User plane security alternatives in the 3G evolved Multimedia Broadcast Multicast Service (e-MBMS)

Simone Teofili, Michele Di Mascolo,
Giuseppe Bianchi, Stefano Salsano
Dip. Ing. Elettronica,
University of Roma "Tor Vergata", Rome, Italy

Alf Zugenmaier
DoCoMo Euro-Labs,
Munich, Germany

Abstract— **The Multimedia Broadcast Multicast Service (MBMS) has been included in the 3GGP architecture to provide broadcast/multicast services. In the 3GPP Long Term Evolution, the evolved MBMS (e-MBMS) architecture is currently being standardized. This position paper discusses the security issues currently being considered for the e-MBMS IP multicast user plane. Currently proposed security architectures "limit" themselves to include Group Security Associations (GSA). In this paper we raise the position that GSA might not be a sufficiently secure solution in the long run. In sight of this, we propose to adopt a secure multicast overlay approach as a possible short-term solution, thanks to its straightforward deployment. To prove this latter point we overview how to set-up a proof-of-concept implementation over public domain linux routers. We functionally compare GSA with the proposed secure multicast overlay approach, showing that the overlay approach provides not only the same level of security, but also a reduced risk of denial of service attacks. We preliminarily (qualitatively) discuss the pros and cons of the two solutions in terms of performance. Ongoing work is targeted to complement these preliminary considerations with a quantitative investigation.**

Keywords: Multicast Broadcast Multimedia Services, 3GPP, MBMS security

I. Introduction

The 3GPP has introduced the Multimedia Broadcast Multicast Service [1] as a mean to broadcast and multicast information to 3G users. MBMS provides much more flexibility than other distribution systems like DVB-H [2] because it includes return channel and it is able to send information to an arbitrary group of receivers (multicast) in addition to distributing the same channels to all users (broadcast).

In the context of the "Long Term Evolution" (LTE) of 3G systems the MBMS will evolve into the e-MBMS [3] ("e-" stands for evolved). The LTE e-MBMS aims at providing broadcast and multicast services combining flexibility and high efficiency in the spectrum occupancy, and outperforming DVB-H for the distribution of broadcast channels. This will be achieved through increased performance of the air interface that will include a new transmission scheme (Multicast/Broadcast Single-Frequency Networking - MBSFN) and the capacity of having the same signal transmitted by tightly synchronized neighbor cells.

In addition to significant improvements in the air interface, the e-MBMS sets forth a rationalization and simplification in the envisioned architecture. This is accomplished through either new dedicated architectural elements as well as new user-plane and control-plane interfaces. Securing these interfaces is a fundamental issue. It calls for additional "network security" solutions to be added to the already existing "application security" solutions inherited from the original MBMS architecture.

While control plane interfaces, being unicast, may be secured through off-the-shelf IPsec security associations, the user plane interface requires a multicast security mechanism. From a purely algorithmic point of view this is not nearly a problem as many solutions have been proposed in the last decade. However, from an architecture and deployment point of view, an issue to carefully considered is that the Multicast version of the IPsec protocol has not yet been extended to support source authentication mechanisms such as, e.g., TESLA[4].

This problem appears circumvented by the assumption, currently carried out in 3GPP documents (such as [5]), that a potential attacker is not able to violate the physical entities that builds up the architecture. As a consequence, these analyses conclude that IP multicast security can be restricted only to the usage of Group Security Associations (GSA) [6]. However, while this may be true in the short term evolution, this assumption appears overly restrictive in the long run (and hence GSA appears to be a solution which in any case needs to be significantly complemented). In a longer time frame, with the emergence of home node Bs and multiple virtual operators sharing a same physical e-MBMS infrastructure, we indeed believe that untrusted evolved node Bs (e-NBs, i.e. base stations) should be considered as possible threats. Also, the growing importance of user-generated content, possibly with local geographic scope and fostered by social networking needs, is deemed to impact such a rigid security assumption. When "local breakout" is considered, a node B can be a further source of multicast distribution in addition to the MBMS gateway, and as such it is hard to guarantee that, by assumption, "malicious" or spoofed traffic cannot be originated by a node B.

In addition, we argue that not only GSA is a solution not completely appropriate for a long term evolution, but also it is not even fully viable for a short-term deployment. Indeed, as discussed later on in the paper, delivery of multicast data over a deployed IPsec architecture is not as straightforward as it might seem. Indeed, the support of multicast in the IPsec architecture has been explicitly introduced only in the latest specification (RFC 4301), and as such existing implementations might not be conformant. Moreover, multicast data delivery over IPsec has non negligible consequences, especially in terms of support of relevant policies, and at the date of writing a complete specification is still at the level of IETF internet Draft [7].

All these consideration suggest that, rather than pushing GSA forward, a more practical and short-term viable way towards the security of the e-MBMS user plane may consist in identifying solutions simpler than GSA and whose deployment can be considered trivial. Specifically we argue that a ready and viable solution is an approach which we call "Secure Multicast Overlay". This is based on the deployment of an overlay (legacy and unprotected) multicast network on top of secured overlay network links, protected by means of off-the-shelf unicast IPsec tunnels.

The rest of the paper is structured as follows. A brief review of the basic concepts related to the e-MBMS architecture and relevant security issues is provided in section II. Section III reviews and discusses GSA. Section IV describes the proposed secure multicast overlay approach. Section V provides a comparison among GSA and the secure multicast overlay approach. To prove the viability of the secure multicast overlay approach, section VI describes how to readily implement it on top of public domain linux routers. Conclusions are drawn in section VII.

II. E-MBMS ARCHITECTURE AND RELATED SECURITY ISSUES

The e-MBMS architecture is illustrated in Figure 1. The e-BM-SC (Broadcast Multicast Service Center) is the entity that is in charge of introducing multimedia content into the 3G network. The e-MBMS GW is the "root" of the distribution tree for the multimedia content, that is used to broadcast/multicast the information towards 3G users through the e-UTRAN (UMTS Terrestrial Radio Access Network). Within e-UTRAN the e-NB (Node B, i.e. the base stations) are the collectors of this information that has to be distribute to users on the air-interface. The MCE (Multi-cell/multicast Coordination Entity) is a new entity needed to coordinate the transmission of synchronized signals from different cells (e-NB). The e-MBMS GW is logically split into two parts, one related to control plane and one related to user plane. Likewise, two distinct interfaces have been defined between e-MBMS GW and e-UTRAN: M1 for user plane and M3 for control plane. Note that the M1 interface will exploit IP multicast to distribute the multimedia content. Note also that the architecture represented in Figure 1 represents one possible solution for locating the MCE, another solution is to have the MCE outside the e-NB, defining an additional control plane interface (M2) between the MCE and the e-NB.

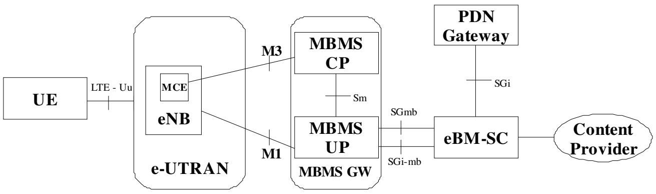

Figure 1 – 3GPP e-MBMS architecture

The e-MBMS needs to be secured against a set of possible threats. A thorough analysis of threats and security solutions in the context of multimedia delivery is provided in [15].

The set of threats to be considered depends on a set of assumptions on the capacity/capabilities of the potential attackers. In particular the most important assumption in the e-MBMS security analysis carried out by 3GPP is that a potential attacker is not able to violate the physical entities that builds up the architecture [3]: e-NBs and MBMS-GW. Therefore all security attacks can be carried out only in the links that connects the nodes. Section V provides more details about the threats that have been considered within 3GPP analysis.

It is worth to now distinguish between the two complementary aspects of "application security" and "network/infrastructure" security. The "application security" is mainly concerned with granting access to content only to authorized customers. In this respect, e-MBMS will simply re-use the approach standardized in the context of MBMS, which handles the application level security "end-to-end" between the UEs and the eBM-SC. On the other hand, the "network/ infrastructure" security is concerned with avoiding denial of service attack, misuse of the transport capabilities, modification of the reach of legitimate traffic and so on.

The network/ infrastructure security of e-MBMS is a current concern of 3GPP. For convenience, the security aspects of e-MBMS has been split by 3GPP in control plane security (e.g. related to the M3 interface) and user plane security (related to the M1 interface). As for the control plane security, 3GPP has opted for using a set of point-to-point IPsec security associations among all nodes involved in the control plane exchange of information. The discussion on how to secure the M1 interface, which uses IP multicast, is ongoing. At the current status of the discussion, emerging IP multicast security techniques, namely the Group Security Association (GSA) [6], are proposed to be used to protect the M1 interface.

III. SOLUTION BASED ON GROUP SECURITY ASSOCIATION (GSA)

Securing IP multicast group communication is a complex task requiring specific mechanisms to provide the same functionalities of common point-to-point protection protocol as for example the source authentication.

According the architectural framework, every multicast group has to contain three functional entities:

- *The Group Controller and Key Server (GCKS)* that issues and manages the cryptographic keys used by a multicast group. The GCKS also conducts user-authentication and authorization checks on the candidate members of the multicast group.

- *The Sender* is an entity that sends data to the multicast group.
- *The Policy Server* is the entity that creates and manages security policies specific to a multicast group.

The above mentioned entities has to provide three different functionalities: i) the Multicast data handling which covers the security-related treatments of multicast data by the sender and the receiver, ii) Group Key Management that is concerned with the secure distribution and refreshment of keying material and iii) Multicast Security Policies that covers aspects of policy in the context of multicast security.

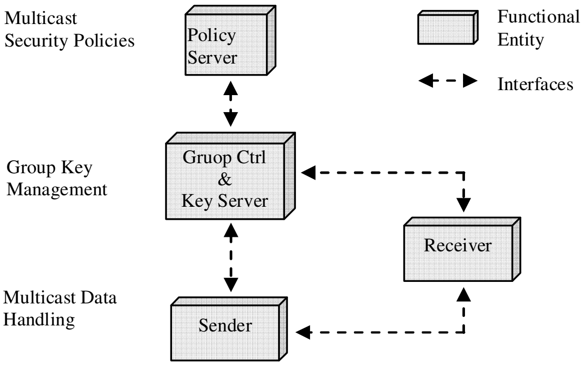

Figure 2 - Multicast Security Reference Framework

A. Group Security Associations (GSA)

A GSA is an extension of the SA concept representing both *an aggregation of SAs* (Figure 2.2.b) used for several independent purposes, and *a superset of the SA concept* (Figure 2.2.a) extending SA parameters with the group policy attributes.

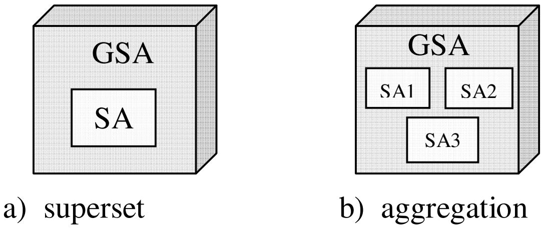

Figure 3 - Relationship of GSA to SAs

A GSA groups usually is composed by three categories of SAs:

- **Registration SA (REG)**: A unicast SA between the GCKS and each group member to pull GSA information (Re-key SA and Data Security SA parameters) from the GCKS. There are as many unique registration SAs as there are members in the group (and this may represent a scalability problem)
- **Re-key SA (REKEY)**: A single multicast SA between the GCKS and all of the group members: a unidirectional multicast transmission of key management messages from the GCKS to all group members
- **Data Security SA (DATA)**: A multicast SA between each multicast source speaker and the group receivers, protecting data between sender members and receiver members

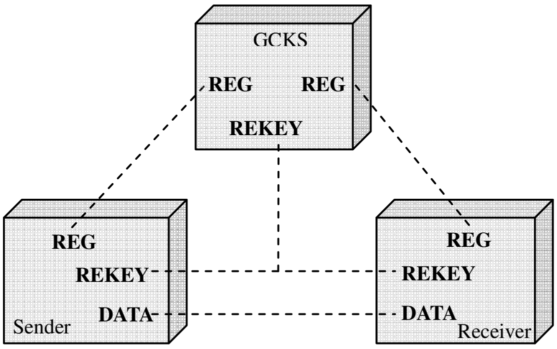

Figure 4 Three categories of SAs that can be aggregated into a GSA

B. Major Ipsec Databases

The support of multicast services requires a further effort in the standardization to extend the IPsec in order to manage the group policy and the entities role within the multicast group. The MSEC group [6] is currently standardizing extensions to the ESP protocol necessary to face the above mentioned problematic. In particular, the major databases defined in the standard IPsec architecture need to be extended with the addition of i) The Group Security Policy Database (GSPD) able to support both unicast security associations and the multicast extensions and ii) Group Peer Authorization Database (GPAD) that specifies which peers are authorized to participate in a group in a given Group Role (i.e. sender, etc).

In addition to the database a number of new security association attributes are defined. The most relevant are i) the directional attribute describing whether a pair of entities needs to set-up two "symmetric" SA or only one in the outbound direction ("receiver only"), or only in the inbound direction (to match "sender only" SPD directionality) and ii) re-key rollover procedure time intervals that is the time that the Group Receiver IPsec subsystems will maintain for the same flow two Data SA overlapped in time, so that there is continuity in the multicast data stream across group re-key events. This capability is referred to as "re-key rollover continuity".

C. Data Origin Authentication

A Message Authentication Code (MAC) is often used to achieve data origin authentication for connections shared between two parties. However, typical MAC authentication methods using a single shared secret are not sufficient to provide data origin authentication for groups with more than two parties. With a MAC algorithm, every group member can use the MAC key to create a valid MAC tag, whether or not they are the authentic originator of the group application's data. When the property of data origin authentication is required for an IPsec SA distributed from a GKCS, an authentication transform where the originator keeps a secret should be used. Two possible algorithms are TESLA or RSA digital signature.

D. Critical Aspects

The fast integration of the entities necessary to set up a GSA within the eMBMS infrastructure does not seem an easy task. First of all the architecture and protocols (not still complete) issued by the IETF MSEC group in order to manage and set-up a GSA has to be discussed and adapted to the LTE architecture by the specific 3GPP groups. Furthermore a deep evaluation on the performance limitation of the GSA together with the evaluation of solutions offering the same security but different performance drawback is necessary to fully understand, in the long term scenario, how to best deploy and dimension the full MSEC architecture

IV. PROPOSED SOLUTION BASED ON SECURE OVERLAY MULTICAST

We present an alternative solution to the deployment of GSAs, that does not require addition of new logical entities as shown in the previous section. Our solution is based on the combination of an overlay network approach combined with security services offered by IPsec standard [7],[8]. We will refer to our proposal as “Secure Multicast Overlay”. As mentioned earlier, this solution takes advantage of IPsec to protect the exchanged data from attackers external to the group while the network overlay allows to virtualize the connections making possible the deployment of multicast/broadcast services based on IP multicast.

Our solution changes the “end-to-end” vision of the security considered in GSA into a hop-by-hop vision. If we refer to a network where all nodes can be considered trusted, our idea is to decentralise the security functions from a single point-of-failure, which in previous solution is the GCKS, to all trusted nodes of the network.

Then it is possible to identify two distinct logical layers that clearly separate security services to those relating to management, establishment and distribution of multicast/ broadcast data. In particular, we refer to these two layers with the name i) Security Layer (Ipsec), ii) Overlay Multicast Layer

The Security Layer (IPsec) is made up of point-to-point IPsec SAs between individual network elements. The full deployment of IPsec SAs can provide authenticity and confidentiality of data transported and at the same time leaves the issue of nodes authentication from a single central entity to all elements of network in a distributed fashion.

The Overlay Multicast Layer is created through the deployment of GRE tunnels [9] among the multicast-aware elements, i.e. among those elements that are able to manage multicast traffic (ex. PIM-SM, IGMP, ecc.). In our implementation these features are handled by XORP [10] (open source software for routing) that allows the management and routing of multicast traffic. Indeed virtual interfaces (ex. gre0, gre1, etc.) created through GRE tunnels, with their IP addresses, will be used by the XORP routers for all operations related to the multicast/broadcast services. In this way is very simple to support multicast services even where not all nodes are multicast-aware, allowing you to bypass these nodes through the overlay network.

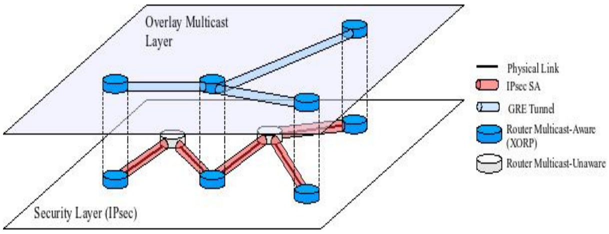

Figure 5 - Logical division of Security Layer from Multicast Layer

This solution is also very interesting in the scenario of a virtual operator, which is not in possess of the physical network. With this architecture, the virtual operator is able to abstract a virtual network through the overlay, which allows an easier deployment and management of multicast/ broadcast services. In this way a large number of overlay networks can co-exist on a single physical network, owned by a single provider. Having multiple virtual operators that share a single network may of course allows a substantial reduction of costs (installation and management of the physical network, etc.).

The adoption of the overlay solution for security may allow an easier and faster deployment of the e-MBMS infrastructure with respect to the GSA solution. A protection infrastructure based on point-to-point IPsec tunnel for the communication protection needs already to be deployed for the Control Plane protection. The User Plane packets could either exploit the encrypted tunnel used by CP packets or a totally new infrastructure common for all data plane flows. The overlay adoption in fact introduces a clear separation between the routing plane and the security procedure. The other solution instead requires that every multicast group has got its own GSA preventing the UP flows to exploit the same GSA.

V. COMPARISON OF THE PROPOSALS

A. Comparison of the solutions from the point of view of security

In order to evaluate the security of the two solutions we adopt the same security assumption made by the SA3 group in the security evaluation of the MBMS system. In particular all the entities belonging to the MBMS infrastructure are considered trusted. This assumption implies that all the attacks against the infrastructure can be lead only by external entities. As such the threats to be analyzed for both UP and CP are

- Packet Deletion
- Packet Modification
- Packet Insertion
- Dos attack

Under the above reported assumption the two solutions appear to offer the same protection against packets modification/insertion while secure multicast overlay is probably less vulnerable against DoS attacks. Both the GSA and the proposed overlay solution, in fact, are able to provide data confidentiality and to assure that a packet has been sent by a group member. However, we note that each re-keying operation in the overlay solution does not involve all the multicast group members as in the GSA. Every communicating pair runs the re-key procedure independently from the other pairs: a Dos attack exploiting spoofed re-keying messages can affect only a specific link of the overlay. Furthermore our solution does not require a central entity (i.e. a single point of failure) to manage the re-keying operations. Therefore DoS attacks against the proposed solution are less effective.

B. *Performance aspects*

Two different aspects have to be considered in order to evaluate the performances of the two solutions: the routing mechanisms and the negotiation and management of cryptographic keys related to different SAs within the same entities. Concerning the routing aspect the adoption of the GSA allows the MBMS infrastructure to fully exploit a network infrastructure supporting multicast routing. The multicast overlay solution instead potentially has higher burden due to the packet forwarding because does not exploit the advantages of native multicast. The performance impact of the packets routing and forwarding in the overlay solution strongly depends on a set of factors: i) the underlying network topology, ii) how the topology allows the multicast to be really exploited, and iii) the overlay multicast network topology (i.e. by having NBs replicating info towards other NBs is it possible to largely improve performances). The number of NBs that a MBMS-GW has to manage and the number of routers (when present) between the MBMS entities are the parameters that have to be considered to choose the best overlay routing infrastructure in order to minimize the performance difference due to the routing factor between the GSA and the overlay solution. The expected load, i.e. the number of broadcast/multicast flows, with respect to the link capacity will also be a critical factor. The other critical factor that has to be analyzed to properly evaluate the performances of the two solutions are the keys phase-over and the re-key procedure load. The key phase-over load depends on the time that an entity spends in order to retrieve the proper decryption key for the specific packet when packets belonging to different SAs have to be managed. In the MBMS scenario the load of the phase over depends directly on the number of active SAs that an entity has to manage at the same time. In fact, due to the type of service offered by the MBMS infrastructure the content providers will keep on transmitting contents for long period.

In the GSA solution the number of keys to be managed depends on the number of broadcast/multicast streams that the MBMS-GW (the data source) has to manage simultaneously. In the overlay solution it depends on the number of established SAs (i.e by the number of eNBs connected to the same MBMS-GW). In fact, In the GSA solution it is necessary to establish a data SA for every multicast group while in the overlay solution an entity has to establish an SA only with the other entities it has to communicate with.

The re-key procedure involving the whole multicast group together with a complex group set up mechanism probably represent the main concerns in the adoption of the GSA solution. A re-keying procedure is required whenever a timer expires. In order to avoid that the network is loaded with re-keying messages of different GSA the re-keying period has to be chosen carefully. The overlay approach is not affected by the re-keying problem since this procedure involves only two entities.

C. *Comparison of the solutions in the light of short-term/long term evolution*

The adoption of the GSA solution should address some criticalities. First of all its standardization is an ongoing task and the specification of important functionalities (e.g. the Group peer and the Group Security Policies databases) necessary to extend the IPsec protocol in order to support the GSA is object of discussion in IETF. Furthermore the addition of the specific entities, like the GCKS, within the eMBMS infrastructure will require a supplementary standardization work within the 3GPP groups. The interfaces and the communication protocol between the MBMS-GW, the eMB and the GCKS will have to be discussed and defined. Therefore it is really worth considering other short term solution that may minimize the impact on the architecture and have a simpler deployment, using off the shelf technologies.

The adoption of the GSA without the source authentication seems, in any case, to be in any case a “short term” solution that does not address the long term needs (home eNB, user generated content, social networking scenarios).

VI. Secure Overlay Multicast: Implementation Issues

To develop and evaluate our overlay solution we have setup a scenario on a virtual platform through the use of the Netkit [11] open source tool, in a Gentoo Linux [12] environment. Through this network emulator we have implemented a simple network architecture that closely represents the situation of interest. In particular we have built a network where only a set of machines are virtual-multicast aware, being nodes of the secure overlay. This machines use the routing software XORP already mentioned above for unicast and multicast traffic. The creation of security layer has been obtained using instead the racoon2 [13] open source software, which offers the possibility of establishing IPsec SAs between network entities and to be able to exploit the

IKEv2 protocol [8] for exchanging keys. GRE Tunnels for creating overlay network have been established only between multicast-aware machines. A GRE tunnel corresponds to the creation of a new virtual network interface that can be exploited by XORP router for multicast routing operations. Finally the proposed architecture has been tested by sending audio/video multimedia streaming in accordance with the procedures of multicast, and analyzed through Wireshark [14] network analyser for verifying the actual behaviour. Currently our work is oriented on the performance analysis of our solution, in terms of the number of streams multicast and number of users that the network can support with related analysis on degradation of service. In addition we are studying ways to achieve a dynamic installation and the adaptation of the network topology to the needs of traffic.

VII. CONCLUSIONS

The aim of this paper was to propose a possible alternative to GSA for the user plane security of e-MBMS, based on a secure multicast overlay over point-to-point IPsec Security Associations. We have provided motivations why GSA could not represent the best possible solution for user plane security. We argued that GSA is a solution not completely appropriate for a long term evolution, and also not easily viable for a short-term deployment. We compared the two solutions in terms of security under the assumptions that are considered for e-MBMS. We believe that the multicast overlay solution has equivalent security with respect to GSA as far as packet modification/insertion threat is concerned. Secure multicast overlay is preferable from the point of view of DoS attacks. In order to provide a complete assessment of the secure multicast overlay solution, a detailed analysis of performance and a performance comparison with GSA is still needed. We are currently working on these aspects.

REFERENCES

[1] 3GPP TS 26.346 V7.7.0 “Multimedia Broadcast/Multicast Service (MBMS); Protocols and Codecs”, March 2008

[2] ETSI EN 302 304 V1.1.1 “Digital Video Broadcasting (DVB); Transmission System for Handheld Terminals (DVB-H)”, November 2004

[3] 3GPP TS 36.300 V8.4.0 “Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN)”, March 2008

[4] A. Perrig, D. Song, R. Canetti, J. D. Tygar, B. Briscoe “RFC 4082 -Timed Efficient Stream Loss-Tolerant Authentication (TESLA): Multicast Source Authentication Transform Introduction ”, June 2005

[5] T. Hardjono, Verisign, B. Weis, Cisco, “RFC 3740 - The Multicast Group Security Architecture”, March 2004

[6] B. Weis, Cisco Systems, G. Gross, IdentAware Security, D. Ignjatic, Polycom, “Internet-Draft - Multicast Extensions to the Security Architecture for the Internet Protocol”, February 22, 2008

[7] S. Kent, BBN Corp, R. Atkinson, @Home Network, “RFC 2401 – Security Architecture for the Internet Protocol”, November 1998

[8] C. Kaufman, Microsoft, “RFC 4306 – Internet Key Exchange (IKEv2) Protocol”, December 2005

[9] D. Farinacci, T. Li, Procket Networks, S. Hanks, Enron Communications, D. Meyer, Cisco System, P. Traina, Junniper Networks “RFC 2784 – Generic Routing Encapsulation (GRE)”, March 2000

[10] http://www.xorp.org/

[11] http://www.netkit.org/

[12] http://www.gentoo.org/

[13] http://www.racoon2.wide.ad.jp/

[14] http://www.wireshark.org/

[15] Anand R. Prasad, Alf Zugenmaier and Julien Laganier, “Security Threats and Solutions: Multimedia in Mobile Communications Systems”, 10th International Symposium on Wireless Personal Multimedia Communications, WPMC 2007