals received can be used for determining the receiver's position by triangulation. This approach works the better, the more senders from diffent relative direction are within reach because the underlaying equation system gets overdetermined thus allowing the correction of errors. However, if the signal propagation is not linear, the results also gets inexact what limits the suitability for indoor measurements a bit.

After the NE has been identified, it checks its internal and external hardware and sends the result to the Operation, Administration and Maintenance (OAM) for an update of the inventory database [14]. Furthermore, the NE checks its software requirements and launches an update [14]. This allows to ship the device with only a very basic set of software that is needed to execute the process to this point. Then, the actual configuration is downloaded to the NE and activated [14]. This is possible with only a limited part of the configuration, because there also exist parameters, that depend on the devices' location and configuration of neighboring cells. This step, referred to as Dynamic Radio Configuration (DRC) is covered in Section 3.

Thereafter, a final self-test and optionally some license management procedures are performed [14]. After that, the eNB is ready for operation and can transit to operational state.

3. DYNAMIC CONFIGURATION

Apart from static configuration parameters whose values are equal all over the network and parameters that are configured manually for each device, there are also variables, that have to be determined in concern of other NEs' configuration, particularly those of the neighbor cells. The procedure that takes this into account is referred to as DRC. DRC takes hardware information, installation measurements (e.g. geolocation, antenna gain), environment parameters (e.g. SiteID), network information (e.g. performance of neighbor cells) and operator inputs [14] and calculates other well-adjusted parameters such as a list of neighbor cells automatically.

DRC is particularly helpful with setting interdependent parameters, so let me first determine which actually have such dependencies on other NEs' configuration and which have not. The 3GPP [2] introduces a classification that categorizes them into five distinctive categories:

A: Specific parameters for each cell without dependencies on others'.

B1: Parameters that have to be the same on all NEs in large parts or even the complete network.

B2: Parameters that must be unique.

B3: Parameters that must differ from their neighbor cells'.

B4: Parameters that need to be aligned with those of neighbors.

A parameters are not relevant for DRC, as the don't have interdependencies.

B1 parameters (e.g. the Public Land Mobile Network ID [5]) are easy to set, because with the ACS, there exists a central instance to make sure that all instances are configured consistently.

B2 parameters (e.g. the Evolved Global Cell Identity) should be set by DRC [13]. A centralized approach is reasonable to guarantee uniqueness. Alternatively the option can in some cases be generated by an injective function from a value that is already guaranteed to be unique (e.g. the SiteID).

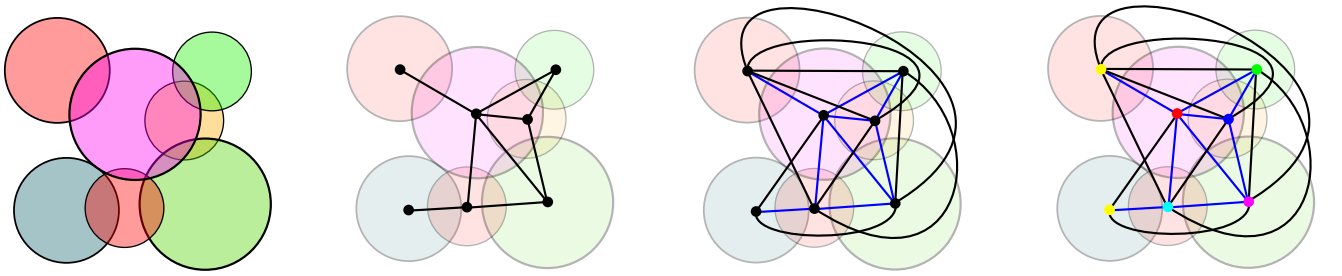
B3 parameters (e.g. the Physical Random Access Channel) should also be assigned using DRC [13]. In contrast to B2 parameters, a distributed algorithm to avoid conflicts is feasible.

For B4 parameters, dynamic assignment is mandatory. These parameters (e.g. Neighbor Relationships) have strong dependencies in their location. An example for this kind of paramater, is Neigbor Relation Table (NRT). Neighbor relations are symmetric by nature, so if one eNB has another eNB in its NRT, this should also apply vice versa.

The main challenge of automatic cell configuration is to take care of the heterogeneity of the network. There are base stations with a huge coverage as well as very small ones (pico and femto cells). The throughput that these stations are able to handle might also vary as their backhaul interfaces may have different capacities. The main goal of configuring the cell parameters automatically is to find a configuration that distributes the clients' load in way such that it takes care of the base stations' heterogeneous coverage and backhaul bandwidth. Also, handover costs should be reduced. As the optimal configuration can not always be determined at the time a new NE is installed and may change by time, improving the configuration parameters is also a constant process at operation time, covered by a technology called self optimization. But because a proper alignment of the cells' parameters is also necessary before the initialization, this also a matter for pre-operational configuration.

First of all, the coverage area of the newly inserted cell is calculated. This parameter is very important for the preceding configuration steps and for the further operation of all cells in the neighborhood. To do so, a radio propagation model is feeded with the antenna and transceiver configuration data. The output is a topological description of the cells reach. Simpler versions may only take the geographic location and make a rough approximation of the radio coverage [12]. Because this piece of information is so important, it may also be recalculated for cells in the neighborhood.

doi: 10.2313/NET-2013-08-1_19



A cellular network topology. Overlapping cells are called neighbors.

All cells are now represented by nodes. Neighbor nodes are connected by vertices.

To avoid confusions, the neigbors of neighbors are also connected with vertices.

Now the PCID assignment can be done by any standard graph coloring algorithm.

Figure 2: Transforming Cell Allocation into a Graph Coloring Algorithm.

The gained information is then used to calculate which cells overlap to generate the pre-operational NRT [14]. Furthermore the 2nd degree neighbors must be known, so a list of them is also collected. Then, B3 parameters that have to be different from their neighbors' can be assigned.

3.1 Cell Allocation

A typical parameter that has to be configured using DRC is the Physical Cell ID (PCID), a low level identifier for the cell. The value must differ from the cells' neighbors (a B3 constraint). Otherwise it would be impossible to determine from which base station a signal originates. It also must be free of confusion. Confusion means that a cell must not have neighbors which are assigned the same value as this would not allow to make a distinctive choice for handover [5]. In addition, there is just a maximum of 504 possible numbers available so it is impossible to assign unique PCIDs for the overall network. As some IDs may be reserved (e.g for new networks), further limitations apply [3]. In consequence an intelligent distribution is mandatory. Various research projects propose a graph coloring approach with colors representing distinguishable PCIDs to address this problem [13, 5, 3, 4]. This approach can be used for a number of similar problems in the scope of self-configuration. In [8] the mapping of a frequency allocation assignment problem to a graph coloring problem is described. Furthermore graph coloring can be applied to set the Primary Component Carrier Selection parameter [3].

For the PCID assignment, NEs are represented as vertices and connected with neighboring NEs by edges in the graph as shown in Figure 2. As long as less than 5 cells are overlapping, coloring these with just 4 colors would be possible, as it results in a planar graph (four color theorem). But because the distribution of PCIDs also has to be confusion-free, two cells must also not have equal PCIDs if they are connected via one other vertex. Therefore, the 2nd degree neighbors are also connected with vertices. Unfortunately this leads to a much more complex graph with lots of cutting edges which makes it hard (actually NP-hard) to determine how many colors or PCIDs are needed.

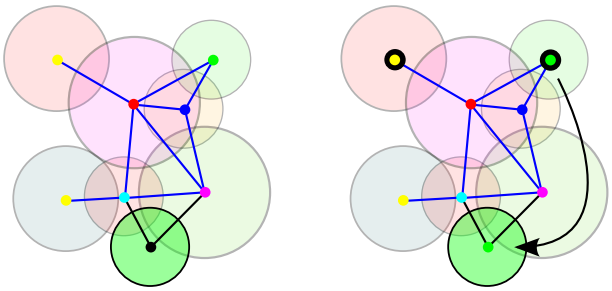
This begs the question of where the algorithm should be executed. One possibility is to execute it distributed by the NEs. On the other side it is possible to choose a more centralized approach with the Network Management System (NMS) in command. The former possibility requires a Peer-to-Peer (P2P) interface between the NEs whereas the latter concentrates more computing and communication effort on a single entity. [13] proposes to locate the management execution the higher, the larger the geographical scope of the input parameters and of the existing cells that may need to be reconfigured is. However, standardization does not provide any limitations here, so where to implement the algorithm is the vendor's choice [11].

In contrast, Ahmed et. al. [3] assessed several distributed graph coloring algorithms for their suitability and performance in the PCID distribution scenario. They concluded that distributed approaches are capable of using much less than the available PCIDs and beyond that can reduce necessary reassignments. A survey [5] tried out to find how many PCIDs are necessary for real world and randomly generated scenario. It concluded that even with a high safety margin, less than 40 PCIDs are enough in today's' deployments, even with 14 hops between each PCID reuse. However, this simulation used the cell topology of a traditional network. Overlaps might rapidly increase the more micro and femto cells are introduced, consequently requiring much more PCIDs.

The standard algorithms always calculate color combinations for a whole graph. Though, in evolutionary growing networks, this is not desirable as it would lead to many reassignment every time a new node is added. A simple algorithm by [4] aims to circumvent that: Every time a new NE is inserted, it collects the PCIDs from 3rd degree neighbors. It then uses one of them that is not assigned to 1st or 2nd degree neighbor. Figure 3 illustrates how PCIDs can be reused by this algorithm. If there is no usable PCID from 3rd degree neigbors available, it introduces a new one. If inserting the NE raised a confusion (neighbors of the new cell have the same PCID), the same assignment procedure is executed for them as well.

Another fact that must be taken into account is that the cell coverage may not allows stay the same. In dense urban environments, removing or adding buildings or even moving vehicles can have an effect on wave propagation. This means cells may become neighbors without intent what might end in the problems of confusion described above. To avoid this problem, it is recommendable to add a safety margin. [5]

doi: 10.2313/NET-2013-08-1_19



A new cell enters the network. The PCIDs assigned to 3rd hop neigbor cells are candidates for the PCID of the inserted cell. As long as they are not already taken by a first or 2nd hop neigbor, one of them is used.

Figure 3: Algorithm for Insertion of a New Cell

suggests to exclude 3rd tier or even farther nodes from the list of possible PCID for a new node.

I propose a slightly different approach. The distance in a graph does not necessarily represent the geographical distance between two cells. For example if a handful of femto cells are situated close to each other the distance between the nodes in the graph representation might be high whereas in the reality it is not. In consequence I recommend to recalculate the neighbor realtions with a probability metric. eNBs that are certainly neighbors because their coverage areas overlap get a score of 100%. Other eNB pairs get a lower value based on coverage are size, distance from each other, urban density. The goal is to express the probability of eNBs becoming neigbors in a number. Therefor it should represent the real possibility as accurately as possible. To weight the factors contributing to unintentional neighborship realtions such that the metric fulfills this requirement, measurements or simulations may be necessary. The outcome is that the network operator is able to generate a neigborship graph based on a threshold. For example all eNBs should be considered neighbors for PCID assignment if the possibility of becoming neibors is above 1 percent. This allows to state the possibility that all PCIDs are set collission and confusion free without loosing to much PCIDs. The resulting safety margin represents the real sitauation more accurately than simpler n-hop margin by [5]. On the other hand this method is much more complicated so it might just be considered when PCIDs or other numbers are about to run out.

There are also some other B3 parameters which are configured accordingly. The general approach is to model all dependencies as vertices on a node graph and then run clustering or coloring algorithms. After these parameters' values are set, handover settings such as the Tracking Area Code (TAC) the Automatic Neighbor Relationship (ANR) can be set. The ANR is another type of NRT. In contrast to the pre-operational NRT, it is enhaced by measurements of UE. Cellphones and other devices resport the PCIDs/E-UTRAN Cell Global IDs (ECGIs) of other cells they received signals from to the eNB. This method gives very accurate information about cell overlap, what makes it more feasible for actual handover execution [14].

4. SECURITY

The overall security concept is to encrypt all connections between the NEs and between the NEs and ACS, as well as to prove the identity of all involved hosts by cryptographic certificates that have been signed by a trusted CA which can be the devices' vendor, the network operator or a public CA depending on the context. Summarizing [15], there are three distinctive cases that have to be secured:

1. A secure connection with the management system is necessary to prevent all communication with the OAM system that is necessary to prevent the self configuration process from being read or manipulated by attackers.
2. The NE has to be identified to be certain its installation is acknowledged by the operator.
3. The new NE must be able to communicate with other base stations nearby. This communication should also be secured properly. For this reason, an asymmetric encryption infrastructure is used that requires the new NE to acquire appropriate certificates.

Because the establishment of a secure connection to the OAM system is so fundamental, this step is to be done very early in the self-configuration process, directly after the base connectivity is set up. For encryption Transport Layer Security (TLS) is used. As the new NE has not yet acquired a trusted certificate that proves the identity of the ACS, certificates issued by a public CA (such as Thawte, Verisign) are used. These certificates are installed by the manufacturer of the base station before shipment to the network operator. Furthermore the manufacturer installs a unique certificate on the NE that is also handed over to the network operator and allows him to identify the NE. Optionally, the NE may create the keypair itself during or after the manufacturing process. Then, the private key has never to be revealed out of the device [15].

After an early secured connection has been set up, certificates issued by the network owner itself can be downloaded from the ACS so that the provider can run its own certification infrastructure. After this step, the initial TLS connection can be torn down to be replaced by a new one which is used in the further configuration process and which uses the operator's own certificate system [15].

A main advantage for security is that because the deployments happens automatically, it is much harder to manipulate. This decreases the vulnerability through social engineering. The installer who is physically handling the device does not need to be trusted, as his influence on the devices configuration is very limited. Indeed, he still has access to the hardware that might provide a debugging interface or similar that can be a vulnerability.

5. STATUS OF ADOPTION

Self-configuration, -optimization and -healing are required features for all LTE deployments [1]. The exact self-configuration procedure is not standardized, however 3GPP published a self-configuration and software management inte-

doi: 10.2313/NET-2013-08-1_19

gration reference point to enable high-level, multi-vendor-capable supervision [14]. This allows to adapt the mechanism to device specific requirements, but also maintains interoperability. As the authentication and certificate exchange structure is specified, auto-connectivity works across devices from different manufacturers and Plug&Play behavior of eNB hardware is guaranteed.

Because self-configuration is a technology that assists with installation, but not operation of cellular networks, it is likely that the adoption will be a slow, evolving process rather than a punctual restructuration. There is little benefit in replacing working nodes with self-configuration capable devices, but the reduction of OPEX and Capital Expenditures (CAPEX) rules out the decision of applying or not applying self-configuration in future infrastructure components. However, the main rationale for applying self-configuration are not current cost savings but developments in the future: The increasing performance requirements on cellular networks demand a higher frequency reuse and denser distribution of bases station, so more but smaller NEs will be needed. In conclusion the main driver is the expectation of higher OPEX in the future [11].

The slacky specification allows much flexibility in implementation and use allowing gradual adoption of this technology. The operator is able to choose which parts of eNB deployment he wants to automate and which not. For every configuration parameter, there exist more than one method of assignment. Thus allowing the operator to fit Self Configuration seamlessly into existing business processes.

Self-configuration already is a market-ready technology that can be purchased with the latest eNB and OAM products offered by the mayor network infrastructure companies and is successfully reported working in real-life deployments. For example, the femtocell base station FAPe-hsp 5600 from Nokia Siemens Networks is delivered with a 5-step installation procedure that requires the installer only to plug in a network and a power cable to get it working.

6. CONCLUSION

Self Configuration provides a framework and a set of methods to make deployment of network infrastructure easier, more cost effective and flexible. Self Configuration decreases the planners' and commissioners' tasks from manually planning and setting configuration parameters to providing rules and constraints for them to be assigned automatically and to monitor the setup's behavior.

This paper outlined how the mechanisms behind self-configuration work and how the process is organized. First, connectivity to the operator's central configuration serves needs to be established. Security measures have to be applied to this step. Then, the automatic configuration is executed. There exist several different categories of parameters in terms of interdependence on other nodes' configuration. This survey presented a general algorithmic approach to assign parameters that need to differ from a pool of possible values. Furthermore some methods to identify the geographical site were discussed. Finally the current status of adoption was summarized.

Self-configuration raises the network's flexibility thus allowing more complex and heterogeneous infrastructure setups that is able to meet the increasing demand in availability and bandwidth. Additionally self-optimzation allows to further enhance the configuration parameters during operating time and lets the network be responsive to changing performance demand, network structure and user behaviour.

7. REFERENCES

[1] 3rd Generation Partnership Project, Sophia Antipolis Cedex. *LTE; Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Self-configuring and self-optimizing network (SON) use cases and solutions*, 2008.

[2] 3rd Generation Partnership Project, Hangzhou. *Starting material for AURANCODAP (Automatic Radio Network Configuration Data Preparation)*, 2009.

[3] F. Ahmed, O. Tirkkonen, M. Peltomäki, J.-M. Koljonen, C.-H. Yu, and M. Alava. Distributed graph coloring for self-organization in lte networks. *JECE*, 2010:5:1–5:10, 2010.

[4] T. Bandh, G. Carle, and H. Sanneck. Graph coloring based physical-cell-id assignment for lte networks. In *Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly*, IWCMC '09, pages 116–120, New York, NY, USA, 2009. ACM.

[5] T. Bandh, G. Carle, H. Sanneck, L. Schmelz, R. Romeikat, and B. Bauer. Optimized network configuration parameter assignment based on graph coloring. In *IEEE Network Operations and Management Symposium (NOMS), 2010*, pages 40–47, 2010.

[6] T. Bandh and H. Sanneck. Automatic site identification and hardware-to-site-mapping for base station self-configuration. In *IEEE 73rd Vehicular Technology Conference (VTC Spring), 2011*, pages 1–5, 2011.

[7] V. Chandrasekhar, J. Andrews, and A. Gatherer. Femtocell networks: a survey. *Communications Magazine, IEEE*, 46(9):59–67, 2008.

[8] R. Chang, Z. Tao, J. Zhang, and C.-C. Kuo. A graph approach to dynamic fractional frequency reuse (ffr) in multi-cell ofdma networks. In *IEEE International Conference on Communications, 2009. ICC '09*, pages 1–6, 2009.

[9] S. Hamalainen. Self-organizing networks in 3gpp lte. In *IEEE 70th Vehicular Technology Conference Fall (VTC 2009-Fall), 2009*, pages 1–2, 2009.

[10] H. Hu, J. Zhang, X. Zheng, Y. Yang, and P. Wu. Self-configuration and self-optimization for lte networks. *Communications Magazine, IEEE*, 48(2):94–100, February.

[11] N. Marchetti, N. Prasad, J. Johansson, and T. Cai. Self-organizing networks: State-of-the-art, challenges and perspectives. In *8th International Conference on Communications (COMM), 2010*, pages 503–508, June.

[12] F. Parodi, M. Kylvaja, G. Alford, J. Li, and J. Pradas. An automatic procedure for neighbor cell list definition in cellular networks. In *IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, 2007*, pages 1–6, 2007.

[13] H. Sanneck, Y. Bouwen, and E. Troch. Dynamic radio configuration of self-organizing base stations. In *7th International Symposium on Wireless Communication Systems (ISWCS), 2010*, pages 716–720, 2010.

[14] H. Sanneck, C. Sartori, P. Szilágyi, T. Bandh, C. Schmelz, Y. Bouwen, E. Troch, J. Goerge, S. Redana, and R. Kausl. *Self-Configuration ('Plug-and-Play')*, pages 81–134. John Wiley & Sons, Ltd, 2011.

[15] H. Sanneck, C. Schmelz, E. Troch, and L. De Bie. Auto-connectivity and security setup for access network elements. In *IFIP/IEEE International Symposium on Integrated Network Management, 2009. IM '09*, pages 691–705, 2009.

[16] R. Waldhauser, M. Staufer, S. Hämäläinen, H. Sanneck, H. Tang, C. Schmelz, J. Goerge, P. Stephens, K. Kordybach, and C. Suerbaum. *Self-Organising Networks (SON)*, pages 39–80. John Wiley & Sons, Ltd, 2011.