Secured VPN Models for LTE Backhaul Networks

Madhusanka Liyanage, Andrei Gurtov
Centre for Wireless Communications
University of Oulu, P.O. Box 4500, FI-90014 Oulu, Finland
Email: [madhusanka, gurtov]@ee.oulu.fi

***Abstract*—The Long Term Evolution (LTE) architecture proposes a flat all-IP backhaul network. 3rd Generation Partnership Project (3GPP) specified new security and traffic transport requirements of new LTE backhaul network. However, existing LTE backhaul traffic architectures are incapable of achieving these security requirements.**

In this paper, we propose two secured Virtual Private Network (VPN) architectures for LTE backhaul. Both architectures are layer 3 Internet Protocol security (IPsec) VPNs which are built using Internet Key exchange version 2 (IKEv2) and Host Identity Protocol (HIP). They are capable of fulfilling 3GPP security requirements such as user authentication, user authorization, payload encryption, privacy protection and IP based attack prevention. We study various IP based attacks on LTE backhaul and our proposed architectures can protect the backhaul network from them.

I. Introduction

Affordable, truly accessible mobile broadband has matured with HSPA (High Speed Packet Access), HSPA+ and LTE/LTE-A will be used in the near future. However, the LTE architecture proposes a flat all-IP backhaul network. Furthermore, new security and traffic transport requirements of LTE backhaul are specified by 3GPP. The motivation of this research is to identify these security challenges of the LTE backhaul and to provide a secured backhaul traffic architecture.

Additionally, various types of traffic will be transported by the LTE backhaul starting from evolved nodeBs (eNBs), such as S1-U traffic to the Service Gateway (SGW), S1-C traffic to the Mobility Management Entity (MME), X2-U and X2-C traffic to other eNBs etc [1]. There are two crucial traffic transport issues identified due to these heterogeneous traffics. First issue is to backhaul different traffics in to the correct destination. Second problem is to provide different levels of Quality of Service (QoS), priority and fault management requirements for different traffic types. A VPN based backhaul traffic architecture is a promising solution to fix above issues.

Therefore, we propose two IPsec VPN architectures not only to fulfill LTE backhaul security requirements but also to solve the above traffic transport problems. This is the first secured VPN architecture proposal for the LTE backhaul network. Our first architecture is an IPsec tunnel mode VPN which is built using IKEv2. Second architecture is an IPsec BEET (Bound End-to-End Tunnel) mode VPN which is built using HIP. Both architectures are able to secure the backhaul traffic by fulfilling 3GPP security requirements for LTE backhaul such as user authentication, authorization, payload encryption, privacy protection and IP based attack prevention.

The rest of the paper is organized as follows. Related work is mentioned in Section II.The background of LTE backhaul network and used protocols are presented in Section III. The proposed VPN architectures are described in Section IV. We discuss our simulation model and the results in Section V. Section VI and VII respectively contain the discussion and conclusions of the research.

II. Related work

All-IP LTE backhaul needs to satisfy several architectural requirements such as traffic transportation, mobility management, security etc. A summary of these requirements can be found in [1] [2]. Furthermore, the network operators will be encountered a number of migration challenges when they move from the existing 2G/3G backhaul to a LTE backhaul and these challenges are detailed in [3] [4] [5]. A thorough understanding of these requirements and issues ensures operators to choose the right technology, network topology and architecture to implement a successful LTE backhaul network [4].

The backhaul network security is one of the key challenges of the future LTE architecture. Mutual authentication of eNBs and IP attack prevention are required for steady operation of the LTE backhaul. Further, 3GPP specification demands to encrypt data and signaling traffic when the use of an untrusted network. However, LTE backhaul is lacking of these security requirements. Therefore, LTE backhaul traffic should be secured by the upper layer techniques [1].

Multiple types of traffics will be transported in LTE backhaul. Thus, proper backhauling of the different traffics and providing different levels of QoS, priority levels are challenging for network operators. Various layer 2 and layer 3 VPN architectures can be used to overcome these issues [2] [1]. In [2], authors presented the advantages and disadvantages of different layer 2 and layer 3 VPN architectures for LTE backhaul.

VPN based backhaul traffic architecture is a promising exemplary to model the LTE backhaul traffic. It can be modeled as a layer 2 VLAN or as a layer 3 VPN. However, moving from a pure layer 2 topology to a full layer 3 VPN architecture has more advantages such as less complexity, flexibility and scalability [3].

However, above VPN proposals for LTE backhaul are not accounting the security requirements of LTE backhaul. Hence, a secured VPN architecture for the LTE backhaul is a novel and well-timed research topic.

III. Background

A. LTE Mobile Backhaul Network

LTE transport network contains three sections, namely radio access, backhaul and core network. Among them, the backhaul network can subdivided in to access network and aggregation network. Hence, the backhaul network extends from the first transport equipment connecting cell sites (e.g. eNBs sites) to the transport aggregation equipment connecting central sites (e.g., SGWs/MME sites) [3]. In addition, several transport interfaces (e.g. S1,X2) are also belong to the backhaul network.

1) Security issues and protection requirements of LTE backhaul: LTE is about evolving to all-IP architecture. This evolution introduces several security ricks to the LTE backhaul. Three main reasons have been identified for such security risks [1] [2].

First, the LTE backhaul consists of the IP-based control /service elements (MME, SGW,eNBs) and interfaces (X2,S1). As a result, there is a possibility of several breaches and IP based attacks to the backhaul. For instance, an IP based attack which initiates in access network could affect the core gateways directly. However, such risks were never seen in previous non IP mobile backhauls.

Second, LTE backhaul network is now a carrier Ethernet environment with hundreds or thousands of end users (eNBs). Each node may have different level of security and these end nodes provide plenty of potential entry points for intruders. Thus, it is important to implement all network security features by considering the LTE backhaul as a public network.

Third, LTE backhaul does not have built-in security in bearer data as it is the case with 2G/3G networks. Prior to the LTE evolution, traffics in backhaul network secured by radio network layer protocols. However, the air interface encryption of user plane traffic will be terminated at the eNBs in LTE architecture. LTE backhaul traffic can be eavesdropped by unauthorized users. Hence, there is a requirement in the 3GPP standard [1], to encrypt both signaling and data traffic in backhaul network.

B. IP security (IPsec)

IPsec is a protocol suite for securing IP traffic of a network. IPsec defines two new protocols; Authentication Header (AH) and Encapsulating Security Payload (ESP) [6]. AH protocol ensures the authenticity of an IP packet. ESP protocol ensures the authenticity and additionally encrypts the IP packet.

IPsec has three modes of operation. First, transport mode of operation, the original IP header is retained and the IPsec header is inserted between the IP header and the header of a higher layer transport protocol. Second, tunnel mode of operation, the entire IP packet is encapsulated in another IP datagram and an IPsec header is inserted between the outer and inner IP headers [6]. Third, Bound End-to-End Tunnel (BEET) mode of operation, it is a combination of transport and tunnel modes. IPsec tunnel mode uses two pair of addresses; outer addresses for wire and inner addresses for application. As inner addresses are fixed for the life time of a Security Association (SA), BEET mode left out of transmitting them in packet headers [7] .

C. Host Identity Protocol (HIP)

Host Identity Protocol (HIP) is a new security and mobility protocol standardized by IETF(Internet Engineering Task Force) [8]. It separates the end-point identifier and the locater roles of IP addresses. HIP introduces a new layer to the TCP/IP model and it operates in between the transport layer and the internetworking layer. HIP defines a new Host Identity (HI) name space based on a public key security infrastructure and it will be considered as end-point identifier. 128-bit hash of HI is called as Host Identity Tag (HIT) and HIT is used by the upper layer applications. Hence, typical IP addresses will be used only for the locater role.

HIP nodes follow an initial procedure called Base Exchange (BEX) before the data transfer. BEX is a four-way handshake between users in order to exchange SAs and mutually authenticate each other [8]. This will establish an IPsec BEET mode tunnel between users for communication.

IV. Secure Backhaul VPN architectures

A. IPsec tunnel mode VPN architecture

Our first proposal is a layer 3 IPsec tunnel mode VPN architecture. It uses IKEv2 protocol to exchange SAs which need to build IPsec tunnels. The operation of our VPN architecture is as follows.

A potential user must contact an existing VPN user to get joined to a VPN. Our architecture uses an IP address based access control mechanism. Hence, there is an Authorization Server (AS) which is responsible for IP address based access control. Existing VPN user needs to acquire the permission from this AS to grant the access for the new user. Every VPN user maintains a permanent IPsec tunnel to an AS for this purpose. Furthermore, we are proposing a distributed AS system to avoid a single point of failure and to provide a quick access control service.

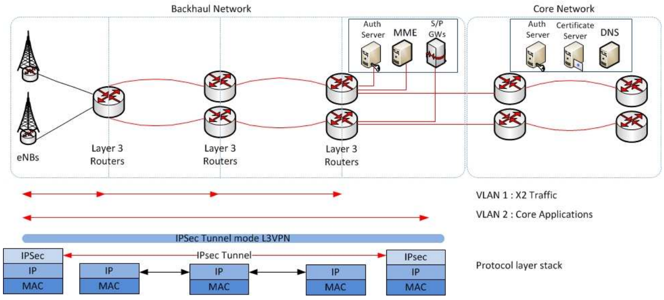

Fig. 1: The protocol stack of IPSec/IKEv2 VPN

Figure 1 exhibits the protocol stack of our architecture. In this case, there are two VPNs used; one for the traffic towards the core networks and the other for X2 interface.

Further, it is important to distinguish the different traffic types into different VPNs at end nodes (eNBs,MME etc).

Thus, we use a separate logical interface with a unique IP for each VPN.

Generally, backhaul nodes are static. Therefore, our architecture keeps longer IPsec tunnels and schedules rekeying event every 15 minutes to secure the connection. In a case of IP addresses change of the backhaul nodes, operators have to update the access control lists in AS. Then users rebuild the IPsec tunnels using new IP addresses.

Furthermore, several modifications are proposed to the IKEv2 and figure 2 illustrates the modified message exchange. Here, the initiator is the potential node to be joined and responder is an existing node of the VPN.

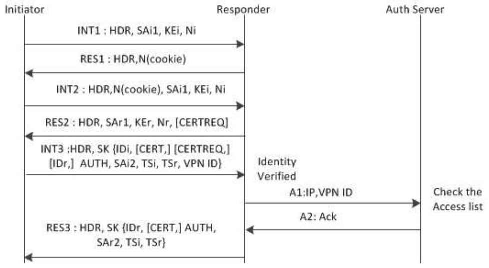
Initiator
Responder
Auth Server
INT1 : HDR, SAi1, KEi, Ni
RES1 : HDR,N(cookie)
INT2 : HDR,N(cookie), SAi1, KEi, Ni
RES2 : HDR, SAr1, KEr, Nr, [CERTREQ]
INT3 :HDR, SK {IDi, [CERT,] [CERTREQ,] [IDr,] AUTH, SAi2, TSi, TSr, VPN ID}
Identity Verified
A1:IP,VPN ID
Check the Access list
A2: Ack
RES3 : HDR, SK {IDr, [CERT,] AUTH, SAr2, TSi, TSr}

Fig. 2: The modified IKEv2 protocol

First five message exchanges are similar to the original IKEv2 messages with DoS (Denial-of-Service) attack protection. However, the message I3 is modified and it contains the potential VPN ID of the initiator. The identity of the initiator is verified after the arrival of I3 packet. Then responder sends an A1 packet to AS and it contains the IP address of initiator and his potential VPN ID. AS checks the access control list of the VPN and it will send an A2 packet to responder which contains an acknowledgement. A positive acknowledgement will grant the access and a negative acknowledgement will discard the connection request.

B. *IPsec BEET mode VPN architecture*

Our second solution proposes a layer 3 VPN architecture based on HIP protocol. HIP is used to create IPsec BEET based VPNs overlaid on top of the backhaul network. The basic model, backhaul element requirements and authorization procedure are similar to previous architecture. However, there are two main changes in this architecture. First, the access control is checked by using HI of the users and second, IPsec BEET tunnels (HIP tunnels) will be built using HI instead of IP address based IPsec tunnels. Hence the underline protocol stack is different and figure 3 illustrates it.

We use a separate logical interface with a unique HI for each VPN at the end nodes to distinguish the different VPN traffics. We keep longer HIP tunnels and schedule rekeying event every 15 minutes. On the other hand, the IP address changes of the backhaul nodes will not affect the existing VPN tunnels or access control lists in AS, because they are built using HIs instead of IP.

Furthermore, several modifications are proposed to the existing HIP base exchange (BEX). Figure 4 illustrates the modified BEX.

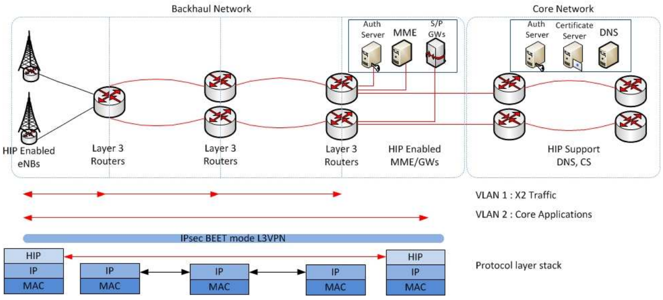

Fig. 3: The protocol stack of HIP VPN

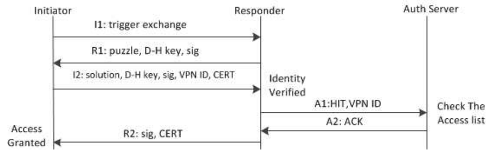

Fig. 4: The modified HIP BEX

First 3 message exchanges are similar to the original HIP BEX proposed in [8]. However, message I2 contains the potential VPN ID of the initiator. HIT based authorization is sufficient enough to avoid spoofing attacks. Even if an attacker is able to generate a valid HIT, it would fail to complete the initial BEX due to lack of knowledge of the private key [9]. Addionally, a trusted third party certificates can be included in I2 for further verification of the HI. Rest of the authorization message exchange procedure with AS is similar to previous architecture.

V. Numerical results

We implement our VPN architectures on MATLab and conduct several extended simulations to study the performance under DoS(Denial-of-Service), DDoS(Distributed DoS) and TCP reset attacks. We use a Transport Layer Security (TLS)/Secure Sockets Layer (SSL) VPN as our reference. TLS/SSL VPN is a layer 4 secured VPN. However it does not provide any layer 3 protection which is equivalent to the existing LTE backhaul traffic architectures.

A. *Impact of DoS Attack*

TCP SYN (synchronization) packet flooding attack is used as the DoS attack model. Our system model contains a single VPN which has 60 nodes and a server. All nodes upload traffic to the server and this server is under attack. It is equivalent to the upload traffic scenario of S1-U interface where all the eNBs uploading data to the S-GW which is under attack. Attacker (TCP packet generator) sends TCP SYN packets to the server by changing the port number and the source IP address (One change per packet). Server allocates one port for every successfully arrived SYN packet. As the TCP timeout value is 270 s [10], an attacked port will not be released until the TCP timeout expires. Likewise, attacker occupies all the ports (64000 per user) [10] and IP address combinations. This will terminate the communication in the network.

The LTE backhaul bandwidth is set to 500 Mbps and the attacker has 100 Mbps connection. We run the simulation for 500 s and the attack is placed between 25 s - 125 s time intervals.

Figure 5 illustrates the normalized average throughput of a user over the simulation time. We can observe that both IPsec tunnel and BEET mode VPNs have no significant throughput drop during the attack period. They achieved the maximum throughput similar to the non-attacking period. However, TLS/SSL VPN has almost zero throughput (total packet drop) during the DoS attack. As the TCP time out is higher than the attack period, TLS/SSL VPN takes at least 270 s to fully recover from the attack.

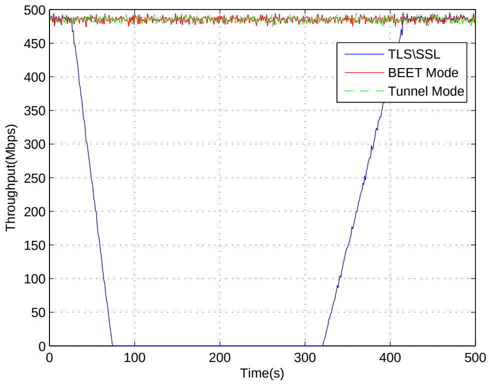

Fig. 5: Impact of TCP SYN DoS attack

B. Impact of DDoS Attack

Same TCP SYN flood attack model is used to study the DDoS attack scenario. We gradually increase the number of attackers from 1 to 20. Figure 6 illustrates the normalized average throughput of a user over the simulation time. As we have similar results for IPsec Tunnel and IPsec BEET VPN architectures for all tests, we present results related to BEET VPN architecture of 20 attackers scenario only. We can observe that both IPsec tunnel and BEET VPNs have no throughput drop even under DDoS attack of 20 attackers. However, TLS/SSL VPN has no throughput (total packet drop) during the DDoS attack also. When the numbers of attackers increase, total system down time also increases and system rapidly approaches to zero throughput status.

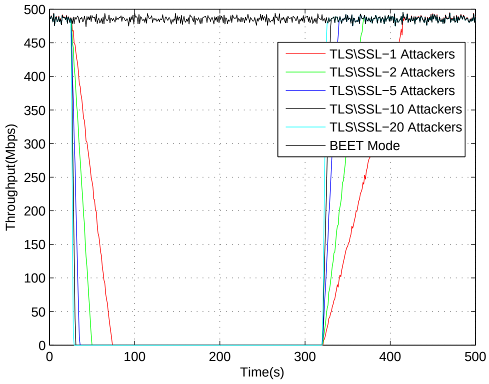

Fig. 6: Impact of TCP SYN DDoS attack

C. Impact of TCP reset attack

TCP reset attack is an IP based attack where an attacker sends forge TCP packets to endpoints by setting the reset bit to one. However, the attacker must include correct IP addresses, port numbers and a valid sequence number in the packet header. Once these forge TCP packets match with the above parameters, end point resets the ongoing TCP connection [11].

We model a TCP packet generator which has the same data rate as the VPN users. Attacker sends forge TCP packets (with no payload) by increasing the sequence number until it resets the attacked TCP connection. For each packet, sequence number is increased by a window size which is 16384 (Typical value for Cisco routers) [11].

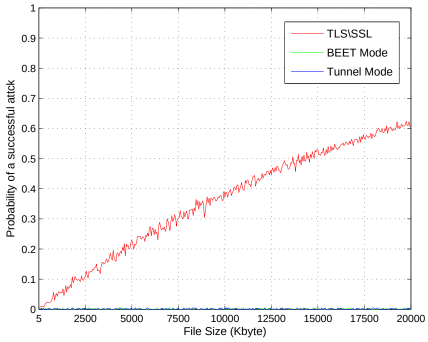

Fig. 7: Impact of TCP reset attack

The probability of attack (figure 7) is calculated against the file size. By considering the file sizes in the Internet, it is found that the minimum file size is 4.5 KB and the maximum size is 20 MB.We see that both IPsec tunnel and BEET VPNs have no effect from TCP reset attack and both architectures have zero probability of attack. However, the probability of attack of the TLS/SSL VPN increases with the file size, because larger file sizes give more time (higher transmission time) for the attacker to guess the correct parameters to reset the connection falsely.

In [11], authors mathematically analyze the TCP reset attacks. The average time which requires to reset a TCP connection can be calculated as

$$Time = \frac{SequenceNumberRange}{WindowSize} * \frac{PacketSize}{DataRate} \quad (1)$$

We evaluated our architecture with these theoretical values and figure 8 shows that they have similar results. It verifies the accuracy of our TCP reset attack simulation model. Here we used sequence number range as 2^{32}, window size as 16384 and attacker packets are TCP packets without any payload. Attackers data rate gradually increased from 50Mbps to 500Mbps. When the attacker's data rate increases, it lowers

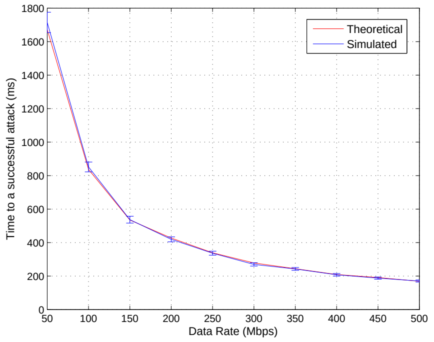

Fig. 8: Analysis of the TCP reset attack model

the time requires to reset the connection as attacker can send more packet in a given time period.

VI. Discussion

In this section, we discuss the security features of our architectures and explain benefits over the existing traffics architectures for the LTE backhaul.

1) User Authentication : New users have to verify their identity by providing a trusted certificate or/and passing a public key authentication during the initial message exchanges (IKEv2 and HIP BEX). It provides the mutual authentication between users and prevent outside breaches to the backhaul.

2) User Authorization : Authorization Server (AS) is the key element for user authorization. Existing VPN users need to get permission from the AS before granting access to a new join request. Hence, malicious users (not in the access control list) will not gain access to the VPN.

3) Payload Encryption : Both VPN architectures use IPsec ESP mode. Hence, payload is always encrypted based on SAs exchanges during the initial message exchanges (IKEv2 and HIP BEX). It will be secured the backhaul traffic by unauthorized eavesdropped attacks.

4) Privacy Protection : In IPsec tunnel mode VPN architecture, the entire original IP packet is encapsulated and new outer IP addresses are added to the header. Hence ESP protection is afforded to the whole inner IP packet and privacy will be protected. In BEET VPN, as long as HI is exposed to the outside world, the original IP addresses are encrypted during the communication. Thus, it will provide the privacy protection.

5) IP based Attack Prevention : Our simulation results (section V) verified that proposed architectures are able to provide a secured backhaul traffic communication during DoS, DDoS and TCP reset attacks. Furthermore, user authentication mechanism prevents IP spoofing attacks as well. Altogether, our architectures provide IP based attack protection.

A. Comparison of IPsec Tunnel mode and IPsec BEET mode VPNs

The IPsec BEET mode VPN architecture anticipates several benefits than IPsec tunnel mode architecture. First, the access control and policy management decisions are taken based on HI instead of IP address. Hence, network operators can freely reallocate the IP address of backhaul element without breaking existing VPNs during new element deployments or a backhaul routing optimization process. Second, single HI can represent several physical/logical interfaces with different IP addresses. Hence multihomed nodes can obtain advantages such as load balancing and link fault protection by redundancy paths. Third, a HIP enabled backhaul architecture can be used to provide new services for mobile networks, for example layer 2 secured automatic VPLS (Virtual Private LAN Service) for mobile users [12].

However, BEET VPN architecture needs an initial capital cost than IPsec tunnel mode, because BEET VPN architecture required new HIP enabled backhaul network elements. Most of the existing network element will support IPsec tunnel mode VPN architecture, hence operators can deploy it with a minimum initial cost.

VII. Conclusion

We presented two new VPN architectures for LTE backhaul. Both architectures are layer 3 IPsec VPNs based on IKEv2 and HIP. The proposed solutions can secure the backhaul traffic by means of user authentication, user authorization, payload encryption, privacy protection and IP based attacks prevention. Simulation results verified that they provide a secured backhaul traffic communication during DoS, DDoS and TCP reset attacks. Future studies are focused on developing a mesh VPN architecture for LTE backhaul and core networks.

Acknowledgment

This work has been performed in the framework of the CELTIC project CP7-011 MEVICO. The authors would like to acknowledge the contributions of their colleagues.

References

[1] M. A. Alvarez, F. Jounay, T. Major, and P. Volpato, "LTE backhauling deployment scenarios," Next Generation Mobile Networks Alliancen, Tech. Rep., 2011.

[2] "Architectural Considerations for Backhaul of 2G/3G and Long Term Evolution Networks," CISCO Cooperation, Tech. Rep., 2010.

[3] "3G/LTE Mobile Backhaul Network MPLS-TP based Solution," UTStarcom, Inc, Tech. Rep., 2009.

[4] "4G Impacts to Mobile Backhaul," Fujitsu Network Communications Inc, Tech. Rep., 2009.

[5] A. Ronai, "LTE Ready Mobile Backhaul," Ceragon Networks Ltd, Tech. Rep., 2009.

[6] S. Kent and R. Atkinson, "Security Architecture for the Internet Protocol," RFC 2401, nov 1998.

[7] P. Jokela, R. Moskowitz, and P. Nikander, "Using the Encapsulating Security Payload (ESP) Transport Format with the Host Identity Protocol (HIP)," RFC 5202, 2008.

[8] R. Moskowitz, P. Nikander, and P. Jokela, "Host Identity Protocol," RFC 5201, 2008.

[9] D. Kuptsov, A. Khurri, and A. Gurtov, "Distributed user authentication in Wireless LANs," in *World of Wireless, Mobile and Multimedia Networks & Workshops*. IEEE, 2009.

[10] W. Eddy, "TCP SYN flooding attacks and common mitigations," RFC 4987, 2007.

[11] P. A. Watson, "Slipping in the Window: TCP Reset attacks," Tech. Rep., 2004.

[12] T. Henderson, S. Venema, and D. Mattes, "HIP-based Virtual Private LAN Service (HIPLS)," sep 2011.