SPONSORED BY THE
Federal Ministry
of Education
and Research

ASMONIA

Attack analysis and **S**ecurity concepts
for **MO**bile **N**etwork infrastructures,
supported by collaborative **I**nformation exch**A**nge

Evaluation of Protection Concepts

Evaluation Report

D5.3-1.0

Contributors:

Cassidian / EADS Deutschland GmbH

ERNW Enno Rey Netzwerke GmbH

Fraunhofer Research Institution for Applied and Integrated Security (AISEC)

Hochschule Augsburg

Nokia Siemens Networks Management International GmbH

RWTH Aachen

Editor: Mirko Haustein (Cassidian / EADS Deutschland GmbH)

Author(s)	Company	E-mail
Mirko Haustein	Cassidian	mirko.haustein@cassidian.com
Paul Kirner	Cassidian	paul.kirner@cassidian.com
Herbert Sighart	Cassidian	herbert.sighart@cassidian.com
Hendrik Schmidt	ERNW	hschmidt@ernw.de
Peter Schoo	Fraunhofer AISEC	peter.schoo@aisec.fraunhofer.de
Mark Gall	Fraunhofer AISEC	mark.gall@aisec.fraunhofer.de
Manfred Schaefer	Nokia Siemens Networks	manfred.schaefer@nsn.com
Peter Schneider	Nokia Siemens Networks	peter.schneider@nsn.com

About the ASMONIA project

Given their inherent complexity, protecting telecommunication networks from attacks requires the implementation of a multitude of technical and organizational controls. Furthermore, to be fully effective these measures call for the collaboration between different administrative domains such as network operators, manufacturers, service providers, government authorities, and users of the services.

ASMONIA is the acronym for the German name* of a research project that aims to improve the resilience, reliability and security of current and future mobile telecommunication networks. For this purpose the ASMONIA consortium made up of several partners from academia and industry performs a number of research tasks, based on the specific expertise of the individual partners. The project running from September 2011 till May 2013 receives funding from the German Federal Ministry of Education and Research (Bundesministerium für Bildung und Forschung, BMBF). Various associated partners further contribute on a voluntary basis.

* The full name is "Angriffsanalyse und Schutzkonzepte für MObilfunkbasierte Netzinfrastrukturen unterstützt durch kooperativen InformationsAustausch" (Attack analysis and security concepts for mobile network infrastructures, supported by collaborative information exchange).

Partners:

Cassidian / EADS Deutschland GmbH

ERNW Enno Rey Netzwerke GmbH

Fraunhofer Research Institution for Applied and Integrated Security (AISEC)

Hochschule Augsburg

Nokia Siemens Networks Management International GmbH

RWTH Aachen

Associated Partners:

Federal Agency for Digital Radio of Security Authorities and Organizations (BDBOS)

Federal Office for Information Security (BSI)

Deutsche Telecom AG (DTAG)

For more details about the project please visit www.asmonia.de.

Executive Summary

This document presents the summary of the various validations of ASMONIA project results, encompassing the evaluation of

- the collaborative security concepts, including the implementation of these concepts as a prototype,
- the evaluation of integrity protection measures for nodes and devices in 4G networks,
- the evaluation of the flexible provisioning of cloud-based resources to mitigate overload situations, including the demonstration implementation,
- the evaluation of continuous security monitoring measures and an adapted model for economics analysis,
- the simulation based evaluations by mean of mobile and fixed network models, network elements and regular and malicious traffic models incl. effects of spreading malware, and
- the penetration testing to assess vulnerabilities of in particular Proxy Mobile IPv6 used in 4G networks.

This presentation is concluded with an overall summary of the project and suggestions for further work.

Table of Contents

1 Evaluation Activities carried out as Part of the Work Packages 1-4

The purpose of this section is to give an overview of the various evaluation activities carried out as part of the WPs 1 to 4 of the ASMONIA project to evaluate the methods developed in these WPs.

1.1 Evaluation for WP1: Comprehensive and Collaborative Security Concepts

Supporting a holistic approach that comprehensively addresses the future threats on mobile communication systems, a collaborative approach is followed by the ASMONIA project. The basic paradigm behind this approach is that collaboration has for participating parties the potential to improve awareness about upcoming security risks and help mitigating the security threats. It was expected that MNO are reluctant to support each other mutually or give information to authorities. First of all this hesitation is based in the expected risk of reputation loss.

The project contributions address this situation: A collaboration method that is free of the reputation risk for the participating MNOs and an overall system design [ASMONIA_D1.1]

which is cognizant of the technical system for mobile communication systems. The latter encompasses the ASMONIA Collaboration Network (ACN) that links the different site of participating MNOs via identified interfaces to basically support the communication of sensors and counter measures – in the widest sense – in access networks, the core network and on mobiles. For these project contributions there were not dedicated evaluations, though the project made some findings, for example, about the UEs in the field, protection schemes, the use of cloud technology etc., discussed further below.

As expected, the proposed collaboration method [ASMONIA_D1.2] was more thoroughly evaluated, compared to the architecture. Concerning the method's design there was no need seen for the earlier on suggested P2P Overlay Network, as the selected MPC solution connects sites full meshed. The design of the collaboration method with a focus on MPC and TAC has been evaluated. The evaluation result is that MPC and TAC complement each other effectively such that the data protection and privacy requirements are fulfilled that make the collaboration methods suitable for a reputation risk free solutions.

This design was eventually implemented as a prototype to demonstrate and evaluate the collaborative method and suggest improvements [ASMONIA_D4.3], [THS2013]. The evaluation focused on size of exchanged warnings; the improvement concerns its protocol algorithm. These investigations were complemented by an additional evaluation in a simulated attack scenario the collaborative method is considered to be operated in [HSTS2013].

Last not least some discussions address the effort and the expected positive effect of the approach the project is following [ASMONIA_D1.4] on the level of an individual MNO as well as in national macro economical scope. The latter is probably of limited impact and should be understood as an early attempt to sketch the contribution for the protection of Critical Information Infrastructure, as there is very little suitable information for such an assessment.

1.2 Evaluation for WP2: Integrity Protection for Nodes and Devices in 4G Networks

The integrity protection and malware detection methods elaborated in work package 2 are described in [ASMONIA_D2.2]. Their effectiveness and fields of application have been reevaluated, reconsidering strengths, weaknesses, remaining risks and trade-offs for implementation.

To evaluate the developed methods regarding malware detection on smart-phones, two scenarios have been used (Detecting Rebundled Malware and Broadening the Model) and also bypass strategies have been considered (Evasion). To shortly summarize, it has been stated that by enriching the model with semantic information of system calls mimicry attacks can be countered (wrt. evasion). Broadening models (monitoring several application in same model) for malware detection lead to higher rate of false positives (lowering the detection rate), but re-bundled malware can be detected in reliable manner.

To evaluate SW-IP methods for NE (as well as the extensions implied for the security infrastructure), the initial requirements have been reconsidered and compared against the elaborated protection mechanisms. It has been examined, to which extend the integrity protection methods fulfill the expectations, taking impacts of different implementations and residual risks into account. Typical trade-offs have been identified, showing that in many situations 'solution finding' needs to balance technical security deliberations with economic effects, system evolution, and feature planning. In one specific case the re-evaluation also detected an insufficiently described method, which now has been completed.

Detailed results of the re-evaluation are described in [ASMONIA_D2.2], Sections 5.4.3 and 5.4.4 (specifically on UE centric malware detection) and in [ASMONIA_D2.3], Section 5 (on Integrity protection for UE and NE).

1.3 Evaluation for WP3: Incorporation of Cloud Systems into the Security Concept

The ASMONIA Collaborative Cloud Architecture denotes the main contribution of WP3 to the ASMONIA project. While most of the effort of WP3 has been spent in order to define the architecture – first the requirements for the use of cloud systems needed to be described and then a corresponding design of the architecture – considerable effort has also been spent in order to evaluate the architecture.

One part of the evaluation effort is the design and implementation of a demonstrator [ASMONIA_D3.3] that incorporates some main features of the ASMONIA Collaborative Cloud Architecture. Implementing the complete architecture was out of scope of the project. From the implementation of the demonstrator we were able to deduce the feasibility of the concept and encounter some practical limitations of it.

The second part considers the evaluation efforts of WP3 regarding the evaluation of cloud mechanisms for data correlation and overload situation based on Intercloud demonstrator as they are described in [ASMONIA_D3.4]. For this it deals with a design security review where the design of the Intercloud demonstrator was reviewed and assessed. Elastic systems/Cloud computing environments are not a strictly defined term or technology and mostly Industry-based origin leads to a lack of standardizations or clear terminology in the domain of Intercloud processes. To get a better understanding of the principles and necessities of cloud networking a design security review was carried out. Additionally it presents the obtained results of the Intercloud demonstrator which are used of a simulation based validation. The goal of the simulation was the validation of the principles of Intercloud networking regarding an extended amount of data exchange between the collaborative clouds and by using different provider distribution methods as well as reduced availability caused by bandwidth limitations.

1.4 Evaluation for WP4: Methodologies for Detection and Presentation of Security Risks

The developed capability set Continuous Security Risk Reduction presents an evolutionary, quantitative approach to enable transparency of the risk and security posture of critical information infrastructures like a mobile telecommunication network. The resulting enterprise architecture for Continuous Security Monitoring, Continuous Security Model Adaptation and Continuous Security Economics Analysis, elaborated in [ASMONIA_D4.1i] and [ASMONIA_D4.1ii], in addition with architecture enhancements for Continuous Security Awareness and Continuous Security Collaboration, developed in [ASMONIA_D4.2], are evaluated and discussed in [ASMONIA_D4.2]. Section 6.2 examines the achieved results and perspectives for networked systems as well as their relevance for technical, economical, regulative and social environments.

2 Evaluation Activities Carried out in Work Package 5

2.1 Evaluation based on Network Simulation

2.1.1 Scope

Experimental cyber security research is in many cases inherently risky. An experiment may involve releasing live malware, operating a botnet, or generate highly risks to the experimental infrastructure as well as the Internet. Infrastructure based experiments are fundamental for a successful research. Data privacy laws forbid or make such investigations more difficult. The evaluation of a test bed with real components for such investigations is hardly feasible because of the high costs. Our work was to increase the scope and usefulness of test bed-based experimental cyber security research by the use of simulation and to generate data for further processing from this test-bed. This evaluation report covers attack scenarios, considers further project results and gives recommendations for further measures and improvements.

2.1.2 Introduction to Simulation

This part is about simulation. However, that statement is not as simple as it may first seem.

> *"Simulation has aspects in common with both theory and experiment. It is fundamentally theoretical, in that it starts with a theoretical model, typically a set of mathematical equations. A powerful simulation capability breathes new life into theory by creating a demand for improvements in mathematical models. Simulation is also fundamentally experimental, in that upon constructing and implementing a model, one observes the transformation of inputs (or controls) to outputs (or observables)." [US_DoE]*

The use of simulation was a novel approach onto the domain of cyber-security. The availability of high fidelity simulation models, the availability of sophisticated simulation tools and high performance computer technology as well as the non-availability of sufficient information and data from real networks caused us to take this path. The bridge between physical reality and computer simulations of physical reality are logical or mathematical models, expressed as sequential process or in terms of a system of equations and based on scientific understanding of the problem being investigated. To bring in such models, four steps had to be applied in order to produce and use computer simulations.

1. ***Model Analysis* -** All components of a cellular network had to be taken into account. A well-defined simulation model of a communication network had to stand on its own as an internally consistent network structure for its computer representation. For that reason, it was necessary to resolve a number of issues regarding the model structure:
   - Did the models consider the functionality of the real physical elements?
   - Did they act, react and interact in the same manner as real systems?
   - Did the 'simplifications' of a model have any impact on the simulation results?

2. ***Approximation and Discretization* -** Simulation models can either be described by state machines, as sequential process or as a mathematical transfer function. In order to represent it on a computer it was necessary to approximate the behavioural response of a real element by a finite number of sampling points in the simulation model. The mathematical issues for this process, called "discretization," include the

extent to which the finite approximation better agrees with the desired behaviour function and the relationship between the choice of approximation and qualitative properties of the solution.

3. ***Model Building*** **-** Once one had defined the physical environment by its network structure, the elements and the traffic model, the behaviour of this network model in best use of the computational resources could be estimated. Issues at this stage include the application of optimally efficient algorithms, and the mapping of computations onto a complex hierarchy of processors and memory systems. Available models are perfect for performance tests on planned or existing network structures but don't fulfil all requirements regarding cyber security applications. This is the reason why not every status- or health-parameter of a real network element is available in the simulation model. Extended models, considering a number of 'useful side-effects', are possible but time-consuming and can extend the duration of a simulation from hours to days. The well-known network-status parameters have been selected from all available possibilities.

4. ***Traffic Modeling*** **-** For the representation of network performance figures and diagrams and furthermore to carry out "what-if" analyses, a network modeling tool requires defined traffic patterns, flows and network architectures. Usually modelers do not deal with real traffic; no packets flow through a modeler. When this paper mentions 'simulation' this means 'modeling' as explained above. Getting meaningful results from a simulation means an amount of preparatory work which had to be carried out to prepare the traffic model. This preparation involved steps such as defining exactly what is wanted and clearing up any ambiguities or uncertainties in the definition of the model. Our intention was to evaluate traffic models of 'DDoS-attacks' because one focus of ASMONIA lies on the detection of cyber-attacks already in their initial phase and to develop measures against such attacks. In the Traffic modeling process we had to consider available resources. The required simulation time and the amount of memory for a simulation experiment were rising rapidly with the complexity of the traffic model. For this reason some restrictions were necessary. Simulation models of communication network components are not exact images of real systems. Commonly they are implemented as behaviour models, as 'black-boxes' showing the same behaviour but applying different mechanisms. The reason is to save calculation time and to improve the performance. Real time simulation is not practicable for realistic scenarios with high active numbers of UEs. Simulation results are recorded and marked comparable by time stamps for later analysis or usage.

2.1.3 Network Simulation Model

Purpose of simulation was the implementation and the adjustment of defined test networks for verification and test purposes. Defined models for the network data traffic have been used to run tests in this simulated environment. One expected result was the identification of dynamic network behaviour patterns from these data records for use in early warning systems.

2.1.3.1 Architecture

A 4G (LTE) model consisting of three separate provider networks, a number of mobile users (UE) each connected to one of the providers and the required infrastructure like backbone networks, servers, firewalls and routers as usual in wide area networks including the internet, were the basis for the applied investigations as described in [ASMONIA_D5.2]. The simulated network architecture was used for collecting status data from simulated network elements for further analysis.

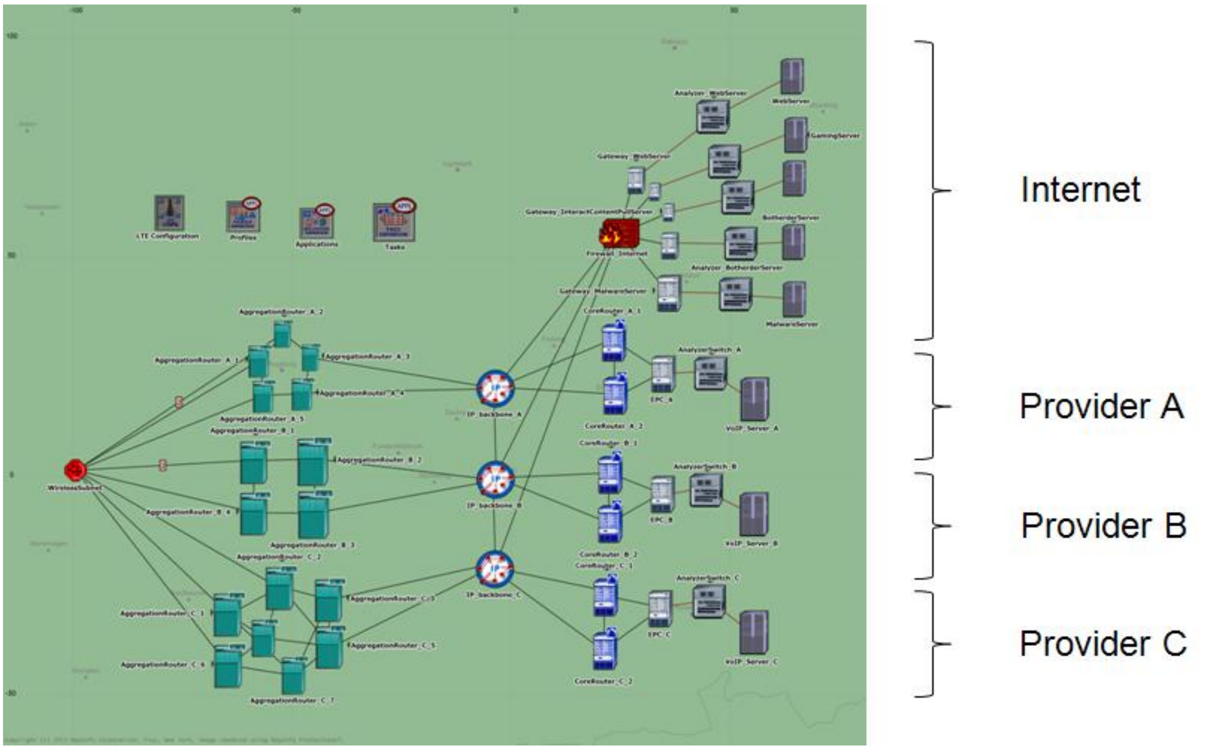

Figure 2-1: Architecture of the simulated network

2.1.3.2 Stimuli

For a further data evaluation it is important that all collected statistics data are reproducible and comparable within a certain time period. To ensure that every data value of a record can be compared against other values, the whole simulated time was set to one hour and statistics values had been be tapped from considered network elements every second. This process was modeled on the usual network management standards for collecting network status data by use of SNMP.

2.1.3.2.1 Modifications

Based on the ongoing investigations there were made some modifications regarding [ASMONIA_D5.2]. Instead of using a collection of assumed traffic patterns based on E-Mail and HTTP, a preconfigured traffic set based on 3GPP technical report [TR36.822] was used for the regular traffic pattern. This report includes measured and analyzed values from real mobile networks and represents different user behavior such as mobile user with background load, gaming profile and the communication with an app store.

This traffic pattern for mobile users was basically provided in OPNET. It takes all the aspects of mobile applications into account and was introduced meanwhile the project was running. Advantage of using such a predefined implemented data set is to reduce the simulation run-time heavily while the generated results are more realistic because they depend on measured and analyzed values from live networks.

The second modification regards to the irregular traffic. This traffic pattern was developed and implemented directly in OPNET Modeler and take the rules for the irregular traffic into account as described in the next section.

2.1.4 Implementation

To run a cyber-attack on a simulated network with the purpose to collect data about the network status, a data set was prepared representing the above outlined tasks (the network element's behavior during normal conditions and during the attack) for each UE. Every UE got its specific user profile (time, duration and kind of communication) and additionally three profiles for the attack case, describing the start time, the kind of communication and the data volume to be transmitted and received during a specified time (the start of each transmission was calculated by the malware distribution behavior model).

As a result two data records were generated; each of them represents the recorded behavior of all observed network elements in the scenario. In a following process both records can be analyzed for the detection of typical behavior patterns from specific network elements, or a group of them, for the early detection of cyber-attacks.

2.1.4.1 Assumptions

It was assumed that all services are coequal to reduce the complexity and to avoid limitations or 'tampering' of the results. Section 2.1.4.2 describes the distribution behaviour of the considered malware, the preparation for the attack, what the attack shall do. In a Denial of Service (DoS) attack, the attacker sends a stream of requests for a service to the server expecting to exhaust its resources like 'memory' or to consume all processor capacity. In Distributed DoS (DDoS) attack, a 'hacker' installs a network of bots or daemons on a number of hosts (malware distribution phase) and also a bot-herder, probably a captured server in the Internet, which has control about this botnet.

It was assumed that a bot-herder controls all registered bots and they execute the attack. DDoS-attacks are harder to combat because blocking a single IP address or network will not stop them. In real networks the attack traffic can derive from hundred or even thousands of individual systems and sometimes the users are not even aware that their computers are part of the attack. In the simulation the number was reduced to only 250 attacking units (caused by limited resources) and the remaining infrastructure was adapted to this by a performance reduction for the included network elements. The attack traffic model follows the principles of such attacks in a simplified form. Each active UE sent a defined amount of data (packets) to a victim server under attack.

2.1.4.2 Malware Model

Section 3.2 of [ASMONIA_D5.2] explains the distribution mechanism for the considered malware model. During the implementation and test phase we learned that increasing complexity of the traffic model causes increasing simulation time and lack of memory space. A reduction of the number of mobile users to 250 UEs (D5.2 calculated with 5000) and a reduction the observation time down to 1 hour (D5.2 considered 26 hours) gave the best compromise for the simulation. This had impact on the settings for the malware distribution behavior calculation as well (see Table 2-1).

Table 2-1: Model Parameters

```
Input Parameters for the Model:

numberOfPart = 250;
clusters = 3;
variance = 0.20;
groupPerCellMin=10;
groupPerCellMax=50;
minAdBook=5;
maxAdbook=20;
maxThreatDelay = 10;
statWeight = 0.8;
```

The final traffic model considered 250 UEs, sub-divided into 3 separated provider networks of differing size. Each provider network included between 10 and 50 communities (groups of participants with similar interests) and each UE owned a specific address book consisting of 5 to 20 entries. This address book defined the communication relations within the network. The number range for each network is shown in Table 2-2.

Table 2-2: Estimated Cluster size

```
Resulting cluster size (random process):

clusterLimits = {1,100} {101,175} {176,250};
```

Provider network 1 included the addresses from 1 to 100, network 2 the addresses from 101 to 175 and network 3 the addresses from 176 to 250. Each address was related to a specific IP-address.

The modifications had also impact on the distribution process:

Figure 2-2 shows the resulting behavior: the left part of the diagram represents the distribution of the information by use of a malicious application which causes the (unwanted) infection after being downloaded (number of infected UEs). Because of the low number of considered UEs a nearby 100% infection was the result.

The second curve represents the number of infected UEs (y-axis) ready to start an attack (considering the fact that not in every case the infection starts immediately after getting the information).

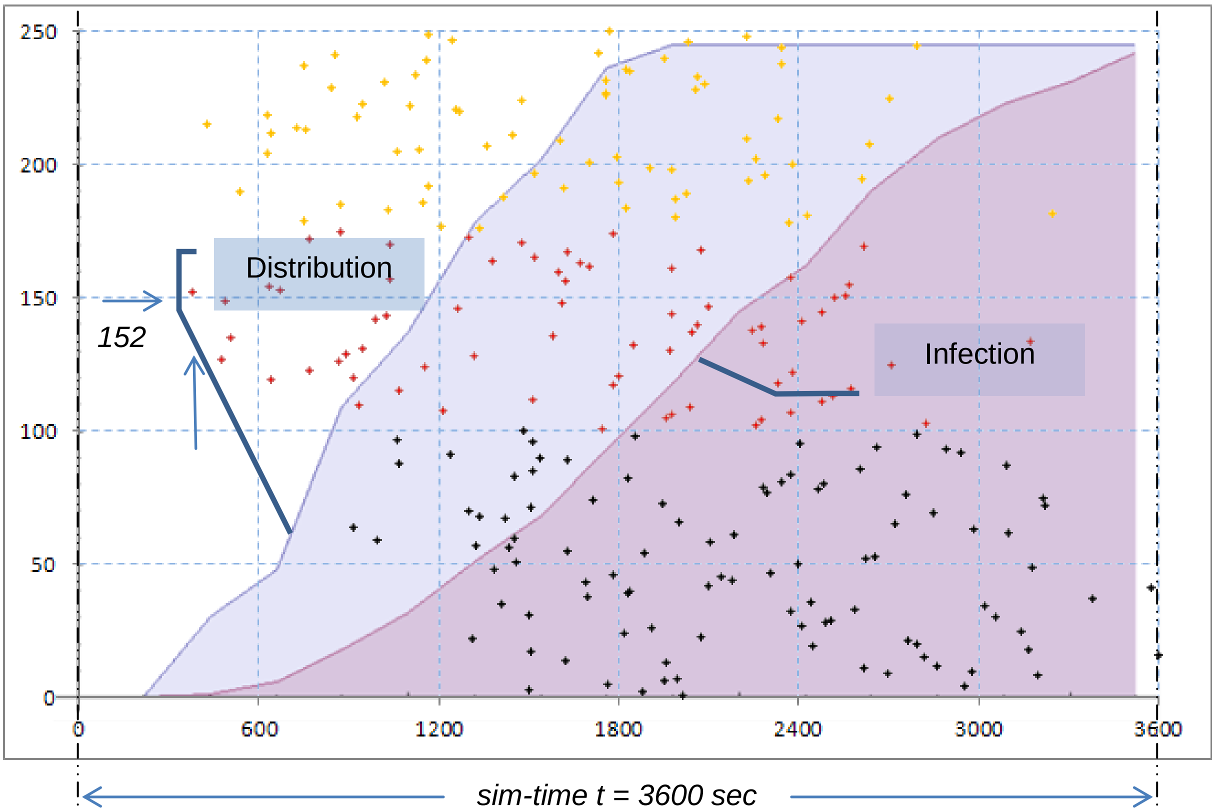

Figure 2-2: Malware distribution behavior for the considered model

The right of both curves of Figure 2-2 represents the infection behavior and shows the resulting number of infected UEs. Because not only the absolute number of infections was of interest, each of these UEs was represented by a dot to give more detailed information. The color of a dot (black, red, yellow) shows the membership to a provider (black = provider 1, red = provider 2, yellow = provider 3) and the resulting affiliated IP-address range for the simulation from this. The vertical axis represents the number (address) of an UE and the horizontal axis marks the time when this UE got infected and was ready to carry out the attack. The infection started from UE 152 and the resulting course of the infection and the spreading to neighbored provider networks is shown in Figure 2-4. An assumption in the distribution model was an initial communication sequence between UE and bot-herder. The infected UE announced itself to the bot-herder by sending a message to its address.

Figure 2-4 represents the graph for this distribution process and also the dependencies and the information flow for each UE. The vertical axis defines the address of an UE (1 to 250) and the horizontal axis shows the path and number of cycles necessary to get the information from the initial address. The graph shows the maximum number of steps to distribute the whole information to all reachable UEs. The process was ending after saturation. Either all elements had been contacted or the distribution chain to several UEs was interrupted due to the address book structure. This graph provides also information about the infection chain and the change-over from one provider to another provider network.

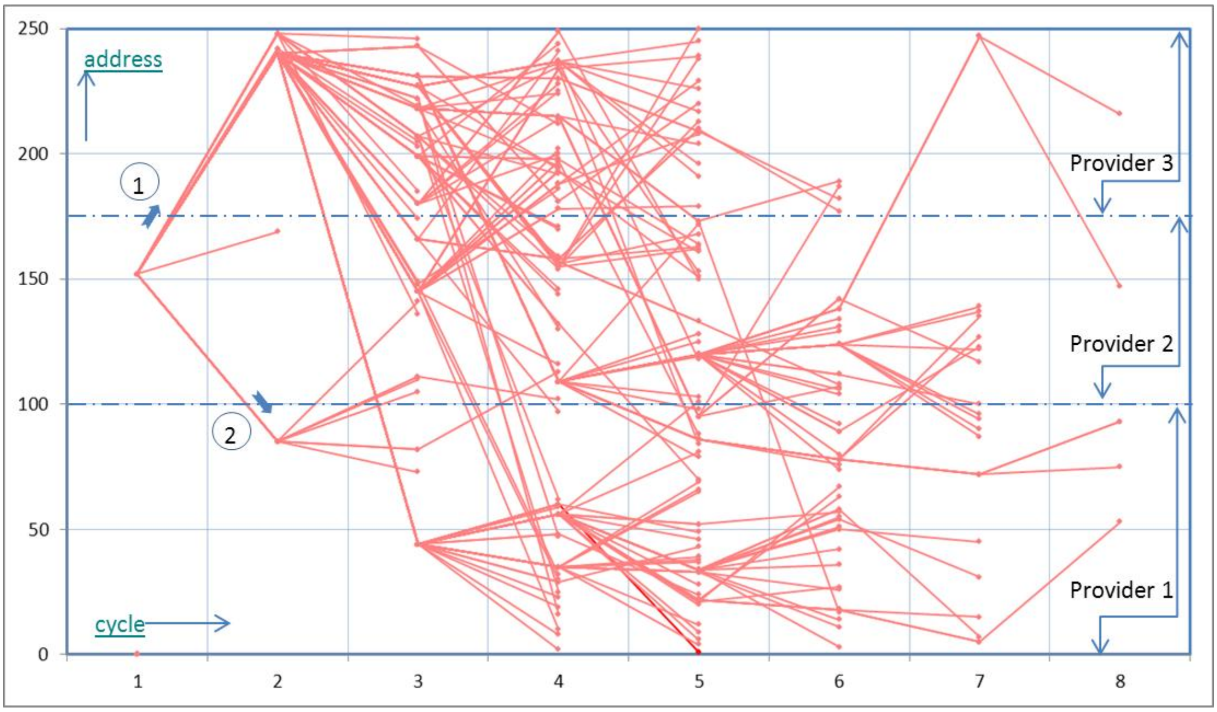

Figure 2-3: Distribution Flow

The distribution process was started in provider network 2 but was spread early to the networks 1 and 3 (markers 1 and 2); the distribution for the infection occurred mainly in network 3. It was shown that, in a later stage of the infection process, the number of infected UEs in network 2 and in network 1 also increased. This illustrated the dependencies between the network users and refers to a possible benefit of cooperative networking by information exchange and the use of the additional information to prevent the attacks.

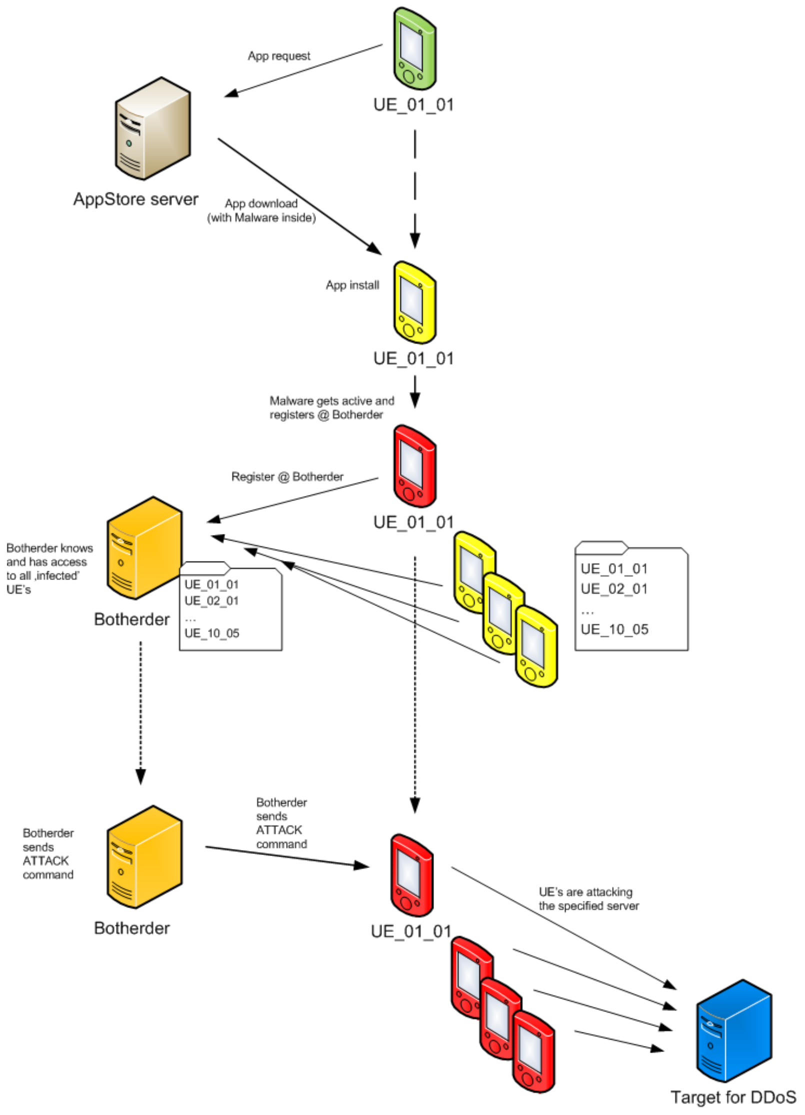

Figure 2-4: Principle of the Malware Distribution Model

Figure 2-4 illustrates the principle related to [AndroidBmaster]:

- An UE, after getting the information (the left curve in Figure 2-2), was sending a request for the download of an (malicious) application to the application server.
- The application-download started from the server and caused a certain amount of data (the same for each UE in case of download).
- When the application got active after being installed, the infection started with the registering of the infected device to the bot-herder (the right curve in Figure 2-2).
- From this the bot-herder had access to all registered UEs for executing the attack.

The distribution model for the information phase (the distribution of the message where to get an application) was relation-based and the relations had been described by the contents of the address book of each UE.

2.1.4.3 Malware Model Implementation

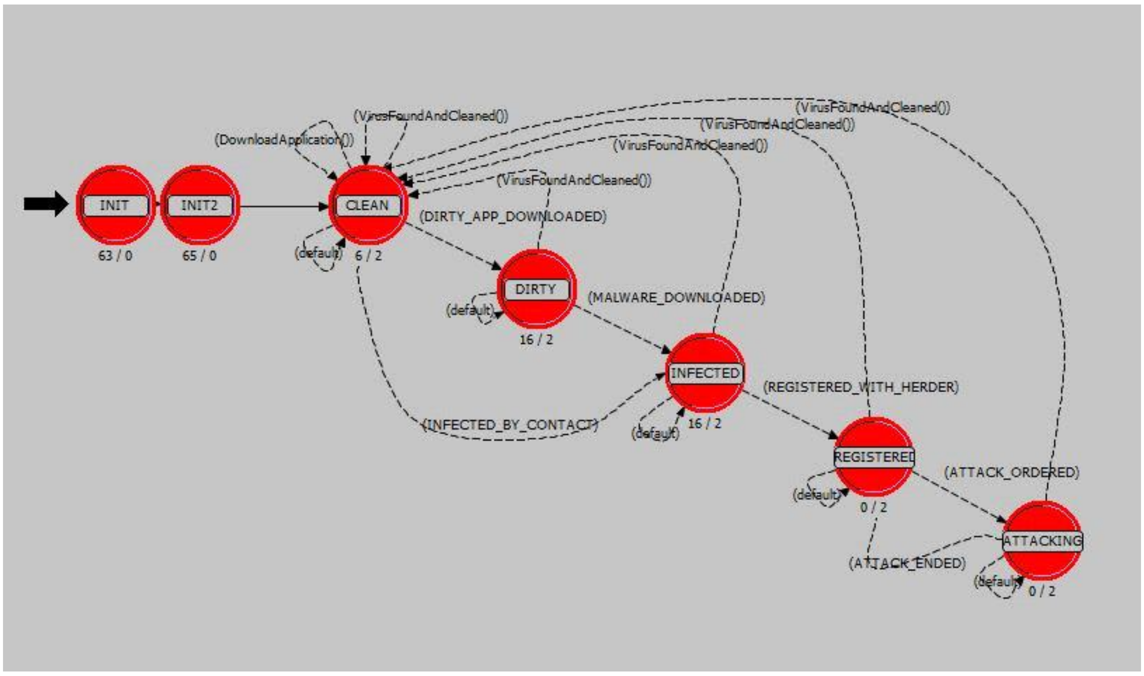

Figure 2-5: Implemented Client Model with Attacker Behavior

Figure 2-5 shows the implemented attacker model. This model was derived from the standard client model. A number of specific actions had been added:

- Malicious application downloads (DIRTY_APP_DOWNLOADED)

  The first step in the infection chain; a malicious APP is downloaded

- Malware downloads (MALWARE_DOWNLOADED)

  The download of the malware starts; alternatively the malware was received directly

- Registering with bot herder (REGISTER_WITH_HERDER)

  The infected client is known by the bot herder and ready to carry out attacks

- Attack order (ATTACK_ORDERED)

  The attack starts/is stopped after receiving specific information

The model is based on the principle described in chapter 2.1.3.2 and ensures an individual behavior for each client. For further investigations this model enables also the analysis of countermeasure mechanisms.

2.1.4.4 Data Analysis

To set up and run a network simulation for data generation within OPNET Modeler the considered network had to be configured in terms of network nodes, links, routing protocols and data transmissions. Because the considered network model represents a compound of three separated network providers, the relation between an UE and its network provider is given by the unambiguous network address of this UE. This address is also necessary for further automated data processing and for parsing purposes. The correct functions of the implemented network model was tested with simulated ‘pings’ sent from selected UEs to defined destinations. Once the network simulation was set up correctly with the right assumptions, the scenario was executed in OPNET Modeler. After ensuring the full desired functionality the simulation model was ready for the data collection process. In a second step the correct function and settings had been tested with a basic traffic model. The resulting records from these early tests have been used as a first test data set for use in the data mining process. In this step also the necessary data exchange format for this process was determined.

2.1.4.4.1 Statistical Data

Result of this network simulation was a number of time-based statistics for the overall network performance. These statistics are represented as a vector and each of them contains a series of abscissa-ordinated entries. The abscissa generally represents the simulation time and the ordinate the corresponding value regarding the probed data sources (i.e. network node) and their functionalities.

The following listed statistics are only an excerpt from the simulation results. In general all available statistics [OpnetModelerLibrary] can be separated into three groups:

- Node statistics
- Link statistics
- Demand statistics

Node statistics represent collected network performance data for individual nodes. These records are specifically defined per node and offer the analysis of protocol-based statistics such as the amount of IP-traffic, sent or received data by a specific protocol or node.

Link statistics records contain status information regarding the network links, for example the utilization or the throughput of a point-to-point link, as depicted in Figure 2-6. Link utilization is a parameter which represents the ‘bandwidth usage’ percentage of a transmission line and is a measure for the ‘economy’. A low utilization means ‘waste of money’ and congestion by overload downsizes the performance of the whole network (loss of money).

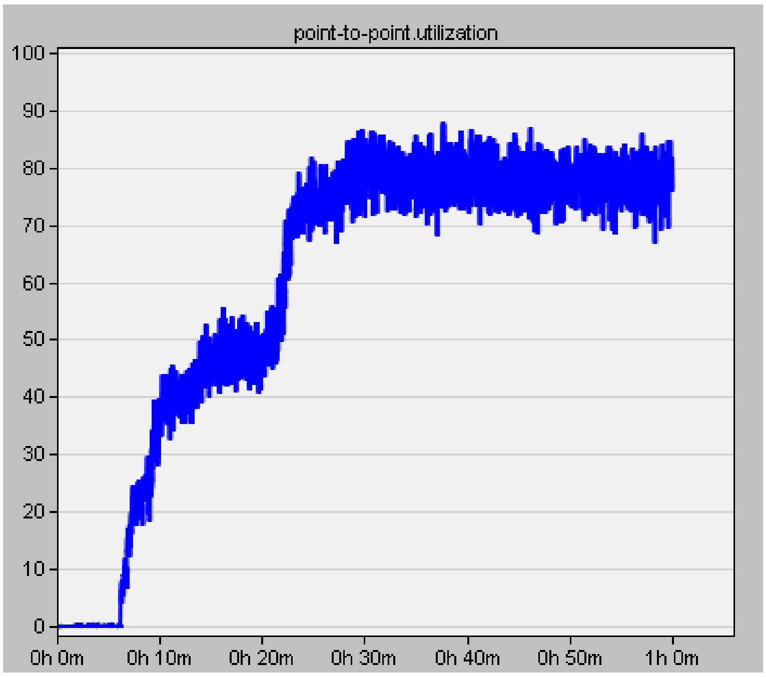

Figure 2-6: Link Utilization Statistics

Demand statistics collect information about point-to-point application demands. As an example, packet end-to-end delay was recorded as well as the amount of data traffic. These statistics help to analyze IT demand across entire applications and services. It shows that all IT is working and how all resources are contributing.

Another important data source is the specific application behavior of a modeled server. This is, for example, the behavior of an application server regarding the amount of data which was interchanged with the server, as well as the task processing time which means how much time the server requires to process a request. This was used to verify that the server can handle the amount of data, and that the server was running into an overload situation.

2.1.5 Results

Comparing both scenarios showed that the influence of the cyber-attack was clearly visible. As expected, all nodes showed a regular behavior which was represented by their quality indicators and transmitted data. This could be seen at first by a comparison of the data throughputs in both scenarios. Especially within the LTE domain the simulation allowed us to get also physical measurement indicators as well. Figure 2-7 (top) depicts the upload utilization of one considered eNodeB under attack as well as under regular conditions (below). These measurement results belonged only to one specific provider. The consequence of link saturation was a limited service in this provider network. For network subscribers this could cause the non-availability for certain services and by this lead to a customer dissatisfaction regarding the services. The results should not only satisfy technical interests, moreover they should be useable as a basis for the determination of the user satisfaction for certain services. High link utilization had also impact on further service quality limitations.

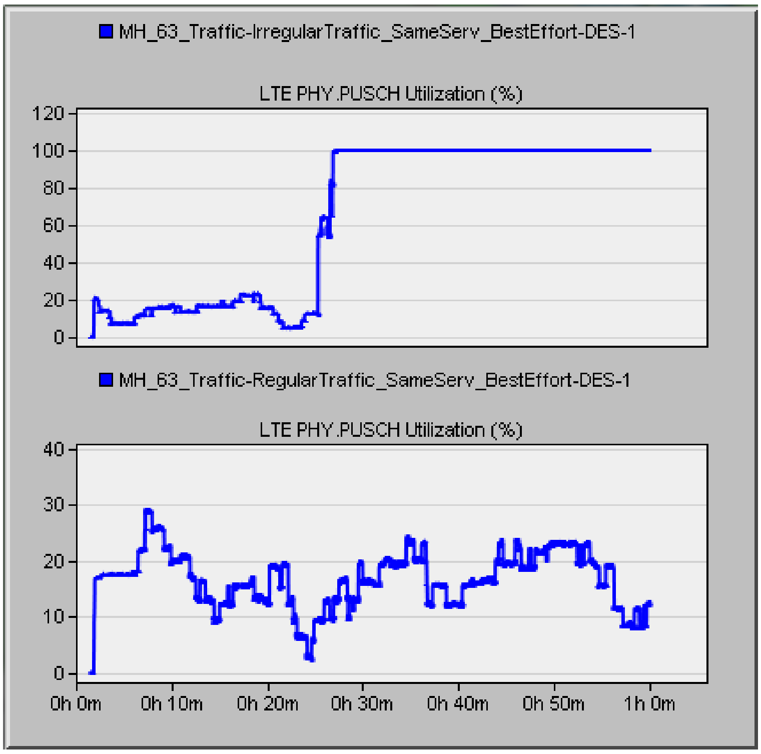

Figure 2-7: Physical Uplink Shared Channel Utilization at eNodeB_01 for both compared scenarios

One of the indicators for quality-of-service and user satisfaction is the end-to-end delay per user, in this meaning the packet delay between transmitting and receiving node. It was clearly visible that the influence of the attack caused a very high packet delay (up to ~18 seconds), compared to the regular scenario (~120 milliseconds). This is depicted in Figure 2-8. The impact of end-to-end delay is especially recognizable in the domain of voice communication.

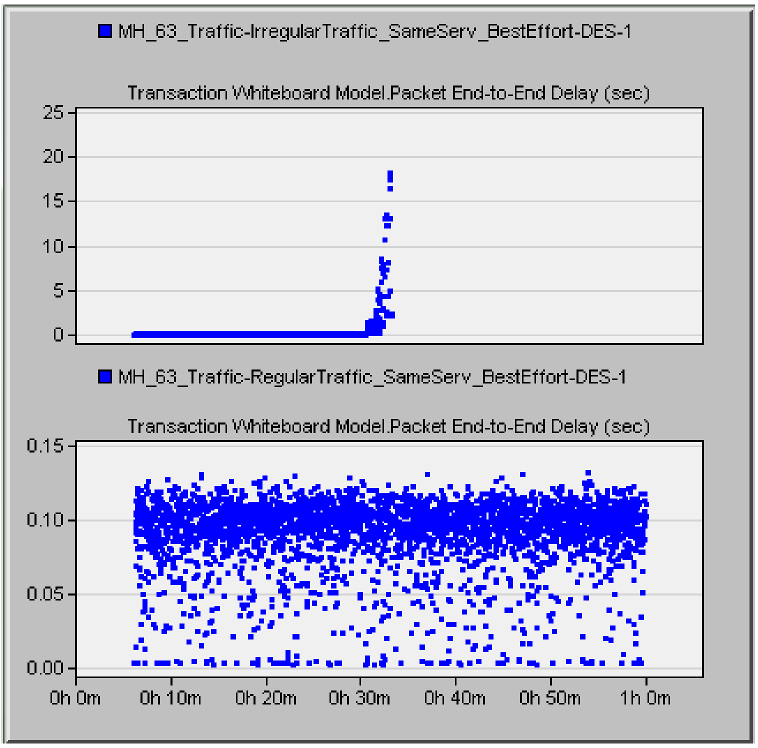

Figure 2-8: End-to-End Delay for UE_01_10 for both compared scenarios

The end-to-end delay for voice-over-IP packets visualized in Figure 2-9 represents the average delay for the top 10 UEs (the most critical subscribers) in the simulated scenario during regular conditions. The constant delay of ~120 milliseconds ensured high quality and low packet latency in case of VoIP communication. In contrast Figure 2-10 represents the top 10 UEs under attack conditions. Increasing packet delay (up to 50 seconds) caused by high link utilization lead to high delays and finally to the impossibility of voice communication by the high delays. The attack had a huge influence on the quality of voice communication.

We had to select specific parameters and statistics to have a relation between technical performance and user satisfaction. The result was a number of (time-depending) correlating results taken from network elements regarding traffic loads and delays, and the UE-specific end-to-end delay as already mentioned for the transmission of voice packets and its impact on service quality. From each simulation run we had generated a number of data sets including information about the status of the network elements regarding provider specific service quality.

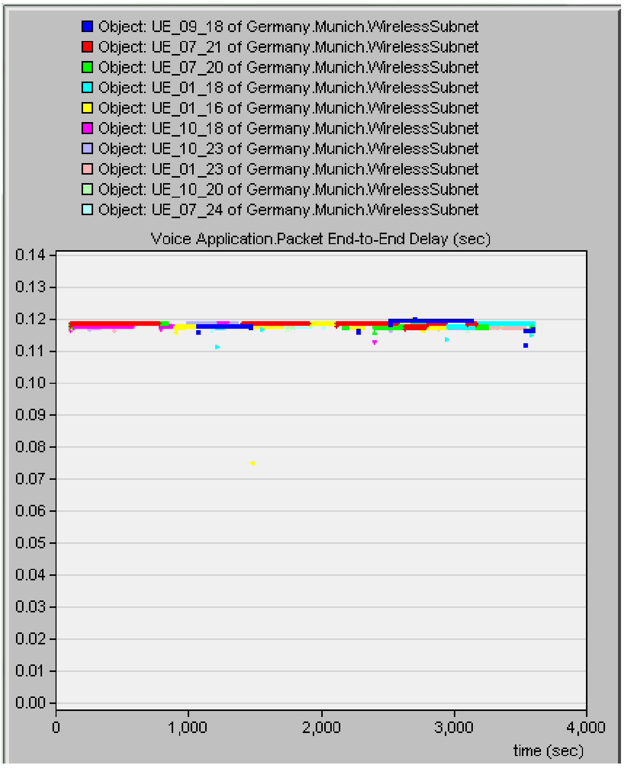

Figure 2-9: Voice Packet End-to-End Delay for Regular Traffic Scenario

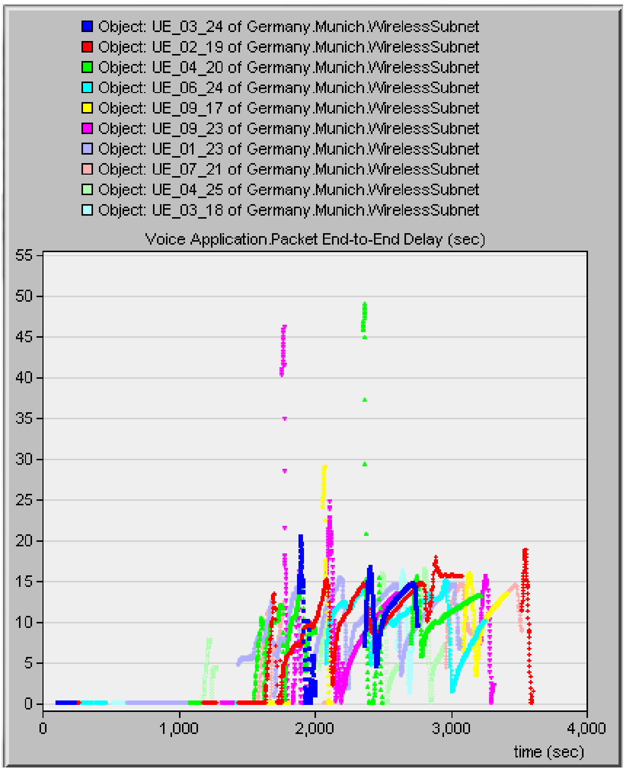

Figure 2-10: Voice Packet End-to-End Delay for an Irregular Traffic Scenario

A technical network simulation allows us to generate and collect data for the discovery of relationships between measurements and stimuli. A mobile telecommunication network as part of a critical infrastructure relates directly to the value provided by the services. Analytical records supplemented by measurements taken from network elements may be a suitable methodology for gathering relevant information about the service indication for the UEs. During a network simulation run status-information records were collected from different network elements. In parallel the quality for the end-to-end transmission between UE and the required service was recorded (UE to UE, UE to server etc.). In a comparative process we investigated if the quality of service could be estimated from available status information. For analysis purposes we separated the data results regarding their relation to consumed or provided services.

2.1.6 Conclusion

Our work demonstrates that simulation represents a suitable instrument for investigative experiments in the cyber domain. The base is a careful planning of such simulation scenarios and the exact definition of the applied models and parameters, taking into account the given limitations. An extension of the presented methods and concepts and an improvement of the applied models are possible and applicable in a wide range.

In our simulation experiments we used all available status information gathered from the systems in a communications network. The comparability of the results generated in the simulation, and their reproducibility made it possible to supply data for statistic processing.

The resulting data were subdivided relating the two types of elements (agents and services) to match the model as outlined in D4.2.

Agents

- Agents which use (consume) provided network services corresponding to
    - Mobile users, represented by UEs and their behavior.
- Agents which provide network services corresponding to
    - Network operators providing consumable services, represented by a subset of the network elements, required for the considered services, e.g. backbone.

Services

- Services which are used (consumed) or generated (provided) by agents. Agents may consume services like 'voice' or 'data' provided by technical infrastructure of network operators. In this network simulation these services were generated and used by simulated network elements.

Our intention was the provision of data which enabled the connection between these agents and their services. The time-based data correlation allowed the processing of those data sets in a following data mining process. The obtained simulation results should give information whether an overall co-operation of network providers represents an effective method for the protection against cyber-attacks, with consideration of the impact on the assumed commercial profit.

2.2 Evaluation of Risk Assessments by Pentesting

The necessity of penetration testing comes up with the acceptance of risk, compliance, and elimination of vulnerabilities as described in several international standards and is one of the main factors in a vulnerability management process. The risk acceptance process furthermore is regulated by governments (e.g. KonTraG, Germany) and must be identified and documented in corporate environments, including telecommunication provider.
For identification and documentation of these risks the method of penetration testing is a reasonable method, assisted by a risk scoring and rating system.

This necessity also arrive the telecommunication industry in using IP technologies, caused by becoming more and more important due to a higher publicity and therefore being more in focus of attackers.

2.2.1 Introduction

Proxy Mobile IPv6 (PMIPv6) is based on the Mobile IPv6 (MIPv6) protocol. It is a Network-based mobility management protocol which has some major advantages to the former MIPv6 specification. The difference to MIPv6 is that the end-user doesn't need to participate in any mobility-related signaling procedures. Instead the mobility entities in the network take care of tracking the host movement and perform the required mobility signaling on its behalf. The basic idea is to let the mobile nodes take their IP with them into any mobile network (or any other non-3GPP network) that is connected to the access link of a mobile entity that is part of a PMIPv6 environment.

According to the acceptance of risk, several telecommunication components were analyzed and evaluated in [ASMONIA_D5.1]. In this context, several penetration tests were performed and described, supporting the performed risk assessment.

In addition of the protocol analysis in [ASMONIA_D5.1], this document covers the analysis of Proxy Mobile IPv6 (PMIPv6). PMIPv6 is a protocol, supported by gateway nodes, providing a mobile IP implementation to the customer, without the need of support by the client itself. Because PMIPv6 may be an additional technology used in provider networks, a protocol analysis was performed. On the one hand the following chapters will describe a theoretical analysis of the protocol, and on the other hand the results of a penetration test of a PMIPv6 implementation.

2.2.2 General

Proxy Mobile IPv6 (PMIPv6) is specified in [RFC5213] and uses the terms of Mobile IPv6 (MIPv6) which is defined in [RFC3775] and from the Goals for Network-Based Localized Mobility Management [RFC4831]. The goal of PMIPv6 is to get an access technology and joint protocol which is independent no matter what mobile core network technologies are in used. One of the main functionality is to enable IP-layer mobility for all clients whether they support MIPv6 functionality or not. This means that the mobility agents in the network take care of the client's movement and its mobility signaling.
The client whose mobility is managed by the mobility entities in the network is called Mobile Node (MN). The main components in a PMIPv6 network are the Mobile Access Gateway (MAG) and the Local Mobility Anchor (LMA) which is equivalent to the Home Agent of MIPv6.

The allocated role of the MAG is to manage the mobile-related signaling on behalf of the connected MN. An important functionality of the MAG is that an attached MN notices no difference between the different MAGs as if it is connected directly to its home network. It receives all IP-layer related information for the corresponding MN. As the MN moves from one MAG to another, it shall receive the same IP information from the new MAG as it received from the ancient one. The MAG also instructs the LMAs that are assigned to it in the PMIPv6 domain about attaching or detaching MNs. The MAG is thereby the link between the MN and its home agent.

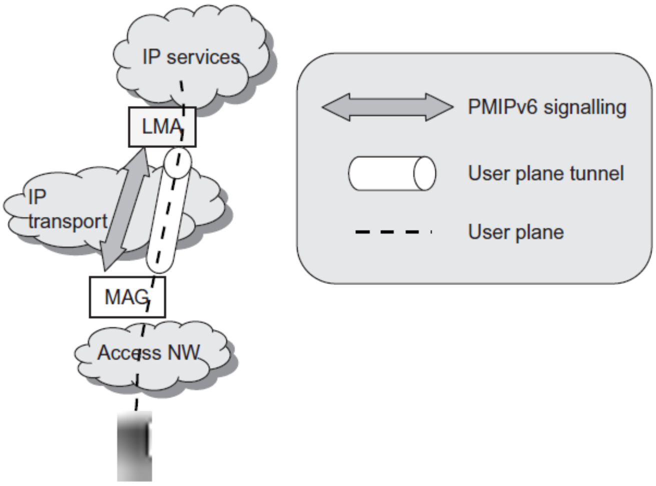

Figure 2-11 Proxy Mobile IP [SAEEPC09]

The LMA takes care of the home network prefix (or prefixes) of the MN and is the mobility anchor point to manage the binding between the MN home address (MN-HoA) and its current point-of-attachment [SAEEPC09]. Every packet sent to the MN-HoA end up by the LMA. There they will be forwarded through a bi-directional tunnel to the MN's attached MAG. All together it builds the Proxy Mobile IPv6 domain for an MN.

2.2.3 Functional principle

Unlike MIPv6, the PMIPv6 protocol is only used within backbone networks. It serves as a protocol between the LMAs and MAGs to manage mobility sessions for MNs that are outside of these networks. LMAs and MAGs exchange signaling messages among each other to accomplish service functionality. It will never be exposed to an end-user, referenced as MN in this document.

2.2.3.1 Signaling Messages

PMIPv6 most likely uses two types of signaling messages to accomplish binding functionality. To utilize the whole extent of binding registrations, PMIPv6 relies on Mobility Options which are presented in the Appendix Annex A.

2.2.3.1.1 Proxy Binding Update (PBU)

The PBU message as described in [RFC5213] is an extension to the definition of the MIPv6 message format [RFC3775]. It's an additional header on top of the IPv6 Mobility Header. PBU messages have to be constructed as follows:

- IPv6 header (Mobility header (Mobility Options ( ))).

For a more detailed description one can read the corresponding chapter in [RFC5213].

2.2.3.1.2 Proxy Binding Acknowledgement (PBA)

The PBU message of PMIPv6 extends the PBU of MIPv6 [RFC3775] (with the additional R flag specified in [RFC3963]) by the P flag. The P flag indicates that the LMA that processes the corresponding PBU supports proxy registrations. The construction is identical to PBU messages, as it can also contain zero or more Mobility Options. Typically the PBA contains the same Mobility options as the corresponding PBU with the identical values set. However, there are some exceptions e.g. if a timestamp is valid or not, which will be discussed later.

2.2.3.1.3 Error Handling

The most decisive header field of the PBA is the status field. If the status-code is equal to, or greater than 128, an error has occurred. Depending on the error it is common for the MAG to repeat the previous step. As solicited before the PBA will mostly just contain the same values in the Mobility Options as it previously received, with a status code corresponding to the occurred error. However, there are two other possibilities:

- LMA silently drops the PBU.
- LMA has to update a Mobility Header value.

The latter seems to be ignored in some cases by Cisco's PMIPv6 implementation, which will be addressed later on.

2.2.3.2 Initial Binding Registration

When a MN attaches to an access link connected to the MAG, it typically follows the procedure of IPv6 Stateless Address Autoconfiguration [RFC4862]. By receiving Router Solicitations on the access link, the MAG recognizes the MN as a new client. Therefore it initializes the PMIPv6 binding registration process by sending a Proxy Binding Update (PBU) to the MN's LMA. If the MNs link-layer address is not registered in the corresponding PMIPv6 domain, meaning there is no Network Access Identifier (NAI) configured with the present link-layer address, the Mobile Node Identifier (MN-Identifier) option is set to the MNs link-layer address. Although if the MAG hasn't any knowledge about existing bindings for the given MN-Identifier, the Home Network Prefix option is set to an all-zero value.

A PBU with the Home Network Prefix option that is set to an all-zero value indicates the creation of a binding registration. Otherwise, if a home network prefix is provided in the Home Network Prefix option (so a non-all-zero value), the PBU indicates a lifetime refreshing of an existing binding cache entry.

After receiving a PBU, the LMA checks the local Binding Cache Entries for an existing binding. If there is no existing binding, the LMA must allocate one or more home network prefixes to the MN and assign it to a new mobility session. If there is no existing bi-directional tunnel to the MAG, the LMA must establish one. Also the LMA has to create a prefix route through that tunnel for forwarding any traffic received for the MNs home network prefix associated with that mobility session. Finally, after successfully setting up the mobility session and the bi-directional tunnel to the corresponding MAG, the LMA must send a Proxy Binding Acknowledgement (PBA) with the assigned home network prefix for the MN back to the MAG.

After a successful binding registration process the MAG sends a Router Advertisement on the access link where the MN is connected. The MN will setup the IPv6 address on the interface that is attached to the access link, based on the given home network prefix from the Router Advertisement.

2.2.3.3 Default Router

The MAG acts as the IPv6 default router for the MN on the access link, therefore it will send the Router Advertisements. As the MN moves from on access link to another, the MN would always detect a new default-router after every handoff, if the Router Advertisements are sent using a different link-local or link-layer address. Therefore all MAG's have to either share the same link-local and link-layer address in the corresponding PMIPv6 domain or the LMA has to generate the link-local address and provide it to the MAG as part of the signaling messages.

2.2.3.4 Security considerations

PMIPv6 itself has no security mechanism implemented. As defined in [RFC5213], signaling messages exchanged between MAG and LMA must be protected using end-to-end security associations offering integrity and data origin authentication. Such mechanisms are not mandatory for any communication between a MN and a MAG.
To accomplish integrity and data origin authentication IPsec must be implemented to protect PMIPv6 signaling messages (PBUs and PBAs). Because confidentiality protection is not required, instead of using Encapsulating Security Payload [RFC4303], the IP Authentication Header can also be implemented.
Access security protocols should ensure that a MN on the access link is authenticated and authorized to use the PMIPv6 service. However, this is recommended by [RFC5213], there are no further terms of reference of how this could be accomplished. The PMIPv6 specification operates with the stated assumption of having an established trust between the MN and the MAG before protocol operation begins.

In PMIPv6 domains, the use of IPsec is implemented by design of IPv6 and therefor depends on the implementation/architecture of the IPv6 network. Generally, using IPsec is recommended in IPv6 but has to deal with the same issues as in deployments of Ipv4. That means dealing with a high configuration complexity and key management mechanisms, sometimes resulting in an operational overhead. Furthermore, a lot of IPv6 stacks do not today support IPsec, or maybe questionably implemented. Therefore, PMIPv6 (and IPv6) might be deployed largely without cryptographic protections of any kind.

2.2.4 Cisco implementation

The following sections display the results of a test of Cisco's PMIPv6 implementation. Therefore, a laboratory has been configured, using a Cisco ASR 1002 (with IOS 15.2.4S1) as LMA. For MAG functionality two Cisco 2921 Integrated Services Router using IOS 15.2.4M1[1] with activated datak9[2] technology are used. The focus of the analysis was on implementation faults and violations against the specifications (mainly [RFC5213]).

2.2.4.1 PMIPv6 Domain Configuration

[RFC5213] describes a problem in message ordering while receiving binding upgrades from a mobile node. To solve this problem two methods are specified, using timestamps and sequence numbers. In this context, several flags are introduced, *MUST* be adjustable in the domain configuration. Unfortunately, Cisco does not support the adjustment of two of those flags. The CLI options are still implemented, but are not supported in the tested IOS version.

[1] PMIPv6 is supported since IOS15.2.4M.

[2] Software Upgrade needed for PMIPv6.

2.2.4.1.1 Sequence Number option for Message Ordering

If LMA cannot determine the sending order of the received Proxy Binding Update messages (e.g. due to latency problems), it may potentially process an older message sent by the MAG, as described in [RFC5213]. To solve these problems, two alternatives are adopted by specification:

On the one hand, MIPv6 [RFC3775] uses a message ordering scheme based on sequence numbers. This scheme may cause problems in case of handover from one MAG to another. For this scheme to work, the serving MAG in a Proxy Mobile IPv6 domain must have the ability to obtain the last sequence number that was sent in a binding registration message for that mobility session. This can either be realized by *context transfer schemes* or by maintaining the sequence number in a policy store.

The other approach to solve this problem is based on timestamps, sent with each signaling message to the LMA. As this is a portion of PMIPv6 where the whole service relies on, the validity of timestamps has to be ensured properly.

Because clock drifts reduces the effectiveness of the timestamp mechanism, the first variant, using exchange of sequence numbers would be the better solution. In the analyzed laboratory environment, the ordering scheme of sequence numbers is not supported either by the Cisco LMA or MAG. Because this functionality is introduced as one of two alternatives, this is not directly a violation of the PMIPv6 specification, but would be the more comfortable way.

Another differentiation between Cisco implementation and specification was found in receipt of *Proxy Binding Update* message while using timestamp based ordering scheme. In case of checking the validity of timestamp [RFC5213] says that

“The timestamp value contained in the Timestamp option MUST be close enough (within TimestampValidityWindow amount of time difference) to the local mobility anchor’s time-of-day clock. However, if the flag MobileNodeGeneratedTimestampInUse is set to a value of 1, the local mobility anchor MUST ignore this check and perform only the following check.”

And

“The timestamp MUST be greater than all previously accepted timestamps in the Proxy Binding Update messages sent for that mobile node.”

Unfortunately, the option *MobileNodeGeneratedTimestampInUse* was not implemented in the above described setup, leading to another indirect violation of the RFC.

2.2.4.2 Cisco’s Timestamp Approach

According to [RFC5213] the used timestamp in PMIPv6 messages is defined as follows:

> *“A 64-bit unsigned integer field containing a timestamp. The value indicates the number of seconds since January 1, 1970, 00:00 UTC, by using a fixed point format. In this format, the integer number of seconds is contained in the first 48 bits of the field, and the remaining 16 bits indicate the number of 1/65536 fractions of a second.”*

Based on observations of the communication in the laboratory setup, exchanging PMIPv6 signaling messages, the Cisco devices are using a different approach. The used approach is packed as 64 bit integer string and is similar to the Unix timestamp. It follows the format

time() + 2208992388, with time() as current Unix timestamp.

This calculation does work at all, but is a violation of the RFC in Cisco’s implementation.

2.2.4.3 Cisco's Timestamp in Proxy Binding Acknowledgements

In context of the above described Binding Update messages, containing timestamp for message ordering, another suspicious behavior could be observed. According to [RFC5213] on receipt of the Proxy Binding Update message, one of the two actions must apply:

- If the timestamp is valid (or if the MobileNodeGeneratedTimestampInUse flag is set to 1), the LMA MUST return the same timestamp value in the PBA message it sends to the MAG.
- If the timestamp is not valid the LMA must reject the PBU and send a PBA message with the status field set to TIMESTAMP_MISMATCH. The value of the Timestamp option MUST be set to the current time of day on the LMA.

Even though the specification enforces the way the timestamp in PBU is constructed (based on the validity of the received timestamp), Cisco's implementation does not follow the specification. Even if the received timestamp is invalid, it sends back the received and therefore invalid timestamp back to the corresponding MAG and not, as specified, the current time of day on the LMA.

2.2.5 Summary

As future technology of 4G networks, PMIPv6 is a variant to provide mobility to users through different locations. This feature offers functions equivalent to the common Mobile IP approach, but without depending on client functionality. All interaction is handled by the PMIP backend, called MAG and LMA. To get an idea of the implementation in future, in this context a laboratory was set up and analyzed. This practical part of the analysis showed up some differentiations between the implementation and the specification, not leading to a security impact. The analyzed implementation currently misses specified features and options, which should be added to the implementation and be configured by the provider. Therefore, it can be assumed that the current implementation is still under development and raises new challenges for Mobile IP and IPv6.

Another important issue is the use of IPsec for securing the communication between LMA and MAG, otherwise it would be possible for an attacker to insert self-crafted packets, eavesdrop or control the control data traffic. As for similar control plane protocols (like demonstrated in [ASMONIA_D5.2]), the use of IPsec is recommended, but not mandatory and will therefore only optionally be used in all deployments. Although recommended in standards, IPsec may possibly not be used due to its complexity. Therefore a strict isolation and hardening of control components and infrastructure is required. Otherwise there will be a lack of security in control networks.

3 Conclusion and Outlook

When starting the project we carried out a threat and risks analysis. Various threats were identified which were necessary to be identified and assessed but which are no surprise in the context of complex systems as MNOs operate today. The proposals we have created and elaborated in the ASMONIA project each have their limitations based on the respective stakeholders.

In the future, end users cannot be engaged to fight threats. Currently, their terminals cannot be used as instruments that enrich the sensor infrastructure, because no means are specified allowing to convey such information to the network. Although technically the protection of mobiles could be improved, a wider deployment to the mass consumer market seems questionable. Standards would be needed in the first place to indicate loss of integrity on UEs or to deploy malware sensors and thus instrument such terminals as a sensor infrastructure [ASMONIA_D2.3].

MNOs can and will continue to improve their protection- as they have done before. ASMONIA has made some contribution for the protection of NEs and software on NEs in the mobile network. Also, malware collection and analysis and information about the propagation of malware are very helpful information for the individual MNO to initiate (development of) countermeasures.

Sharing information amongst MNOs is yet seen a suitable means to broaden situational awareness based on experiences competitors are gaining. There is no indication that learning from experiences of competitors cannot be fruitful. Though, probably, the larger the individual MNO the less informative will an information sharing be. Nevertheless, MNOs are conservative, cost sensitive and reluctant to exchange information. The reason might be more a psychological disposition than that the reluctance is actually build on technical facts.

There is no reason anymore to hide away information about vulnerabilities or attacks an MNO undergoes. While an operator under attack may conceive this fact negative for its image, there is no reason to not communicate such security relevant information: ASMONIA has elaborated a collaborative method that ensures reputation loss free collaboration.

Such information exchange may also create a secondary effect: Less hidden information about security relevant incidences can be helpful to improve the assessment of threats concerning their frequency and potential impact. Exchanging information, as an informational side effect, helps building better statistics.

At the end of the ASMONIA project the resulting findings suggest the next steps for improving the protection of the mobile communication infrastructure as follows:

- **Re-assess regularly threats and risks, use pentesting tools where helpful**.
  The technology landscape a MNO has to operate is complex and constantly subject to change. The introduction of new technology and services is naturally influenced by legacy technologies and hence does not reduce the vulnerabilities – it rather bears the risk to introduce new vulnerabilities. To understand the changed resulting threats regular re-assessment seems to be a helpful approach. By covering in addition the potential gap between specification and their implementation in products and by disclosing (mostly unintended) misconfiguration issues pentesting will help to improve the confidence in the system integrity of mobile communication infrastructures.
- **Reconsider mobile terminals as sensors**
  Threats for the mobile infrastructure may basically arise from the Internet or, if UEs are used as launching pads, threats may arise and propagate on the terminal side and harm the network. So far UEs are not suitable to be used as a sensor infrastructure - current standards have not identified this support as helpful. It seems

helpful for an improved operation of the mobile infrastructures, if on future mobile devices such capabilities are encompassed in the signaling or information exchange between the UEs and the MNO.

- **Apply SW integrity protection to NEs in the mobile network**
  NEs are getting more exposed to threats while instruments and knowledge about how to launch attacks is more easily accessible. Some security baseline decisions that were taken in the past and implanted in 2G legacy standards are overcome today and it is hence fair to say that older systems can become a risk factor. Also, the SW production has today more widely distributed supplier chains, while on the other hand MNOs may ask for more detailed source authentication. SW integrity protection to date has suitable and technically viable solutions to improve trust and reliability between MNOs and vendors.
- **Engage malware sensors in networks**
  Increasing spread of malware and more sophisticated botnet activities can be expected to expand. It is basically only a question of time. Suitable sensors, mitigation solutions and countermeasure are thus very attractive for MNOs as a future field of competitive differentiation.
- **Share information**
  We argue that information sharing is for MNOs the key to improve situational awareness beyond the scope of the own network. The ASMONIA focus was to improve the security of mobile communication networks by supporting the collaboration related to security between MNOs. The solution elaborated fulfills the MNOs’ security and privacy requirements and does not set the reputation at risk.

References

[ASMONIA_D1.1] ASMONIA Deliverable 1.1, “”, Reference Architecture for Collaboration in Mobile Networks – Use Cases, Requirements, and Concepts”, May 2011, available from www.asmonia.de

[ASMONIA_D1.2] ASMONIA Deliverable 1.2, “Collaborative Procedures for Mobile Network Infrastructure Architectures”, Mar. 2012, available from www.asmonia.de

[ASMONIA_D1.4] ASMONIA Deliverable 1.4, “Validation of cooperative methods”, Jun. 2013, available from www.asmonia.de

[ASMONIA_D2.1] ASMONIA Deliverable 2.1,” Evaluating Methods to assure System Integrity and Requirements for Future Protection Concepts”, Apr. 2011, available from www.asmonia.de

[ASMONIA_D2.2] ASMONIA Deliverable 2.2, “Protection Methods for Target Systems”, Jul. 2012, available from www.asmonia.de

[ASMONIA_D2.3] ASMONIA Deliverable 2.3, “Establishing UE and NE Protection Methods – Security Infrastructure Integration and Re-Evaluation”, Jun. 2013, available from www.asmonia.de

[ASMONIA_D3.3] ASMONIA Deliverable 3.3, “Design and Implementation of an Intercloud demonstrator”, May 2013, available from www.asmonia.de

[ASMONIA_D3.4] ASMONIA Deliverable 3.4, “Evaluation of the Intercloud demonstrator”, Jun. 2013, available from www.asmonia.de

[ASMONIA_D4.1i] ASMONIA Deliverable 4.1i, “Recommender System for Security Risk Reduction – Situational Awareness for Critical Information Infrastructures”, Nov. 2011, available from www.asmonia.de

[ASMONIA_D4.1ii] ASMONIA Deliverable 4.1ii, “Recommender System for Security Risk Reduction – Situational Awareness for Critical Information Infrastructures”, Nov. 2012, available from www.asmonia.de

[ASMONIA_D4.2] ASMONIA Deliverable 4.2, “Methods for Classification, Assessment, Treatment and Evaluation of Information Security Risk – Continuous Security Risk Reduction for Critical Information Infrastructures”, May 2013, available from www.asmonia.de

[ASMONIA_D4.3] ASMONIA Deliverable 4.3, “Methods for Collaborative Detection and Analysis”, Feb. 2013, available from www.asmonia.de

[ASMONIA_D5.1] ASMONIA Deliverable 5.1, “Threat and Risk Analysis for Mobile Communication Networks and Mobile Terminals”, Feb. 2012, available www.asmonia.de

[ASMONIA_D5.2] ASMONIA Deliverable 5.2, “Evaluation of protection concepts – Documented simulation model of the test network”, Oct. 2012, available from www.asmonia.de

[OpnetModelerLibrary] OPNET Modeler Library Models Documentation, Version 17.5

[US_DoE] Office of Science U.S. Department of Energy, “A Science-Based Case For Large-Scale Simulation”, July 30, 2003

[AndroidBmaster] Forensic Blog – Detailed Analysis of Android.Bmaster, 2012, http://forensics.spreitzenbarth.de/2012/02/12/detailed-analysis-of-android-bmaster/

[RFC3963] “Network Mobility (NEMO) Basic Support Protocol”, 2005, http://tools.ietf.org/html/rfc3963

[RFC4303] “IP Encapsulating Security Payload (ESP)”, 2005, http://tools.ietf.org/html/rfc4303

[RFC4330] “Simple Network Time Protocol (SNTP) Version 4 for IPv4, Ipv6 and OSI”, 2006, http://tools.ietf.org/html/rfc4330

[RFC5213] “Proxy Mobile Ipv6”, 2008; http://tools.ietf.org/html/rfc5213

[RFC4831] “Goals for Network-Based Localized Mobility Management (NETLMN)”, 2007; http://tools.ietf.org/html/rfc4831

[RFC4862] Ipv6 Stateless Address Autoconfiguration

[RFC3775] “Mobility Support in Ipv6”, 2004; http://tools.ietf.org/html/rfc3775

[RFC5094] “Mobile IPv6 Vendor Specific Option”, 2007, http://tools.ietf.org/html/rfc5094

[SAEEPC09] Magnus Olsson et al, „SAE and the Evolved Packet Core – Driving the Mobile Broadband Revolution“; 2009; ISBN 9780123748263

[DIZZY] http://c0decafe.de/

[THS2013] D. Titze, H. Hofinger, P. Schoo, Using Secure Multiparty Computation for Collaborative Information Exchange, submitted for publication, 2013

[HSTS2013] M. Haustein, H. Sighart, D. Titze, P. Schoo, Collaboratively Exchanging Warning Messages Between Peers While Under Attack, submitted for publication, 2013

[TR36.822] 3GPP TR 36.822 v11.0.0, “Technical Specification Group Radio Access Network; (RAN) enhancements for diverse data applications (Release 11), Sept. 2012

Abbreviations

Abbreviation	Explanation
3GPP	3rd Generation Partnership Project
4G	4th Generation
ACN	ASMONIA Collaborative Network
C&C	Command and Control
DDoS	Distributed Denial of Service
DoS	Denial of Service
eNodeB	Evolved NodeB
GPS	Global Positioning System
HTTP	Hyper Text Transfer Protocol
IMEI	International Mobile Station Equipment Identity
IMSI	International Mobile Subscriber Identity
IOS	Internetwork Operating System
IP	Internet Protocol
IT	Information technology
LMA	Local Mobility Anchor
LTE	Long Term Evolution
MAG	Mobile Access Gateway
MIB	Management Information Base
MN	Mobile Network
MNO	Mobile Network Operator
MPC	Multi-party Computation
NE	Network Element
OS	Operating System
P2P	Peer-to-Peer
PBA	Proxy Binding Acknowledgement
PBU	Proxy Binding Update
PMIPv6	Proxy Mobile Ipv6
RFC	Request for Comments
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SW-IP	(Cryptographic) SW Integrity Protection
TAC	Traceable Anonymous Certificate
TCP	Transport Control Protocol
TR	Technical Report
UDP	User Datagram Protocol
UE	User Equipment
VoIP	Voice over IP
WP	Work Package

Revision History

Version	Date	Changes
0.1	2013-02-21	Initial skeleton version
0.2	2013-05-15	Review version
1.0	2013-06-24	Final version

Annex A

A.1 Mobility Options

The mobility options are basically for additional information that may not be needed in every use of a particular Mobility Header. In the PBU and the PBA the following mobility options are mandatory:

- Mobile Node Identifier option
- Home Network Prefix option
- Handoff Indicator option
- Access Technology Type option

The Timestamp option is according to [RFC5213] not mandatory if the Sequence-Number-based scheme [RFC3775] is used for PBU and PBA. The main problem at this is to synchronize the sequence number between all components. This could lead to the problem that if a LMA cannot determine the sending order of the received PBU messages. It may potentially process an older message which was sent by a MAG where the MN was previously anchored. The result is that the LMA updates the MN Binding Cache entry incorrect and create a routing state to the previous MAG of the MN. According to the [RFC5213] the alternative solutions is to use timestamps. Additionally, there can be one or more instances of the Vendor-Specific Mobility option [RFC5094].

Mobile Node Link-layer Identifier Option

The Mobile Node Link-layer option is used for exchanging the MN’s link-layer identifier in the PBU and PBA between MAG and LMA.

Home Network Prefix Option

The Home Network Prefix Option is used for exchanging the MN’s home network prefix information in the PBU and PBA between LMA and MAG. The Option can be added multiple times to a PBU or PBA for all MN’s home network prefixes.

Handoff Indicator Option

The Handoff Indicator option is used for exchanging the MN’s handoff-related information in the PBU and PBA between MAG and LMA. The following values are defined at the moment:

0. Reserved
1. Attachment over a new interface
2. Handoff between two different interfaces of the mobile node
3. Handoff between mobile access gateways for the same interface
4. Handoff state unknown
5. Handoff state not changed (Re-registration)

Access Technology Type Option

The Access Technology Type option is used for exchanging the type of the access technology which the MN uses at its current attached MAG. It will extend the PBU or PBA message between MAG and LMA. The following values are defined at the moment:

0.	Reserved	("Reserved")
1.	Virtual	("Logical Network Interface")
2.	PPP	("Point-to-Point Protocol")

3.	IEEE 802.3	("Ethernet")
4.	IEEE 802.11a/b/g	("Wireless LAN")
5.	IEEE 802.16e	("WIMAX")

Timestamp Option

The Timestamp option principle is to add to the massage the current time of day. If a node receives the message it checks that this timestamp is greater than all previously accepted timestamps. To avoid the clock drift all mobility entities in a PMIPv6 domain have to synchronize their clocks to a common time source (the nodes may use the Network Time Protocol [RFC4330] for synchronizing).

Upon receipt of a PBU with the timestamp option the LMA have to check the validity of the timestamp. To accept it as valid the timestamp value must be close enough to the LMA’s time-of-day clock and must be greater than all previously accepted timestamps in the PBU messages sent for that MN. If the value is lower or not valid then the LMAs reject the PBU and send a PBA with the status field set to TIMESTAMP_LOWER_THAN_PREV_ACCEPTED or TIMESTAMP_MISSMATCH along with the value of the timestamp option set to the current time of day of the LMA.