CUT 3

CUT 1

NOMADICLAB DAY 2013

BEYOND CONNECTIVITY

CUT 2

NOTES

CONTENT

NOTES

NOTES

AGENDA

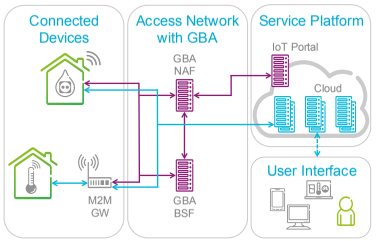
9:00 – 9:10	Stage	Event Opening	
9:10 – 9:30	Stage	Introduction to NomadicLab	Johan Torsner
9:30 – 10:00	Stage	Future Wireless Access	Janne Peisa
10:00 – 11:30	Länsitori	Demos and Coffee	
11:30 –12:30	Antell	Lunch	
12:30 – 13:00	Stage	Internet Challenges	Jari Arkko
13:00 – 13:20	Stage	Security Assurance in 3GPP	Bengt Sahlin
13:20 - 13:40	Stage	WebRTC Standardization	Christer Holmberg
13:40 - 14:00	Stage	Secure IoT Cloud	Jimmy Kjällman, Patrik Salmela
14:00 – 14:15	Länsitori	Coffee Break	
14:15 – 15:15	Stage	Cyber Arms Race	Mikko Hyppönen
15:15 – 16:00	Stage	Panel Discussion	
16:00 – 16:15	**Stage**	**Event Closing**	

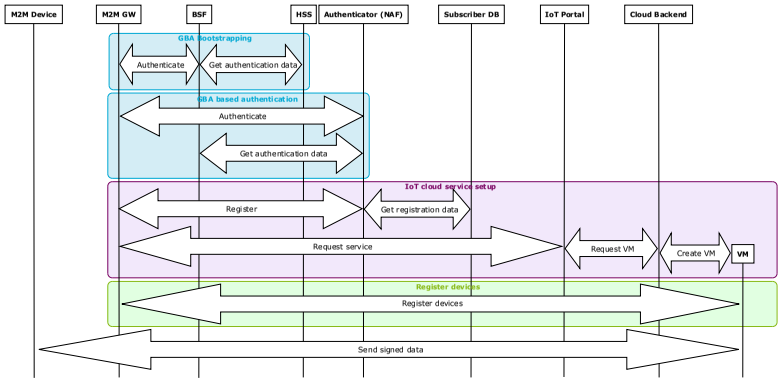
NOTES

SECURE IOT CLOUD

End-to-end solution for connected devices

- Automatic provisioning of cloud resources for devices
  - Dynamic configuration of services and networking
  - Customizable and scalable
- Authenticated access via Generic Bootstrapping Architecture (GBA)
  - 3GPP standardized authentication based on SIM credentials
  - Authentication for getting access to cloud resources
  - Secure and user-friendly mechanism
- End-to-end authentication and integrity protection of data from devices
  - Public-key elliptic curve digital signature algorithm (ECDSA)
  - Protection of data all the way through the network and cloud
  - Suitable even for constrained devices
- Horizontal solution
  - Application, service and user agnostic





Jimmy Kjällman jimmy.kjallman@ericsson.com
Patrik Salmela patrik.salmela@ericsson.com
Mohit Sethi mohit.m.sethi@ericsson.com
Tero Kauppinen tero.kauppinen@ericsson.com

INTRODUCTION TO NOMADICLAB

Ericsson is the world's leading provider of telecom technology and services to mobile operators, playing a major part in setting the standards for mobile technology and broadband. You find us in more than 180 countries, and 40% of mobile calls are made through our systems.

Ericsson Research performs cutting-edge research and innovation through cooperation with partners, customers, universities and research institutes around the world, as well as within the global Ericsson organization. Ericsson Research is a global organization consisting of approximately 600 employees in 9 research areas.

NomadicLab is Ericsson's research organization in Finland with 40+ researchers committed to making Ericsson's vision of the networked society happen. In Finland, we focus on Packet Technologies, Wireless Access Networks, Network Security and Multimedia Technologies research areas. We collaborate with major research organizations in Finland and have a strong presence in international standardization and collaboration fora. Concepts and innovations from NomadicLab are key components of 3G and 4G systems.

NOMADICLAB DAY
BEYOND CONNECTIVITY

The theme of this years NomadicLab Seminar Day is *Beyond Connectivity*. This event serves as a showcase for the ideas and projects that are shaping how we understand networking and telecommunications in the Networked Society in Ericsson Research, Finland. For the last couple of years, we have attracted the main innovators and researchers in the Finnish scene. This year, we are also inviting industry partners and other researchers in the telecommunications, networking and Machine to Machine (M2M) areas.

During the day, you will have the opportunity to hear presentations from Janne Peisa, 3GPP RAN standardization coordinator, Jari Arkko, IETF chairman, and Mikko Hyppönen, Chief Research Officer in F-Secure. Furthermore, you will have the opportunity to visit demo stands to see some of our research results. The day will end with a panel discussion on the topic "Future Challenges in Communication".

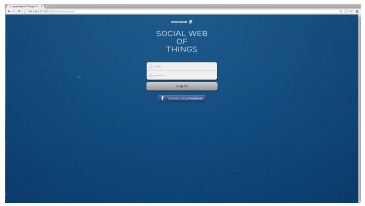
SECURE
IOT
CLOUD

NOMADICLAB DAY 2013

SOCIAL WEB OF THINGS

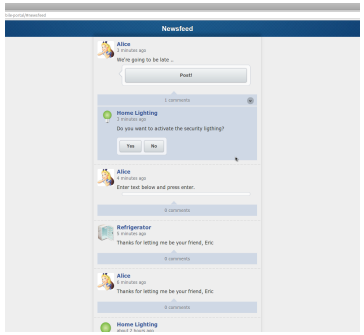
Introduction

Social Web of Things (SWoT) is an Ericsson platform prototype for Smart Homes where ordinary household items such as lamps, fans, and refrigerators are made intelligent by enabling them to communicate with each other. Using the SWoT portal, users can control their devices from anywhere in the world. Users can interact with their devices in a similar way they would interact with their "human" friends in popular social network platforms.



SWoT Portal

Users communicate with their 'Things' by posting messages on the wall. The 'Things' respond to user's post by commenting on it.

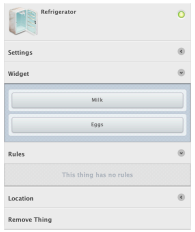


Set-Up

SWoT provides a platform where users can interact with and control a wide variety of 'Things' using a single portal. The SWoT portal is hosted in the cloud which can be accessed from anywhere and any device using the internet. An OSGi Gateway acts as an interface between the SWoT portal and the 'Things'. These 'Things' communicate with the OSGi Gateway using protocols such as Z-Wave, 6LoWPAN, CoAP etc.

Demo

In our demo, we will show how one can control lights, fan and interact with a refrigerator using an intuitive and exciting user interface. We welcome you to BLISS lab to experience our demo. See you there!



Afaque Hussain (Afaque.Hussain@ericsson.com)

Miika-Petteri Matikainen (miika-petteri.matikainen@ericsson.com)

SPEAKER PROFILES

Janne Peisa:

Janne Peisa is a Principal Researcher with Ericsson Research Wireless Access Networks in Jorvas, Finland. At Ericsson Research, Janne has been involved in the design of all major air interfaces for mobile broadband (WCDMA, HSPA, LTE). He has not only been leading various Ericsson standardization activities in 3GPP RAN for the last seven years, but also the Wireless Access research group in Jorvas. Currently, Janne is responsible for overall Ericsson technical standardization in 3GPP RAN.

Janne has a Ph.D. in Theoretical Physics, and has more than 100 patented inventions. He has also been nominated as the Ericsson Inventor of the Year 2001.

Jari Arkko:

Jari Arkko is an Expert in Internet Architecture at Ericsson Research, Finland. Currently, he is serving as the General Area Director and IETF Chair. At the IETF, he has also served six years as one of the Internet Area Directors in the Internet Engineering Steering Group (IESG) and one year as a member of the Internet Architecture Board (IAB). Jari has published IPv6 related documents and 36 RFCs, including specifications for Mobile IPv6, EAP-AKA, Diameter, and SEND. He has previously served as a chair of three IETF working groups.

Jari has also worked in the Technical Advisory Board for the IP Smart Objects Alliance (IPSO) and is involved in a number of research projects at Ericsson. In the past, Jari has worked on the implementation of routers, VPN software, testing tools, modem banks, cellular network nodes, AAA systems, compilers, and AI systems. He received his Licentiate's degree from Helsinki University of Technology in 1996.

Jari's main interests in the Internet include architecture, IPv6, small protypes, the Internet of Things, social media, Internet governance, and cutting through hype that often surrounds some aspects of our technology. He likes to build and use the technology that he works with. For instance, he moved to an IPv6-only network in 2010 and builds smart home networks as a hobby. He frequently communicates with his laundry on Facebook.

SPEAKER PROFILES

Mikko H. Hyppönen (Guest Speaker):

Mikko Hyppönen is the Chief Research Officer of F-Secure. He has worked with F-Secure in Finland since 1991 and he is also a TED Speaker.

Mr. Hyppönen has led his team through the largest outbreaks in history. He named the infamous Storm Worm, was part of the Conficker Working Group, and he has produced classified briefings on the Stuxnet worm. Mr. Hyppönen has assisted law enforcement in USA, Europe, and Asia on cybercrime cases. He has written for international publications such as Scientific American, Wired and Foreign Policy, and The New York Times.

Mr. Hyppönen has addressed the most important security-related conferences worldwide. He has been the subject of hundreds of interviews in global media, including a 9-page profile in Vanity Fair.

Mr. Hyppönen was selected among the 50 most important people on the web by the PC World magazine and was included in Foreign Policy's Top 100 Global Thinkers list. He also received the Virus Bulletin Award, awarded every ten years, as the "Best Educator in Industry". Mr. Hyppönen sits in the advisory boards of ISF and The Lifeboat Foundation.

Apart from computer security issues, Mr. Hyppönen enjoys collecting and restoring classic arcade video games and pinball machines from past decades.

Andras Vajda (Guest Panelist):

Andras Vajda is an Expert on Cloud Architecture and Management within the CTO office. He was one of drivers for establishing Ericsson's cloud program, scoping and initiating both the cloud management track as well as the initial scope and strategy for Ericsson's cloud system. He's currently supporting the execution of the strategy within product line Cloud Systems.

In the past, he was one of the initiators of Ericsson's cloud and many-core programming research efforts, driving the strategy and architecture work. He was also responsible for co-coordinating Ericsson's software research activities and the interaction with external parties in the area of many-core programming. He is the author of the book "Programming Many-core Chips", published by Springer in 2011.

SOCIAL WEB OF THINGS

NOMADICLAB DAY 2013

ERICSSON 3D VIDEO CONFERENCE SYSTEM

Overview

Ericsson 3D Video Conference System is an innovation prototype, which aims to provide user better experiences with Video Conferences by bringing 3D video effects. Today's demo is a early phase prototype.

Target Applicable Use Cases

Ericsson 3D Video Conference system can potentially be used in following areas:

- Mega sized international cooperation
- Remote education providers
- Telecommunication operators
- E-Health
- Show product prototype in 3D mode
- Private consumers with 3D home theater

Our Objectives

We are working on implementing the Video Conference System in 3D mode with following features:

- Video conference with glasses-free multi-viewer 3D display
- 2D/3D clients interworking

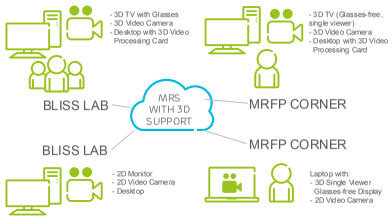
Currently we have only the 3D TV with glasses in our lab and used for today's demo

3D Video camera and TV is available in the market from different vendors

In Ericsson Research's Lab in Kista we have one 3D glasses-free multiviewer TV

Our Lab Environment

The prototyping is still ongoing but the following illustration clarified the future 3D Video Conference test environment in our lab.



Ge Liu (ge.liu@ericsson.com)

Dietmar Fiedler (dietmar.fiedler@ericsson.com)

PRESENTATIONS

Future Wireless Access (Janne Peisa)

Wireless access systems have evolved from the first generation analog systems to the current state of the art fourth generation systems providing gigabit per second mobile broadband connectivity. The future radio access ("5G") will fulfill the Ericsson vision of connected society, and will consist of the evolution of the existing systems as well as complementary radio interfaces to address the situations where the evolution of the existing systems is not feasible.

The main challenges that the future radio access needs to handle are massive growth in traffic volume, massive growth in connected devices, as well as wide range of requirements and characteristics.

The evolution of data rates and latency will continue for 5G, and the traffic capacity can be enhanced by increasing available spectrum, densifying the network, and improving spectrum efficiency. The main available spectrum for time up to 2020 is expected to be below 6 GHz. While the capacity of higher frequencies are promising, more research is needed to exploit them. For network densification, simple deployment and back-haul availability are the main challenges, while for spectrum efficiency the main improvements are expected to come from advanced antenna systems and interference coordination.

Internet Challenges (Jari Arkko)

Working with Internet technology often involves details deep inside the technology. But it seems that this year has been a perfect storm of highly visible and important technical developments: A major upgrade to HTTP, the basis of all web communications, work on future transport protocols, including proposals to add security directly to TCP, making voice and video calls directly in web browsers without special applications or plug-ins, and, of course, mass Internet surveillance. These were clearly the discussion that have received most attention at our recent IETF meeting in Vancouver.

What can we do about improving the situation? And should we? This presentation summarizes where we are and what the IETF is going to do with regards to pervasive monitoring. Of course, technology is only a partial solution, but we are treating pervasive monitoring as a sign of inherent privacy problems in the Internet technology, and are looking at ways to make widespread collection of information harder. One approach is making a larger fraction of Internet traffic encrypted.

PRESENTATIONS

Security Assurance in 3GPP (Bengt Sahlin)

In the Networked Society, everything that can benefit from a connection, will be connected. Appropriate security will be an instrument in realizing the full potential of the Networked Society.

Traditionally, 3GPP specifies interfaces between communicating nodes and protocols needed for interoperability. The security work in 3GPP has concentrated on ensuring appropriate security among these interfaces. Consequently, 3GPP has not earlier indicated security requirements for the nodes. The security assurance work will change the situation and Security Assurance Specifications (SAS) will be specified in 3GPP in the future.

The first SAS will be specified for the MME network product class. Global and open specifications for communication protocols security and Security Assurance Specifications are important to ensure appropriate security for the Networked Society.

WebRTC Standardization (Christer Holmberg)

WebRTC is a new technology, providing the means to incorporate real-time media in web browser applications without the need for third-party plug-ins. In addition to the web community, traditional telecom community is also showing interest in the new technology to see how it can be integrated with existing services, and how it can be used to provide new value.

The presentation gives a status update of the standardization work related to WebRTC that currently takes place in different standardization organizations.

Secure IoT Cloud (Jimmy Kjällman and Patrik Salmela)

We present a horizontal end-to-end solution for automatically connecting devices, such as smart objects, to a cloud backend where data from the devices is stored and processed. The solution enables easy deployment of connected devices and M2M gateways since allocation and customization of resources in the OpenStack- and KVM-based cloud is handled automatically by an IoT Portal. Moreover, access to cloud resources is secured via 3GPP-standardized GBA bootstrapping and authentication using SIM credentials, which requires no user interaction.

Another important concept that we demonstrate is end-to-end integrity protection and source authentication of data objects with elliptic curve-based signatures in an environment where data passes through multiple intermediaries. Our solution shows that this protection mechanism is feasible even when the devices are very simple and constrained.

ERICSSON 3D VIDEO CONFERENCE SYSTEM

NOMADICLAB DAY 2013

SPACES: CONTEXTUAL COMMUNICATION PLATFORM

Contextual Communication

Contextual communication refers to the ability to embed unified communications (e.g., telephony, video, presence, messaging, and content sharing) into the context of other applications. Examples include:

- Embedding communication methods directly into business processes and applications. As an example, embedding video communication into a purchase order approval software
- Adding real-time video to a web-based chat between a customer and a call center agent
- Field engineer and a Network Operations Center (NOC) agent dynamically adding document sharing and video into an ongoing VoIP session

WebRTC

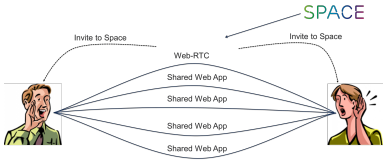
Web Real-Time Communication (WebRTC) turns web browsers into full-blown standards-based unified communication endpoints without requiring any plugins to be installed. WebRTC, together with HTML5, makes it possible to communication-enable for instance web-based business applications.

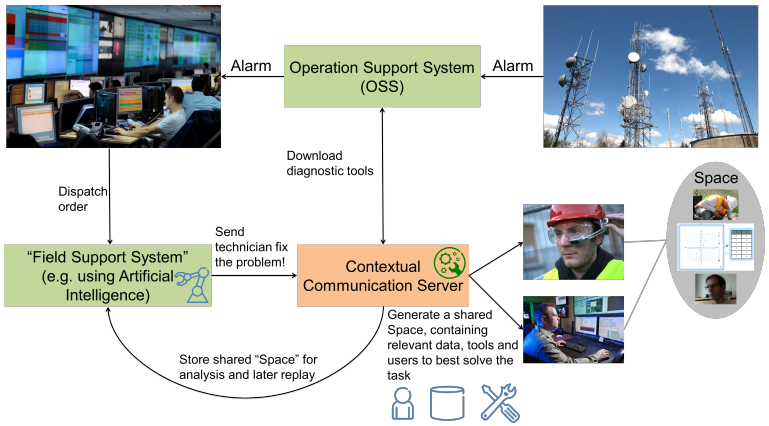
Spaces

Spaces is a web-based toolkit for building WebRTC-enabled contextual communication applications. Spaces consists of a number of components:

- Galaxy - widget repository
- Spaces – framework allowing widgets to be assembled into a contextual communication application
- Distributed Shared Memory (DSM) – synchronization engine to synchronize content on different users' screens
- Nebula – command line widget development tool running in the browser

Spaces enables the rapid creation of customized contextual communication applications tailored to the needs of the current communication situation.



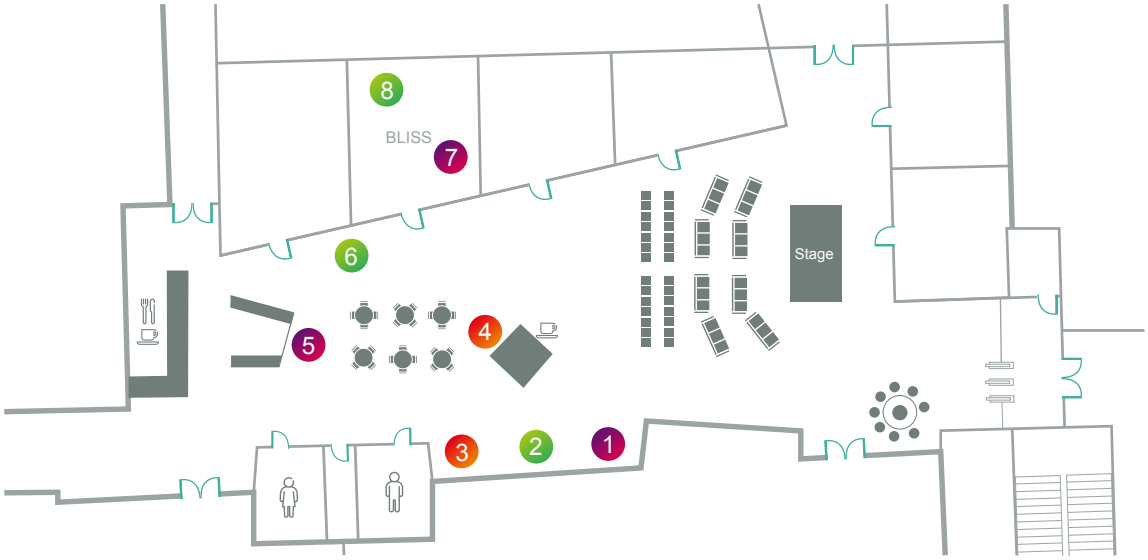


PRESENTATIONS

Cyber Arms Race (Mikko Hyppönen)

Protection against online attacks is hopeless without understanding the enemy. In this presentation, Mikko Hyppönen will present mechanisms to analyze potential attackers, their motives, as well as examples of possible attacks, and how online infections are detected. Another interesting aspect is the way companies in security business work and how F-Secure has become successful in this area. Mr. Hyppönen will give an update on current IT security, revolution in defense technology, and what is going to happen in the future.

MAP OF THE VENUE



1 Self-configuration in Capillary Networks
2 Heterogeneous Network Indoor Demonstrator
3 Competition: Heterogeneous Network for Paris
4 Security-SLA for the Cloud
5 IDS Integration in OpenStack Cloud
6 Spaces: Contextual Communication Platform
7 3D VisualCom
8 Social Web of Things

SPACES: CONTEXTUAL COMMUNICATION PLATFORM

NOMADICLAB DAY 2013

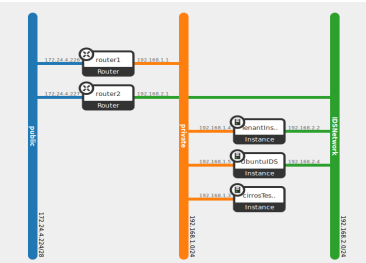
IDS INTEGRATION IN OPENSTACK CLOUD

Objective

- Integrating IDS interface with Tenant Networks in OpenStack Cloud.
- Monitor network intrusions in the Cloud network in a scalable and flexible manner.
- Expose everything via a REST API.
- Techniques Used: Port Mirroring and sFlow.

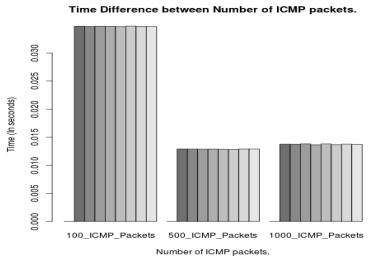
Network Topology

- A multi-NIC Tenant instance is spawned and it connects to two networks: the private network and the IDS network. The private network connects to the external world whereas the IDS network is a local network.
- On starting the IDS service, the IDS instance on Ubuntu is spawned on the same network as the Tenant instance. The instance now mirrors the network traffic from the Tenant instance.



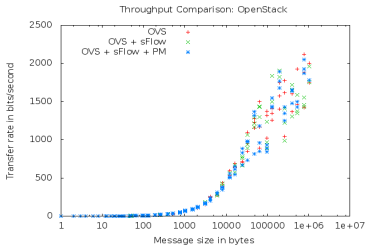
Port Mirroring

- We create a "dummy" port on the IDS instance in Ubuntu and mirror the network traffic from the Tenant instance to the IDS instance.
- There is a time difference between packets that are received on the Tenant port and the packets received on the IDS port.
- Experiment conducted to load the tenant instance with varying number of ICMP and UDP packets and measure the time difference in packets received on the Tenant instance and the IDS instance.



sFlow

- Using sFlow we send the virtual switch traffic to a sFlow client. The traffic can then be analyzed using a sFlow client tool such as sFlow Trend.
- However, sFlow, if not configured properly, can hamper the network throughput.
- Experiment conducted to compare the throughput comparison in OpenStack using Open vSwitch Plugin.



Udit Anand (udit.anand@ericsson.com)

Abu Shohel Ahmed (ahmed.shohel@ericsson.com)

DEMONSTRATIONS

1 Self-configuration in Capillary Networks

Our assumption is that there are going to be 50 billions of connected devices by 2020. Most of them are not going to be directly connected to the 3GPP network, but rather through a Capillary Networks based on 802.11 or 802.15 standards such as WLAN, Bluetooth Low Energy (BLE), or XBee. As a consequence, the number of Capillary Gateways will increase. The cost of devices' and gateways' manual configuration and management are expensive, due to their sheer amount and problematic deployment. Therefore, automatic algorithms will become commonplace.

In this demo we focus on the Capillary Network, a part of a larger Machine-to-Machine (M2M) scenario. Machine devices, i.e., sensors and actuators, are connected to the capillary network through capillary gateways with 3G/4G connectivity. Our aim is to simplify management by automation and utilization of cloud technologies. The configuration and addressing of the capillary network is automatically performed using HomeNet. With a large number of gateways, we demonstrate a case of automatic management, where the gateways share information and collaborate to select their channels and sleep schedules in order to reduce interference. Machine devices are automatically connected to the most optimal gateway in terms of battery and load level. The configuration of each gateway and device can be remotely monitored using the visualization and management interface. Channel assignments are presented graphically on a map.

2 Heterogeneous Network Indoor Demonstrator

The Heterogeneous Networks Demonstrator is a tool for visualizing simulation results for different HSPA and LTE radio network deployments. The demonstrator is capable of visually presenting different Key Performance Indicators (KPIs) of a currently selected radio network deployment for different cities as a function of increasing traffic load.

The Heterogeneous Networks Demonstrator visualizes how an operator can cope with increased traffic load by improving the deployed radio network, densifying the radio network and adding low power nodes to the radio network. The demonstrator application shows how to achieve this goal with both outdoor and indoor nodes. Additionally, the demonstrator shows that adequate power and coordination between radio network nodes improves performance.

DEMONSTRATIONS

3 Competition: Design a Cost Effective Heterogeneous Network for Paris

At this demo stand, you will have a chance to participate in a competition where you will try to improve the network coverage and end user performance for Paris (France) using our radio network simulator.

The simulator provides a base deployment that allows you to modify your own heterogeneous network by, for example, improving, densifying, and adding small cells in order to achieve the most cost-effective solution.

4 Security-SLA for the Cloud

Service Level Agreements (SLA) play a very important role in today's cloud based service delivery model. Nonetheless, security has not yet been included in the mainstream cloud SLA. However, if we can include security in the SLA, it can aid in boosting trust towards the cloud.

Our research focuses on analyzing the feasibility of Security-SLA in the cloud, developing a process for Security-SLA management, and a proof-of-concept (PoC) prototype implementation to demonstrate how the Secure-SLA works in the cloud. Our demo presents a Security-SLA solution starting from the SLA negotiation to the monitoring in the cloud. This negotiation is done using a web-based user interface. After that, our automated Security-SLA manager takes over and makes necessary decisions and monitoring for Virtual Machine deployment. When the deployment is finished, a monitoring agent running inside the VM, sends monitored data to a centralized server. In this way, the customer can monitor the current security status of the VM on a web interface, notice possible violations, and be able to resolve the issues in time.

5 IDS Integration in OpenStack Cloud

In this project, we demonstrate an implementation that integrates an existing Intrusion Detection System (IDS), SNORT, with OpenStack Cloud. The OpenStack Networking Component has an extension framework, which allows it to deploy and manage additional network services such as IDS, load balancing, firewalls and virtual private networks (VPN) within the OpenStack Cloud.

We provide a proof of concept by mirroring the network traffic from a user network interface of the cloud infrastructure to an interface located on a different virtual machine. At this mirroring interface, the traffic is continuously monitored using the IDS. Furthermore, we implement an API, "IDSstart", which can initiate the IDS services for the infrastructure user from the management UI.

IDS INTEGRATION IN OPENSTACK CLOUD

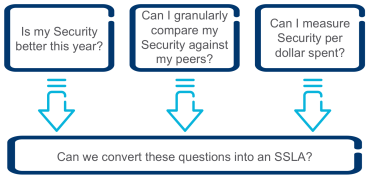
NOMADICLAB DAY 2013

SECURITY-SLA FOR THE CLOUD

Objective

Service level agreements (SLA) plays an important role in today's cloud based service delivery. Nonetheless, it is intriguing to notice that, security, being one of the major concerns in the cloud arena, has not been included in the mainstream SLA yet. Therefore, our goal is to i) Investigate the feasibility of Security-SLA for the cloud, ii) Process development for Security-SLA management and finally iii) Develop a Proof-of-Concept (PoC) prototype.

Driver for Security-SLA



Security Parameters

In our PoC implementation, we have considered two different security parameters. These are:

i) VM Container Security profile: this identifies the security level of the physical machines where the VMs will be deployed.

ii) VM Application Security profile: this indicates the application level security requirements for the VM.

Key Aspects

PoC consists of three main components:

i) SLA ENGINE:

Presentation, metric definition, and deployment of SLA.

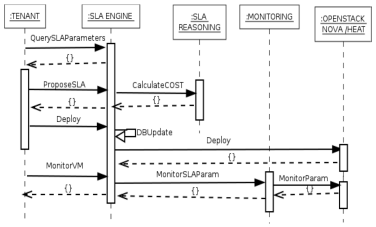
ii) SLA REASONING:

SLA splitting, cost calculation and constraint solver.

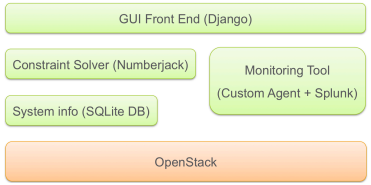
iii) MONITORING:

Real time/periodic monitoring of security-SLA parameter, dashboard for user-friendly display.

Sequence Diagram of our Solution



Components of the PoC



Challenges

The challenges that we faced during our research mostly are very generic to security itself. These are:

- Security is not quantifiable or measurable easily.
- Without an appropriate observable/measurable quantity, it is not possible to monitor a service for QoS performance analysis
- *"If it is not measurable, then it is not manageable"*
- Security is very subjective.
- Security risks are propagated–difficult to give insurance.
- Lack of motivation from Industry: Compliance over Security SLA.

Kazi Wali Ullah (kazi.wali.ullah@ericsson.com)

Abu Shohel Ahmed (ahmed.shohel@ericsson.com)

DEMONSTRATIONS

6 Spaces: Contextual Communication Platform

Spaces is a web-based toolkit for enabling contextual communication applications with Web Real-Time Communication (WebRTC). The rapid creation of customized contextual communication applications is tailored to the needs of the current communication situation. It turns web browsers into full-blown standards-based unified communication endpoints without requiring any plugins. Together with HTML5, Spaces makes it possible to communication-enable for instance web-based business applications.

In this demo, we demonstrate two different components of the Spaces, i.e., a Graphical User Interface (GUI) and a Distributed Shared Memory (DSM) which synchronizes content on different users' screens.

7 3D VisualCom

Ericsson 3D Video Conference System is an innovation prototype, which aims to provide better experience with Video Conferences by bringing 3D video effects. The demo shows an initial prototype, where each side of the test environment consists of 3D camera with 2 lenses, a video procession card, 3D enabled monitor, a prototype version of Ericsson Video Conference client (VIC), and a headset/microphone. The 3D communication is realized by sending side-by-side video in real time.

8 Social Web of Things (SWoT)

Social Web of Things (SWoT) is an Ericsson platform prototype for Smart Homes where ordinary household items such as lamps, fans, and refrigerators are made intelligent by enabling them to communicate with the user.

Using the SWoT portal, users can control their devices from anywhere. They can also interact with their devices in a similar way they would interact with their friends in popular social network platforms.

SECURITY-SLA FOR THE CLOUD

NOMADICLAB DAY 2013

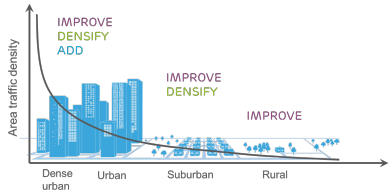
HETEROGENEOUS NETWORK FOR PARIS

Heterogeneous Networks

Mobile broadband is all about providing a seamless user experience for smartphones and mobile broadband services – whether on the move, in the office or at home. To meet the demand and competition, it is essential to expand capacity and coverage in a smooth, cost-effective way.

Improving Macro

Improving existing macro cell sites involves deploying more spectrum, advanced antennas, higher-order diversity on the receiver and/or the transmitter, and greater baseband processing capacity within and between nodes.



Densifiying the macro

Densifying the macro network involves the targeted addition of strategically located (smaller) macro cells to improve capacity and data rates, particularly when it is no longer feasible to continue improving the macro network to meet the demand alone. This approach keeps the total number of sites relatively low, while network performance becomes less sensitive to traffic location.

Adding small cells

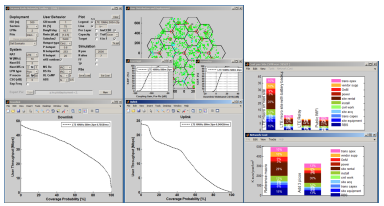
Adding small cells involves complementing macro cells with micro cells, pico cells and Wi-Fi, as well as dedicated indoor solutions. It delivers high per-user capacity and rate coverage in high-traffic areas, with the potential to improve performance in the macro network by offloading traffic generated in hotspots. Overall network performance will depend on the degree of integration and coordination that can be achieved throughout the heterogeneous network.

How and when to use each tool depends on the existing networks (macro site density), the availability of backhaul (whether owned or leased), the availability of spectrum (whether licensed or unlicensed), estimated traffic volumes, and required data rates, as well as the technical and economic feasibility of each individual approach.

Competition

Your mission is to improve the network coverage and end user performance of Paris (France) using our radio network simulator with the most cost effective solution.

The simulator provides a base deployment that you will be allowed to modify in order to reach the goal.



Edgar Ramos (edgar.ramos@ericsson.com)
Riikka Susitaival (riikka.susitaival@ericsson.com)

POSTERS

COMPETITION: HETEROGENEOUS NETWORK FOR PARIS

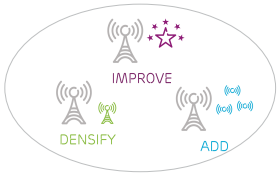
NOMADICLAB DAY 2013

HETEROGENEOUS NETWORK INDOOR DEMONSTRATOR

Improving network performance

Mobile broadband is all about providing a seamless user experience for smartphones and mobile broadband services. The key is to improve network performance involves a combination of improving and densifying the macro cellular layer for general coverage and capacity and adding small cells in strategic places.

How and when to use each tool depends on the existing networks (macro site density), the availability of backhaul (whether owned or leased), the availability of spectrum (whether licensed or unlicensed), estimated traffic volumes, and required data rates, as well as the technical and economical feasibility of each individual approach.



Improving indoor performance

Aside from the general need to improve coverage and capacity, one specific challenge for mobile operators is to meet end-user expectations indoors. The macro network has always been designed to meet the needs of general indoor coverage, but there will be areas or buildings that require improvement in order to achieve an acceptable level of service coverage.

If additional outdoor sites can be found – either for macro cells or street level micro cells – that is an attractive option to resolve general coverage and capacity needs. Alternatively, promising potential applications for dedicated in-building solutions include:

•Locations where end-user need and willingness to pay for higher performance justifies indoor solutions, for example at enterprise sites

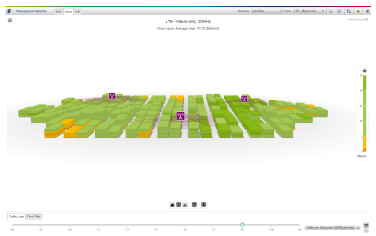
•Indoor traffic hot-spots like airports and malls where substantial traffic is captured by the indoor solution

•Key buildings which need coverage, for example to meet regulatory requirements, but where outdoor-to-indoor penetration loss is high.

The indoor demonstrator

The Heterogeneous Networks Demonstrator is a tool for visualizing simulation results for different HSPA and LTE radio network deployments. The demonstrator is capable of visually presenting different Key Performance Indicators (KPIs) of a currently selected radio network deployment for different cities as a function of increasing traffic load.

The Heterogeneous Networks Demonstrator visualizes how an operator can cope with increased traffic load by improving the deployed radio network, densifying the radio network, and adding low power nodes to the radio network. The demonstrator application shows how to achieve this goal with both outdoor and indoor nodes. Additionally, the demonstrator shows that adequate power and coordination between radio network nodes improves performance.



Stefan Wager (stefan.wager@ericsson.com)

SELF-CONFIGURING CAPILLARY NETWORKS

NOMADICLAB DAY 2013

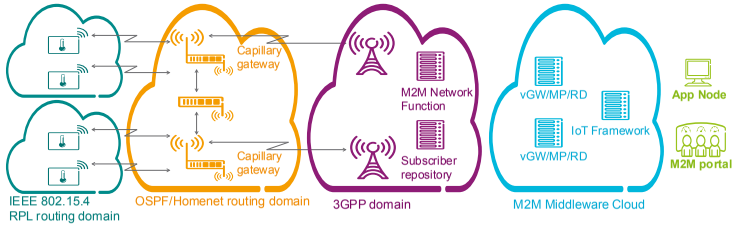
SELF-CONFIGURING CAPILLARY NETWORKS

The idea

In machine-to-machine (M2M) networks with a high number of devices, the need for manual management must be minimized. For that purpose we prototyped an autonomous, self-configuring M2M network. This demo focuses on two cases of self-configuration of the capillary network: channel coordination and gateway selection.

Channel coordination

As the number of gateways increases, the network planning quickly becomes complex. The first demo shows a case of automatic management where the capillary gateways collaborate to select their channels in order to reduce interference with the surrounding gateways.



Testbed components

M2M devices: Contiki based devices with different sensors and actuators accessible via a CoAP API. Each device is connected to the M2M network through a IEEE 802.15.4 capillary network with RPL routing.

Capillary gateways: Provide 3G/4G connectivity to the capillary network. Gateways are self-configured using HomeNet and support the capillary network via prefix delegation and automatic gateway selection. Our gateways are implemented on OpenWRT based Buffalo routers with a Contiki based RPL root for IEEE 802.15.4 connectivity.

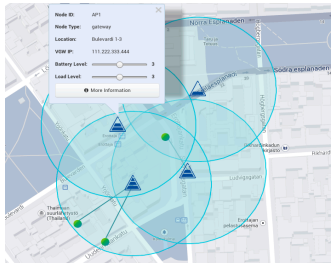
M2M Middleware cloud: An OpenStack cloud platform in which we can instantiate virtual machines for M2M devices to provide an M2M middleware component for them. The IoT Framework provides advanced services based on the device data.

M2M Network Function: Manages connectivity for the capillary network and controls instantiation of virtual machines. Middleware and devices connect to it via a HTTP REST interface.

Visualization and management interface: Provides a graphical interface for displaying and modifying various properties of the gateways, sensors and actuators in the M2M network.

Gateway selection

The second demo shows how the M2M devices are directed to the most optimal gateway in terms of load and battery power. To demonstrate this, the load and battery constraints can be adjusted. The M2M Network Function provides the gateways with the policy specifying the goals for the selection. The policy, the constraints and the connectivity information is distributed between the gateways using OSPF.



HETEROGENEOUS NETWORK INDOOR DEMONSTRATOR

NOMADICLAB DAY 2013