tMULTICAST SECURITY FRAMEWORK FOR MULTI-SPOT BEAM SATELLITE NETWORK

Jani Puttonen[1], Sami Rantanen, Frans Laakso, Budiarto Herman, Janne Kurjenniemi
Magister Solutions Ltd., Sepänkatu 14, FIN-40720 Jyväskylä, Finland,
Email: {firstname.lastname}@magister.fi

Jani Suomalainen, Mikko Majanen, Janne Vehkaperä, Jukka Mäkelä,
Mika Rautila, Kari Seppänen
VTT Technical Research Centre of Finland, P.O. Box 1000, FIN-02044 VTT, Finland,
Email: {firstname.lastname}@vtt.fi

Olivier Smeyers
European Space Agency/ESTEC, Noordwijk ZH, the Netherlands,
Email: {firstname.lastname}@esa.int

1. Abstract

This article presents an overview of a secure multicast framework as well as a secure multicast system demonstrator used for end-to-end performance assessment of secure multicast service delivery over satellite. The security framework relies on IP security with multicast extensions and Group Domain of Interpretation (GDOI) multicast key management. The framework addresses challenges in the delivery of secure multicast services on top of multi-spot beam satellite networks by proposing several enhancements to overcome the bottlenecks.

2. Introduction

The global data traffic is growing rapidly due to video content and new emerging applications. Consequently, multicasting technologies are deployed to reduce redundant traffic and communication burden in networks. Examples of applications, which could benefit from secure multicast communication, include Internet Protocol Television (IPTV), Collaborative Working (CoW), remote medical assistance, distant learning, and Intenet of Things (IoT). These applications have specific security requirements: from backward and forward secrecy of communication, group and source authentication, and availability protection, to access control over multicast groups.

On the other hand, next generation of multi-spot beam satellite systems based on DVB-RCS2 [1], DVB-S2 [2] and DVB-S2x [3] specifications are finally emerging and changing the way satellite services are offered to the end users. The State-of-the-Art in high throughput broadband satellite communications systems rely typically on Ka frequency band and geostationary multi-spot beam satellites. These multi-beam architectures allow for a significant boost in capacity e.g. with usage of frequency reuse and multiple polarizations. Examples of such satellite systems are e.g. *Wildblue-1, Anik F2, KaSat, GlobalExpress* and *ViaSat-1*. In addition to traditional broadcasting services (e.g. IPTV), new satellite systems offer also broadband interactive services with the DVB-RCS2 based return link.

Secure multicast services on top of multi-spot beam satellite networks is an attractive combination. The services can benefit from the inherent advantages of the satellite system, such as large coverage area, as well as effective multicast transmissions. However, security solutions must address multi-spot beam interactive satellite system specific challenges to offer seamless access for the users. Such challenges - including e.g. long latency, channel fading, large bandwidth-delay product, variable channel conditions, service scalability, large user-space – make basic security operations, such as security establishment and secret key delivery, unreliable and expensive.

[1] Contact person: Jani Puttonen, Principal Scientist, Magister Solutions Ltd., Sepänkatu 14, FIN-40720 Jyväskylä, Finland, Phone: +358 44 5640814, Email: jani.puttonen@magister.fi

This article presents a secure multicast system capable of providing secure multicast communication by means of IP security (IPsec) and Group Domain of Interpretation (GDOI) key management. Secondly, a set of performance enhancements are proposed to overcome the challenges of secure services with multicast communications. Thirdly, multicast secure system demonstrator architecture is presented aimed for validation of the proposed enhancements and demonstration and performance assessment of the end-to-end secure multicast system.

3. Secure multicast framework

The proposed security framework consists of components and protocols enabling end-to-end secure multicast (and unicast) communication for different interactive satellite applications. The proposal addresses satellite specific challenges and enables availability of secured applications through satellites but also through terrestrial networks. The essential components in the framework are illustrated in Figure 1. The key server has a central role in the framework. It is responsible for delivering group keys for the group members according to the authorizations from the application servers. The group members include security end-points – for end-user terminals and applications servers - as well as to trusted Performance Enhancement Proxies (trusted PEP), which accelerate communication over satellites.

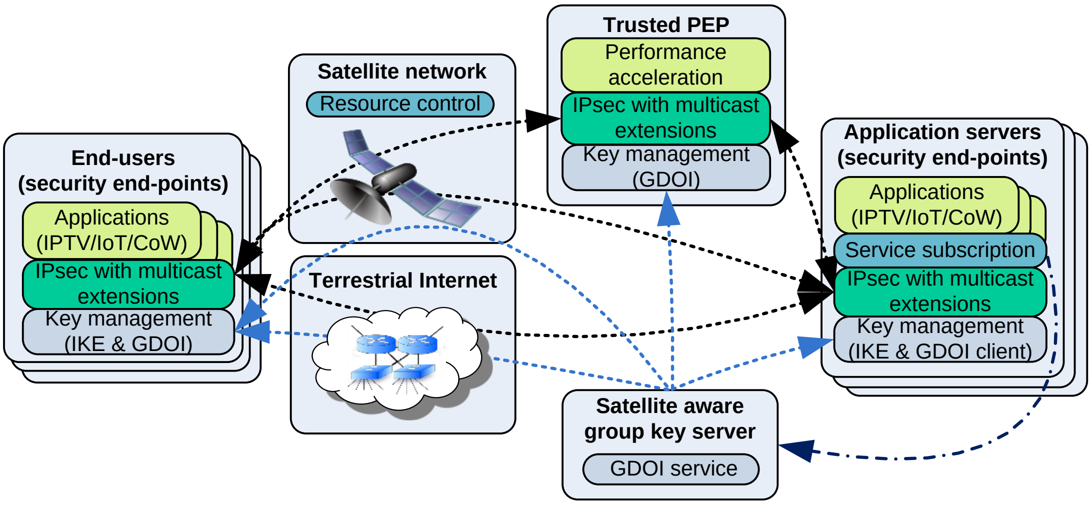
Trusted PEP
Performance acceleration
IPsec with multicast extensions
Key management (GDOI)
Satellite network
Resource control
End-users (security end-points)
Applications (IPTV/IoT/CoW)
IPsec with multicast extensions
Key management (IKE & GDOI)
Terrestrial Internet
Application servers (security end-points)
Applications (IPTV/IoT/CoW)
Service subscription
IPsec with multicast extensions
Key management (IKE & GDOI client)
Satellite aware group key server
GDOI service

Figure 1. Essential components, functions, and relations in the security framework.

To assure reliability, availability and, interoperability the security framework is based on the established and standardized security protocols. Communication security is based on IPsec protocol suite [4] with multicast extensions [5]. IPsec protocols provide basic end-to-end security services: confidentiality, integrity, authentication, and replay protection. IPsec based approach can be used with different applications and on top of different IP multicast routing approaches. To enable connectivity over network segments without multicast support and to IPv4 private networks, tunnelling and Network Address Translation (NAT) techniques can be utilized.

For authentication, different Message Authentication Code (MAC) algorithms may be used for group authentication (to identify that the sender was within the group) or RSA signatures for source authentication (to identify actual sender). In addition to standardized RSA signature based IPsec authentication scheme, more efficient elliptic curve cryptography based signatures are recommended. To enable simultaneous group and source authentication – which is currently not possible in multicast IPsec - the framework proposes a new combined authentication model where IPsec authentication data field concatenates both group and source authentication data. The model enables better availability protection and use of authenticated encryption algorithms while at the same time providing protection against group insider threats.

The framework enables group access control as well as satellite resource protection. Group Domain of Interpretation protocol (GDOI) [6] is utilised for group key distribution: for pulling keys from the server and for pushing rekeys to the clients. Group keys are updated when members join or leave group – to enable forward and backward security. GDOI optimises use of satellite resources with rekey multicasting and hierarchical key management (Logical Key Hierarchy, LKH [7]). The framework uses IP Multimedia

System' Resource and Admission Control Subsystem [8] and Open IPTV Forum requirements [9] as guidelines to enable network resource reservations and development of secure content delivery applications.

4. Performance enhancements

The satellite channel causes several challenges for the communication, including long delays, high bit-bit-error rates, burst errors, and asymmetric capacity. Overloading and error situations may cause situations where group key distribution fails, which in turn makes services and communication unavailable. The following subsections propose mechanisms for accelerating the end-to-end secure communication as well as for improving robustness and efficiency of key delivery in satellite communications context.

4.1 Acceleration of end-to-end secured communication with trusted PEPs

The framework enables performance acceleration over encrypted connections with trusted performance enhancement proxies (trusted PEP). These are network components, which are allowed to intercept, decrypt, accelerate and again encrypt secure communication flow. Possible acceleration schemes for satellite context are e.g. Split TCP (unicast), Robust Header Compression (ROHC) and packet aggregation. Ordinary PEPs cannot operate on the secured connection as they cannot read or modify headers and data that has been encrypted and integrity protected. Trusted PEP is an extension to the PEP concept where PEPs are given memberships to multicast groups and thus they are given group keys, which they can use to access secured communication.

Trusted PEP can be used with group authenticated communication session. Distributed trusted PEPs (with a component on both sides of a satellite) may also be used in some source authenticated scenarios. However, trusted PEPs are not recommended for source authenticated communications where PEPs would be required to possess private keys of individual members.

Trusted PEPs are suitable for application scenarios where it is acceptable that a trusted party can intercept communication. The group owner, e.g. an application service provider, has a control what connections can be accelerated.

4.2 Optimized rekeying by coupling key hierarchies with satellite beams

To enable forward and backward security, key server must multicast a rekey message to a group each time a member joins or leaves. The rekey messages must be protected so that group communication is available only for authorized members. A straightforward and inefficient approach is to encrypt rekeying material with member specific keys and deliver protected rekeying material separately for each group member. For large groups, the rekeying costs can be optimized with key hierarchies and satellite network architecture based key delivery strategy. In key hierarchies, such as LKH, group key is secured with key chains, which are organized using a tree structure. Hierarchical models are more efficient as when a member leaves the group it suffices to send two key update messages for each node contained in the branch from the removed leaf node to the root of the tree. One message updates the parent key of a node that belongs to the branch, and one message updates the parent key of root node of some maximal subtree that does not contain any nodes from the branch. Thus the rekeying cost of leaves of one member is effectively logarithmic.

In satellite-beam based communication architecture, the key hierarchies can be further optimized by coupling the key hierarchies with members' location information – by creating an own key hierarchy for (members under) each beam. The beam-coupled hierarchy minimizes traffic as keys must be delivered only for those members that are under the beam. For instance, when considering a case where a single user leaving a group: the amount of transmissions of a new group key for one beam (of leaving user) is a logarithm taken from the member amount under the beam; the amount of transmissions for every other beam is one.

4.3 Prioritized key management

The loss of key management and rekey messages has more significant effects than the loss of ordinary application messages. E.g. a delayed or dropped rekey message may result in dropped application packets due to lack of up-to-date security associations as well as increased signalling load due to resulting key pull messages. Thus, the satellite network should try to improve the delivery success rate of the signalling messages by means of dedicated Radio Resource Management (RRM), e.g. in terms prioritization and less aggressive ACM.

Dedicated RRM for higher layer control messages requires the identification of higher layer control packet flows and dedicated packet handling in the satellite link protocol stacks, in both forward (DVB-S2) and return (DVB-RCS2) links. The identification utilizes DiffServ Code Point (DSCP) labelling and RRM is handled by means of a dedicated lower layer service configuration, prioritized packet scheduling and usage of the most robust MODCOD for the higher layer control messages.

4.4 Adaptive rekey repetition and prolonged key usage

Signal conditions for satellite beams may change within time, for example, due to weather conditions. Key servers, which are aware of satellite link status of each beam, may adapt their behaviour to minimize the rekeying related communication costs. When a server knows that a member is behind an unreliable or overloaded link, it can apply different transmissions procedures than it would normally apply for members behind high-capacity connections. Particularly, a key server may anticipate that a delivery of rekeying message fails with some probability. The server may then send rekey messages several times to beams with high failure rates and thus increase probability of successful key delivery. As a result, the server minimizes key requests from members and amount of (application) packets being dropped due to missing group keys. When amount of rekey messages increases the amount of keyless users and time of users without keys should decrease. However, when the size of a single rekey message is large (e.g. in the case where there are many users in a group), the costs of sending duplicate rekey messages may be significant. In these cases, the server should perform rekey repetitions in moderate manner.

The rekey repetition may be reactive or proactive. In the reactive case, a rekey message is repeated when bad signal conditions are detected. In the proactive case, the key server knows that signal conditions are going to change for worse it may send rekey push messages before the push was originally scheduled. For instance, the server may utilize weather forecasts to anticipate changes in signal conditions and need to send rekey messages in advance.

Another approach to minimize key management signalling is to *prolong the usage time of group keys* based on the satellite signal conditions i.e. to delay the change of group keys when the signal conditions are bad and to change to the new key when the signal conditions are good. The approach is suitable for non-asynchronous applications where there is one server that multicasts packets to clients behind the satellite and which is aware of the satellite link status. The scheme also limits backward secrecy as changes in the group become into effect only after a new key is in use.

5. Multicast security system demonstrator

One of the objectives of the study was to develop a demonstrator for validation of the secure multicast framework on top of multi-spot beam satellite network as well as the proposed enhancements for seamless integration. Network Simulator 3 (ns-3) [10] platform was selected as the base platform for the multicast secure system demonstrator. Justifications for the selection of ns-3 based simulative approach were the following:

- Lack of available real open-source key components in a sufficient maturity state or configurable off-the-shelf components, which should have served as the base line for further development for both multicast security and application components.
- Mature support for multi-spot beam satellite system in ns-3 (Satellite Network Simulator 3 - SNS3) [11] [12].
- Ns-3 provides the benefits of both system simulations (e.g., scalability, large simulation scenarios, system-wide performance analysis) and real-time emulations (attachment of real applications and protocols) [13].

The main components implemented to the ns-3 are:

- Key management client; including Internet Key Exchange (IKE), IP Security Quick Mode (QM) and GDOI client for all group members (GM)
- IP security with Multicast extensions for all IP security related nodes
- Group Controller Key Server (GCKS) responsible for handling the multicast group specific security credentials.
- Session Signalling Module (SSM) client and server handling the application layer signalling for secure application sessions. SSM is modelling OIPF connection management.
- Traffic models based on defined use cases; i.e., IPTV, collaborative working, and Internet-of-Things (IoT).

The demonstrator is capable of functioning in two modes; simulative (see Figure 2) and real-time emulative (see Figure 3). Both approaches utilize almost exactly the same code base apart from the applications and traffic generators.

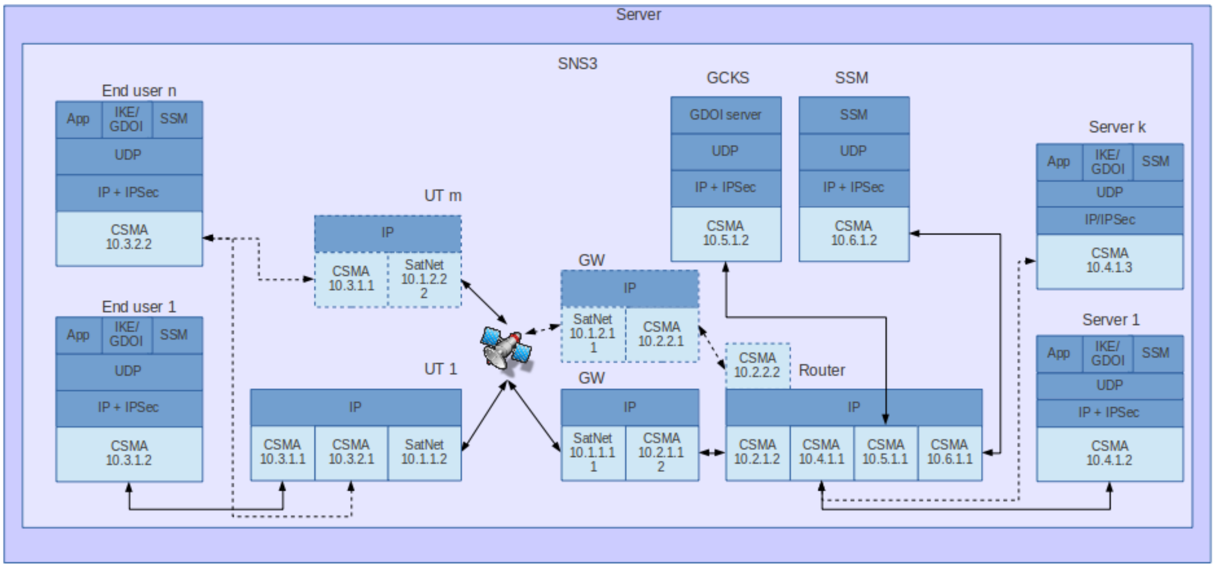

Figure 2. Simulative Multicast Security Demonstrator.

The fully simulated scenario (Figure 2) consists of only one simulation server, which is responsible for modelling the whole system from the satellite link and service/content provider domains to the end users. The scenario does not include real applications, but traffic models are utilised to model the application behaviour. The simulated scenario is capable of capturing system wide statistics from cases where there are, e.g., hundreds of end users. The simulated scenario shall be utilised to verify IPTV, collaborative working and IoT use cases.

The emulated scenario (Figure 3) consists of simulative component(s) running in real-time and several test bed components with real service applications. The environment consists of three nodes: one simulation server machine modelling the satellite network and service/content provider domains, and two laptops modelling the actual end users attached to the User Terminals. The emulated use case captures the effect of secure multicast based service on top of satellite network from the real application point of view. The emulated scenario is utilised to verify the IPTV use case with a Python based User Interface (UI) and VideoLAN client (VLC) as content server and client.

The demonstrator will be able to produce several Key Performance Indicators (KPI), such as application throughput, the signalling load, number of successful rekeys, and rate of packets dropped by the security suite. These KPIs will form the basis of performance analysis and evaluation of the multicast security architecture in this study.

6. Application use cases

6.1 IPTV

The Open IPTV Forum (OIPF) Functional Architecture from [9] is used as baseline for the demonstrated IPTV use case. Besides the nodes which are directly adjacent to the satellite network component, the use case makes use of 4 types of nodes: service provider (a.k.a., the sender), terminal (a.k.a., the receiver), service platform provider and the key server. The demonstrator service provider (SP) is located in IPTV SP/CP domain, OITF TV consumer domain represents a terminal, service platform provider (SPP) and key server (GCKS) nodes are located in Network and Platform Provider domain together with satellite component (SNS3) nodes (UT, GW and Router).

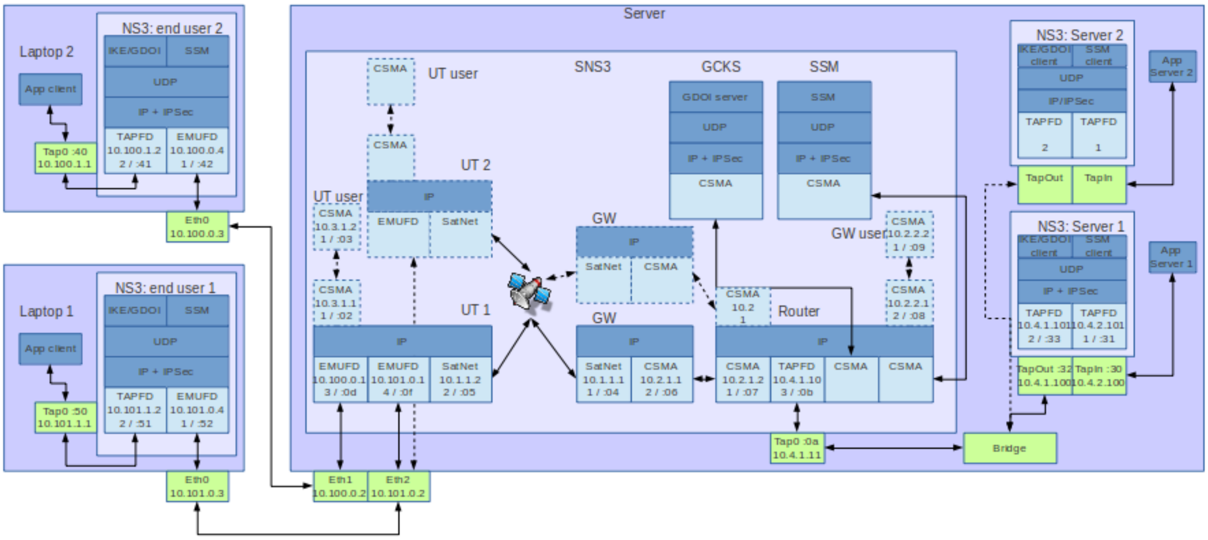

Figure 3. Emulative Multicast Security Demonstrator.

6.2 Collaborative working (CoW)

Besides the key server and satellite component nodes (GW, UT and Router), the network topology in collaborative working use case utilizes another centralized node named the portal server. The decentralized approach is not considered.

The portal server contains, in addition to the required IPsec and GDOI security functionality, a collaborative working server application. This application handles the simplified authentication of the users, i.e., no real passwords are used, but the request-response transaction is modelled. Once the client has successfully authenticated with the portal server, it can initiate the key exchange for the required encryption keys.

Additionally, the server is responsible for securely transferring the collaborative working data from the presenting clients to the group participants. It is assumed that the server does not reprocess or modify the data it shares again with the participants.

6.3 Internet of Things (IoT)

Architecturally the IoT use case resembles CoW use case closely: the portal server is replaced by M2M automated service and the clients are replaced by IoT gateways. IoT gateways have joined a multicast group, so M2M automated service requesting sensor data can get the data from multiple locations as a response from multiple IoT gateways.

The use case implementation does not model the communication protocol between the sensor nodes and IoT gateway as the said protocol can be implementation or vendor specific. Additionally, a more special IoT protocol, such as CoAP, is not implemented, but IoT gateways and the automated service communicate directly over UDP.

7. Simulation results

In this section we present preliminary simulation results from the demonstrator. The simulation case consists of in total 200 end users/group members with IP security with Multicast extensions, one GCKS, GDOI key management, session signalling, and Multicast IP-TV traffic in forward link.

7.1 Dedicated higher layer control message radio resource management

The simulation results in Figure 4 show the benefits of dedicated radio resource management for HL control messages. The HL control packets are both prioritized as well they are using the most robust MODCOD/waveform in both directions. The success rate of the signalling procedures is increased and the signalling load is reduced due to reduced retransmissions. The achieved gains depend on the assumed satellite channel models (e.g. stationary or mobile users).

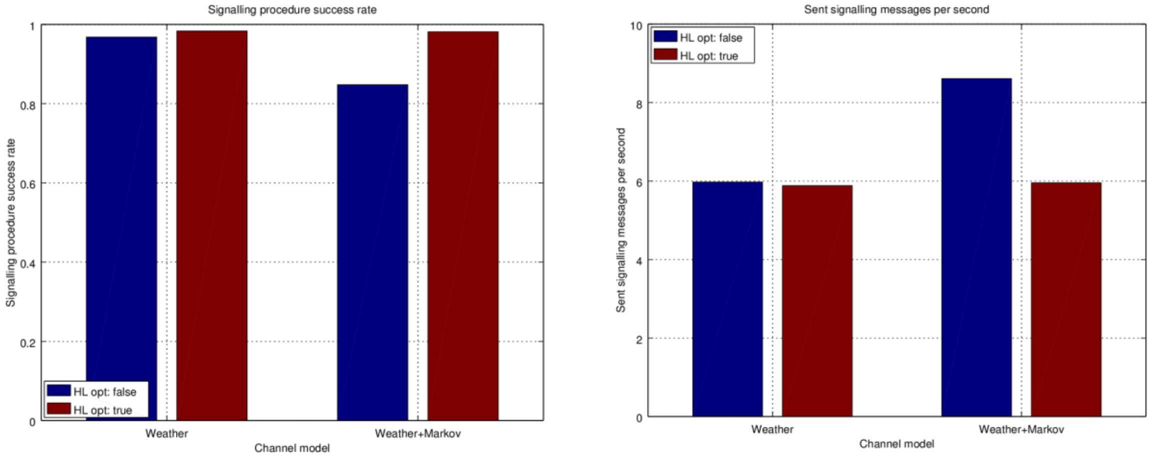

Figure 4. Effect of HL signalling message prioritization and MODCOD.
a) Signalling procedure success rate. b) Signalling load.

7.2 Backward and forward security with Logical Key Hierarchy

Figure 5 presents the signalling load with different key management options (PW = pairwise keys, P=periodic, B=backward security, F=forward security). Basic pairwise keys of course provides the lowest signalling load, but it lacks both periodic updates and forward and backward security. Periodic security is by no means reasonable with only pairwise keys due to increase unicast signalling load. LKH provides both forward and backward security with quite reasonable signalling load.

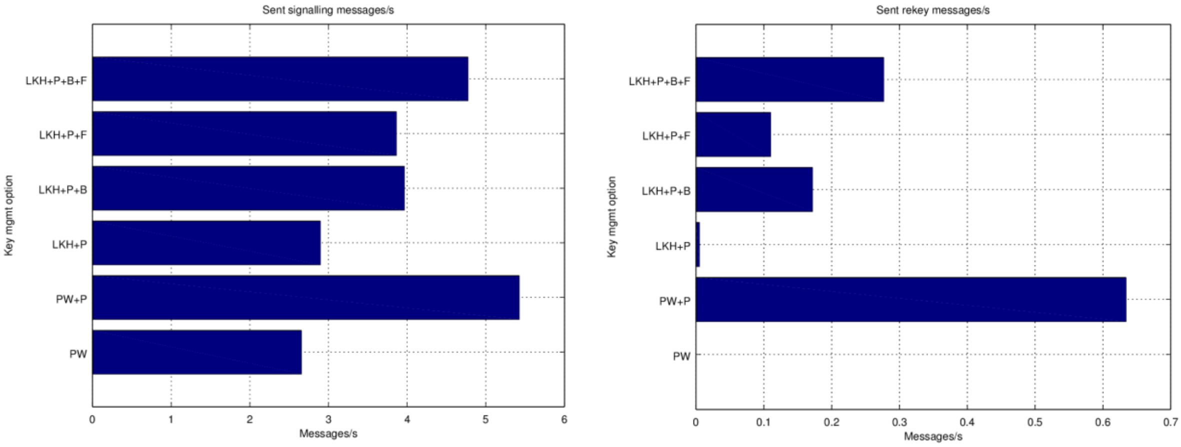

Figure 5. Effect of key management options.

a) Sent signalling messages. b) Sent push messages.

8. Conclusions

This article presented an overview of a secure multicast framework as well as a secure multicast system demonstrator used for end-to-end performance assessment of secure multicast service delivery. The security framework relies on IP security with multicast extensions and Group Domain of Interpretation (GDOI) multicast key management. The framework addresses challenges in the delivery of secure multicast services on top of multi-spot beam satellite networks by proposing several enhancements to overcome the bottlenecks. The enhancements include Trusted Performance Enhancement Proxies (trusted PEP), coupling of LHK trees with satellite network architecture, dedicated Radio Resource Management (RRM) for key management packets and rekey redundancy by means of repetition and lifetime prolonging. Preliminary simulation results have been included to show the benefits of higher layer control message prioritization and LKH. The demonstrator can be utilised in the future to test real secure applications on top of simulated/emulated satellite link.

9. Acknowledgements

This work has been funded by European Space Agency in the scope of ARTES 5.1 AO7476 Network Security on Multi-Spot Beam Broadband Networks for Multicast Based Interactive Systems project (contract no: 4000109719/13/NL/EM).

10. References

[1] ETSI, “EN 301 545-2; Digital Video Broadcasting (DVB); Second Generation DVB Interactive Satellite System (DVB-RCS2); Part 2: Lower Layers for Satellite standard,” 2012.

[2] ETSI, “EN 302 307; Digital Video Broadcasting (DVB); Second generation framing structure, channel coding and modulation systems for Broadcasting, Interactive Services, News Gathering and other broadband satellite applications (DVB-S2),” 2009.

[3] ETSI EN 302 307-2 V1.1.1 (2014-10), “Digital video broadcasting (DVB); second generation framing structure, channel coding and modulation systems for broadcasting, interactive services, news gathering and other broad-band satellite applications. Part 2: DVB-S2 Extensions (DVB-S2X).

[4] S. Kent and K. Seo, “Security Architecture for the Internet Protocol,” IETF specification, RFC 4301, 2005, http://tools.ietf.org/html/rfc4301.

[5] B. Weis, G. Gross, and D. Ignjatic, “Multicast Extensions to the Security Architecture for the Internet Protocol,” IETF specification, RFC 5374, 2008, http://tools.ietf.org/html/rfc5374.

[6] B. Weis, S. Rowles, and T. Hardjono, “The Group Domain of Interpretation,” IETF specification, RFC 6407, 2011, http://tools.ietf.org/html/rfc6407.

[7] Wallner, D., Harder, E. & Agee, R. Key Management for Multicast: Issues and Architectures. IETF specification. RFC 2627. 1999. http://tools.ietf.org/html/rfc2627.

[8] European Telecommunications Standards Institute. ETSI ES 282 003 V2.0.0. Resource and Admission Control Sub-System (RACS): Functional Architecture. 2008. http://www.etsi.org/deliver/etsi_es/282000_282099/282003/02.00.00_60/es_282003v020000p.pdf

[9] Open IPTV Forum, “Functional Architecture,” Release 2 specifications, V2.3, 2014, http://www.oipf.tv/specifications/.

[10] Network Simulator 3 (ns-3), https://www.nsnam.org/.

[11] J. Puttonen, S. Rantanen, F. Laakso, J. Kurjenniemi, K. Aho, and G. Acar, “Satellite Model for Network Simulator 3,” in International Conference on Simulation Tools and Techniques (SIMUTools), Lisbon, Portugal, 2014.

[12] J. Puttonen, S. Rantanen, F. Laakso, J. Kurjenniemi, K. Aho, and G. Acar, “A Packet Level Simulator for Future Satellite Communications Research,” in AIAA International Communications Satellite Systems Conference (ICSSC), San Diego, USA, 2014.

[13] V. Hytönen, B. Herman, J. Puttonen, S. Rantanen, and J. Kurjenniemi, “Satellite Network Emulation with Network Simulator 3,” in Ka and Broadband Communications, Navigation and Earth Observation Conference, Salerno/Vietri, Italy, 2014.