PEP architecture for Broadband Satellite Multimedia (BSM) networks

H. Cruickshank¹, R. Mort², M. Berioli³

Abstract— Satellites had been successful in the past due to their wide area coverage and speedy deployment of new services especially in remote regions of Europe and the rest of the world. The future development of broadband satellite systems providing services based on the Internet Protocol (IP) needs to be stimulated by means of common standards. This paper presents the ETSI BSM PEP architecture which includes the satellite terminal protocol stack, PEP usage scenarios and security configurations for successful PEP implementations.

Index Terms— PEP, SI-SAP, TCP, BSM.

I. INTRODUCTION

The development of broadband satellite systems providing services based on the Internet Protocol (IP) needs to be stimulated by means of common standards. These standards will allow building blocks and services for such satellite systems to become more readily available. The ETSI Broadband Satellite Multimedia (BSM) working group ensures that this work can be carried out in a timescale that will allow development of universal access to everyone, everywhere via a combination of private and public internet access points.

The BSM work is focussed on the efficient transport of IP data streams and on how to interoperate resulting satellite networks with terrestrial IP networks. The BSM standards are being designed to use existing standards (such as DVB-RCS [1]) while remaining open to emerging standards and other available technologies (the ultimate choice is left to the market). This paper presents on the current work in defining the PEP architecture for BSM satellite networks.

In general, the Internet transport protocol (namely TCP) exhibits suboptimal performance due to the following satellite characteristics:

- Long feedback loops: Propagation delay from a sender to a receiver in a geosynchronous satellite network can range from 240 to 280 milliseconds. This will cause slow connection setup, slow to respond to loss and slow discovery of available bandwidth.
- Large bandwidth*delay products: TCP needs to keep a large number of packets "in flight" in order to fully utilize the satellite link.
- Asymmetric capacity: The return link capacity for carrying ACKs can have a significant impact on TCP performance.

One solution to the above problem is implementing a TCP Performance Enhancing Proxy (PEP). Among the TCP PEP proposals, one solution is represented by the splitting approach [2] and [3]. The rationale of the splitting concept is to separate the satellite portion from the rest of the network. In addition to TCP PEPs, there are other complementary solutions such as application layer PEPs, which implement techniques such as data and header compression algorithms; HTTP acceleration (with caching and web page objects prefetching) and DNS caching techniques. Commercial PEPs normally combined some/all these techniques together such the XipLink [4], FastSat [5] and Hughes [6] PEPs. Of course, end-to-end improvements techniques to TCP and web HTTP can be used as well. However, they are not the focus of this paper.

The aim of the current work on PEPs in the Specific Task Force (STF) 344 in ETSI BSM is to describe the current solutions for PEPs in broadband multimedia satellite systems. The range of PEPs considered includes TCP accelerators, TCP header

¹ CCSR, University of Surrey, Guildford, UK
² SysTek, Havant, UK
³ German aerospace center (DLR), Munich, Germany
compression and HTTP proxies. The PEPs are classified in terms of ease of implementation, interworking capability with other PEPs and performance potential. The work also includes an analysis of the various PEP types/mechanisms and recommendations for the use of these PEPs in BSM networks.

This paper is organized as follows: Section II provides an overview of current ETSI BSM architecture. Section III presents the Satellite Terminal (ST) and Gateway (GW) PEP architecture. Section IV presents distributed and integrated PEP scenarios. Section V describes the security implications of using PEPs. Finally section VI concludes this work with a summary and outlook on related work at ETSM BSM group.

II. OVERVIEW OF BSM ARCHITECTURE

The BSM architecture, [7], [8] and [9] is presented in Figure 1 with the general BSM protocol stack for IP services in the Satellite Terminals (ST) and the Gateways (GW). An important feature is the Satellite Independent Service Access Point interface or SI-SAP interface. This interface provides the BSM with a layer of abstraction for the lower layer functions. It allows the BSM protocols developed in the satellite independent layer to perform over any BSM family (specific satellite technologies). Moreover, the SI-SAP also enables the use of standard Internet protocols for example address resolution, QoS, security and network management, directly over the BSM or with minimal adaptation to BSM physical characteristics. Finally the SI-SAP even makes it possible to envisage switching from one satellite system to another and to even a non-satellite technology while preserving the BSM operator's investment in layer 3 software development.

In addition, Figure 1 shows that there are only a small number of generic functions that need to cross the SI-SAP and those are related to connection/session management, resource management or security. The BSM protocols are based on the OSI layered protocol stack. For the IP services most of the work has concentrated on the network layers with links to the underlying data link and Media Access Control (MAC) layers. The reason for this is simple: the developed protocols for IP over BSM should primarily be located in the satellite independent part of the BSM stack to be applicable to a range of different satellite dependent lower layers such as DVB-RCS [1].

Although not shown in Figure 1, this BSM architecture is directly applicable to PEP designs. If the PEP design adopts a satellite-independent approach it can be used with different lower layers without requirement significant redevelopment. This has benefits for both the PEP manufacturers (by reducing the new costs and time of new developments) and also for the end-user who can migrate to a new satellite system while retaining the same or similar “known” PEP properties.

![Figure 1: BSM Protocol Stack](image-url)
Figure 1 also shows that the SI-SAP is further divided into user (SI-U-SAP), control (SI-C-SAP) and management (SI-M-SAP) interfaces. These are used for user data, connection control and network management respectively. The PEP data will use the SI-U-SAP, while related QoS signalling and management functions will use the SI-C-SAP and SI-M-SAP interfaces respectively.

III. PEP TERMINAL ARCHITECTURE AND COMPONENTS

Figure 2 and Figure 3 show the combined PEP protocol stack with the BSM ST and Gateway terminal architectures respectively.

The PEP residing on the BSM ST side is called ST PEP (PEP client) and the one on the BSM gateway side is called Gateway PEP (PEP server). Both PEPs have a similar architecture with two interfaces, one to the BSM satellite network and one to terrestrial networks. On the satellite network sides, the ST/Gateway PEP are connected to BSM ST/Gateway through an Ethernet LAN. However, the Gateway PEP can be located remotely from the BSM Gateway terminal (such as Gateway PEP run...
by a service provider), more detailed are presented in section IV. On the terrestrial network side, normally, the PEP terminal connects to hosts on the same LAN, while the gateway PEP connects to a content server through the general Internet.

The transport protocol in the PEP is divided between standard TCP/UDP and PEP specific transport protocols. The PEP specific transport protocol can be:

- A modified TCP (TCP+) such as the Hypla protocols [10], which is used in integrated PEP configurations, where only Gateway PEP will be used (no ST PEP).
- Standards I-PEP Transport Protocol (I-PEP TP) [11], recommended by the I-Labs and used in the distributed PEP configurations. The I-PEP TP is based on an extension set to TCP termed SCPS-TP, which was produced by the Consultative Committee for Space Data Systems (CCSDS).
- Proprietary distributed Transport Protocol (TP+), where other company specific (non-standard) protocols are used.

The ST/Gateway PEPs can be managed either locally or remotely. For remote management, either SNMP or HTTP protocols can be used to communicate with the BSM management system. In both cases the PEP monitoring and configuration controls can be based on the standard MIB II and enterprise specific PEP MIBs.

Also both figures show the QoS signalling between the PEP and the BSM QoS managers in the ST and Gateway. Such signalling is necessary for QoS monitoring of the ST/Gateway queues and adjusting rate control parameters accordingly to maximize the use of the satellite capacity. The optimum PEP performance is expected to require a close matching between the PEP configuration and the QoS of the associated lower layer bearer services. This signalling can be based on IntServ or DiffServ architectures [12] and [13].

IV. BSM PEP SCENARIOS

Several PEP usage scenarios are presented here and it follows the Satlabs recommendations [11]. All scenarios apply to both star and mesh satellite topologies.

A. Scenario 1: Single user

Figure 4 shows the single user scenario, where there is a clear one-to-one mapping between users and PEP clients (ST PEP). The multi-user scenario expands beyond the single user variant in that several application clients are served by the same PEP client.

This reflects the typical home user or home office scenario. The PEP client may be integrated with the BSM ST, or it may be a stand-alone entity separate from both the end user’s device and the ST.

B. Scenario 2: Independent satellite and PEP gateways

Scenario 1, assumed that the PEP server (Gateway PEP) is co-located with the BSM Gateway (which implies that the satellite service provider either operates the PEP or provides at least hosting facilities for the respective system components). In scenario...
2, the PEP server is external to the BSM Gateway (see Figure 5), motivating two different set-ups:

- PEP server may be run by a separate Internet Service Provider (ISP) on behalf of many users or
- PEP server may be operated by an enterprise on its own behalf.

The primary differences between scenario 1 and scenario 2 are as follows:

- The communication link between the PEP server and BSM Gateway now extends through a wide area network that is not trusted and the satellite service provider may also not be trusted. A typical connection will be an IP tunnel (possibly with IPsec).
- Addressing schemes for PEP clients and BSM Gateway may be controlled by two different institutions.

![Figure 5 Scenario 2: Independent Gateway PEP from BSM Gateway](image)

### C. Scenario 3: Multiple PEP Gateways

In this scenario, there is no longer a single “centralized” Gateway PEP. Instead, multiple Gateway PEPs are used: either due to the presence of multiple ISPs or because performance enhancement is managed directly between user sites (VPN configuration). In comparison to scenario 2, the PEP client needs to interoperate with multiple PEP servers from different vendors. This is an ideal setup for using the I-PEP protocol [11] mentioned in section III.

This scenario is depicted in Figure 6 and it is useful in cases where a remote terminal, has an IP tunnel for enterprise communications as well as a direct Internet connection for general communications. PEP acceleration is required for both and can only be operated independently.

![Figure 6 Scenario 3: ST PEP accessing multiple Gateway PEPs](image)
D. Scenario 4: Integrated PEP

The previous three scenarios showed various aspect of a distributed PEP (PEP client and server at both ends of the satellite link, like the ST and Gateway PEPs). Scenario 4 shows an example of an integrated PEP (see Figure 7).

![Figure 7 Scenario 4: Integrated PEP implemented at the BSM Gateway](image)

Here the TCP connection established among the end hosts, is split in two separated connections, with the integrated PEP at the BSM Gateway. The first connection (between the web server and the integrated PEP makes use of the TCP standard and is terminated at the PEP. The second connection, between PEP and the final user, can exploit an enhanced TCP version compatible with a standard TCP receiver (such as the Hypla protocols [10] mentioned in section III). In comparison to the distributed PEPs scenarios, integrated PEP is simpler but has limited enhancement capabilities.

V. SECURITY IMPACT ON PERFORMANCE ENHANCING PROXIES (PEPs)

There is a requirement that security must be implemented in such away that allows PEP entity (ST or Gateway) access to the transport protocol headers (such as TCP). Thus there are some security implications for using PEP in satellite environment. The most negative implication of breaking the end-to-end semantics of a connection is that it disables end-to-end use of IPsec.

![Figure 8 Successful PEPs with satellite link security](image)

In general, a user or network administrator must choose between using PEPs or using IPsec. If IPsec is employed end-to-end, PEPs that are implemented on intermediate satellite nodes in the network cannot examine the transport or application headers of IP packets, because encryption of IP packets via IPsec's ESP header (in either transport or tunnel mode) renders the TCP header and payload unintelligible to the PEPs. Without being able to examine the transport or application headers, the PEP may not
However there are some steps which can be taken to allow the use of IPsec and PEPs to coexist. If an end user can select the use of IPsec for some traffic and not for other traffic, PEP processing can be applied to the traffic sent without IPsec. Another alternative is to implement IPsec over the satellite link between the two PEPs of a distributed PEP implementation. This at least protects the traffic between the two PEPs.

As shown in Figure 8, PEPs can be used successfully with IPsec in tunnel mode between the BSM ST/Gateway. Here the encryption is performed on incoming traffic after the PEP operations and decryption is performed on outgoing traffic before the PEP operations. Similarly, a link layer security mechanism can be used such as DVB-RCS [1] security or Unidirectional Link Encapsulation (ULE) security [16].

Also end-to-end security can be implemented successfully with PEPs as shown in Figure 9. Here security must be implemented above the transport layer such as Secure Socket Layer (SSL) or application layer security. However, this will not work with web acceleration and it has to be disabled.

Thus the requirement is that security must be implemented in such away that allows PEP entity access to the transport protocol headers (such as TCP). Therefore link and application layer security are transparent to PEPs. If IPsec is used, then PEP operations must be performed outside the IPsec processing. Further information about PEPs and security issues over satellites is provided in [14] and [15].

VI. CONCLUSION

The ETSI BSM standardisation work is focussed on the efficient transport of IP data streams and on how to interoperate resulting satellite networks with terrestrial IP networks. The paper presented the current work in ETSI BSM group in defining the PEP architecture for BSM networks. The ST and Gateway PEP protocol stack has been shown together to some configuration scenarios for distributed and integrated PEPs. The paper shows that PEPs have the potential to improved TCP and web performance over BSM network.

However, security implications must be taken into account. Two possible security solutions are presented to solve this problem, one for securing the satellite link only with either IPsec (tunnel mode) or link layer security such as ULE security, the other is deploying end-to-end security using SSL (or TLS) and application specific security systems.

Future related work in ETSI BSM will analyse various PEP types and mechanisms make recommendations for best usage of PEPs in BSM networks. In addition PEP improvements will be compared to end-to-end techniques for TCP (such as increasing transmission window, selective acknowledgements and timestamps) and for applications layer (such as improving HTTP 1.1 and
Finally, interworking between BSM PEPs entities and BSM management and QoS entities will be analysed.

ACKNOWLEDGEMENT

This work was sponsored by the European Telecommunications Standards Institute (ETSI) [17] and supported by the EU Information Society Technologies SATNEX project [18], plus the European Free Trade Association (EFTA) [19].

REFERENCES

[12] ETSI TS 102 463: “Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM); Interworking with IntServ QoS”.
[13] ETSI TS 102 464: “Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM); Interworking with DifServ QoS”.
[18] Satnex project home page: http://www.satnex.de
[19] European Free Trade Association (EFTA): http://www.efta.int/