Secure Virtual Private LAN Services: An Overview with Performance Evaluation

Conference Paper · June 2015

DOI: 10.1109/ICCW.2015.7247513

4 authors:

Madhusanka Liyanage
University College Dublin
224 PUBLICATIONS **4,925** CITATIONS
SEE PROFILE

Jude Okwuibe
University of Oulu
17 PUBLICATIONS **1,141** CITATIONS
SEE PROFILE

Mika Ylianttila
University of Oulu
219 PUBLICATIONS **6,219** CITATIONS
SEE PROFILE

Andrei Gurtov
Linköping University
335 PUBLICATIONS **8,632** CITATIONS
SEE PROFILE

Secure Virtual Private LAN Services: An Overview with Performance Evaluation

Madhusanka Liyanage[1], Jude Okwuibe[2], Mika Ylianttila[3], Andrei Gurtov[4]
[1,2] Centre for Wireless Communication (CWC), University of Oulu, Finland
[3] Centre for Internet Excellence (CIE), University of Oulu, Finland
[4] Helsinki Institute for Information Technology (HIIT), Finland and ITMO University, Russia.
Email: [1]madhusanka@ee.oulu.fi, [2]jokwuibe@ee.oulu.fi, [3]mika.ylianttila@oulu.fi, [4]gurtov@hiit.fi

***Abstract*—Virtual Private LAN Services (VPLS) is a widely utilized Layer 2 (L2) Virtual Private Network (VPN) architecture in industrial networks. In the last few years, VPLS networks gained an immense popularity as an ideal network architecture to interconnect industrial legacy SCADA (Supervisory Control and Data Acquisition) and process control devices over a shared network. However, legacy VPLS architectures are highly vulnerable to security threats which are initiated at the insecure shared network segment. Thus, secure VPLS architectures are becoming popular among industrial enterprises.**

In this article, we provide an overview of existing secure VPLS architectures with a performance evaluation. We evaluate the performance penalty of security on throughput, latency and jitter in a real world testbed. From these experiments, we seek to highlight the drawbacks of existing secure VPLS architectures after implementing them in a real networking environment. Moreover, we try to underscore future research questions that will help to improve the performance of secure VPLS networks.

***Index Terms*—Virtual Private LAN Service, Security, Performance Analysis. Host Identity Protocol**

I. Introduction

Many industrial networks have various automation and industrial systems. These systems usually consist of legacy SCADA (Supervisory Control and Data Acquisition) products and process control devices. Network engineers are widely utilizing network virtualization techniques to interconnect these systems. The network virtualization techniques offer two main benefits. First, it allows isolating the critical core network devices and servers from production line systems. Second, it allows interconnecting legacy SCADA devices by using existing premise wide shared networks such as wireless networks and wired intra-net. It significantly reduces the implementation cost by eliminating the requirement of parallel network infrastructures within a single industrial premise.

However, the legacy SCADA and process control devices are designed for static network environments. They often use protocols which expect flat networks or single broadcast domains. For instance, most of these systems support only OSI (Open System Interconnect) L2 protocols. As a result, the use of well-advanced Layer 3 VPNs (L3VPNs) is challenging or not even possible in industrial enterprise networks.

Industrial networks need L2 network virtualization techniques. L2 network virtualization techniques can be categorized into two main types; namely, Virtual Private LAN Service (VPLS) and Virtual Private Wire Service (VPWS). VPWS supports only point-to-point communication. However, VPLS supports multipoint-to-multipoint Ethernet communication over IP or MPLS (Multiprotocol Label Switching) based cooperate networks. Moreover, VPLS networks support high-speed connectivity and advanced auto discovery features. Thus, VPLS architectures are popular in enterprise networks than VPWS.

The utilization of network virtualization techniques introduces new security threats to the production line systems. For instance, the legacy SCADA and process control devices are extremely vulnerable to security threats which can originate at the insecure public network or the shared wireless network. Usually, these legacy devices are lacking of intelligence and security mechanisms to avoid such security threats. Therefore, VPLS networks should be capable enough to avoid these security threats. On the other hand, the VPLS network itself is vulnerable to security threats. Attacks on the VPLS network might jeopardize the communication between SCADA devices. Therefore, the establishment of secure VPLS architecture is a mandatory requirement of enterprise networks.

In this article, we provide an overview of existing secure VPLS architectures with a performance evaluation. More importantly, the performance penalty of existing secure VPLS architectures on throughput, latency and jitter is evaluated in a real world testbed. From these experiments, we seek to highlight the drawbacks of existing secure VPLS architectures after implementing in a real networking environment. Moreover, we try to underscore future research questions that will help to improve the performance of secure VPLS networks. Finally, few experiments are conducted to compare the performance of existing secure VPLS products in the market.

The rest of the paper is organized as follows. An overview of secure VPLS architectures is presented in Section II. The experimental testbed and measurement results are illustrated in Section III and Section IV respectively. Section V contains a discussion on industrial applications of secure VPLS architectures and existing secure VPLS products. Finally, Section VI concludes experiment results and presents future research directions.

978-1-4673-6305-1/15/$31.00 ©2015 IEEE

II. Background

A. Virtual Private LAN Service (VPLS)

VPLS is a Layer 2 VPN (L2VPN) architecture which provides Ethernet based multipoint to multipoint communication among different sites. In other words, it interconnects the geographically distributed customer private network segments by using the provider's public IP/MPLS network.

Figure 1 illustrates the network topology of a simple VPLS network.

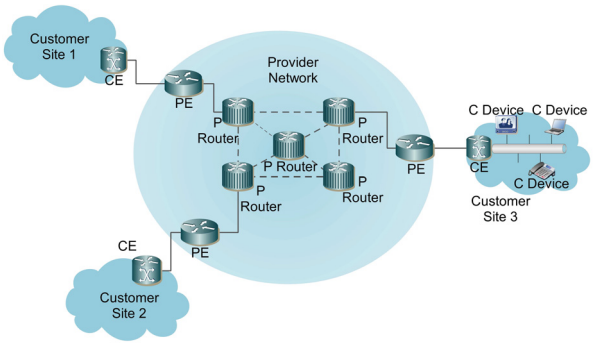


Fig. 1: The network topology of a simple VPLS network

A VPLS has three main components namely, Provider Edge Equipments (PEs), Customer Edge Equipments (CEs) and the provider network. PE devices contain all the VPN intelligence. The provider establishes a full mesh of VPN tunnels over the IP/MPLS based provider network to interconnect these PEs. CE devices are the interfacing devices between the customer and provider networks. Moreover, a VPLS network uses a control protocols to maintain the operation of VPLS.

In industrial networks, VPLS networks are widely used to interconnect their legacy SCADA and process control devices over the existing network infrastructures such as WiFi network and Ethernet based wired network. In our experiments, the premises-wide wireless network is provisioning as the provider network of VPLS.

B. Security considerations of the VPLS

Generally, the customer's private network is a closed and trusted network. It does not contain any open interfaces for insecure public networks. Thus, it is considered as well secured. However, VPLS networks transports customer's private data (the legacy system traffic in SCADA networks) over the provider network. However, the provider network is public, shared and unsecured. As a result, customer's private data is exposed to the public users and vulnerable to attacks which are initiated at the provider network.

Moreover legacy SCADA and process control devices are now vulnerable to security threats through their public network facing interfaces due to VPLS connections. The malformed traffic or abnormal amount of junk traffic might be sufficient enough to crash legacy SCADA devices. Generally, these devices do not have any inbuilt security mechanisms to prevent such attacks.

On the other hand, PE devices and VPLS traffic over the provider network are also vulnerable to third party attacks. which can jeopardize the operation of the VPLS. Such attacks can strain network resources and terminate VPN tunnels between customer's sites. Thus, VPLS architectures should support security services such as PE authentication, payload encryption and control protocol security.

The preliminary procedure to evade malicious users is to utilize a strong authentication mechanism at the tunnel establishment phase. For instance, Public Key Infrastructure (PKI) based mutual authentication mechanism can prevent VPN tunnel establishments with malicious devices. Otherwise, VPLS traffic may be directed to a wrong location and malicious users can easily destroy or modify the customer traffic. The payload encryption is also required for a secure VPLS traffic transportation. Otherwise, attackers can eavesdrop the ongoing communication data and use eavesdropped information to perform various attacks such as DoS (Denial of Service), identity spoofing and replay attacks. However, most non-secure VPLS architectures [1]–[4] use TCP based control protocols and they are vulnerable to various IP/TCP based attacks such as TCP reset and TCP DoS attacks.

C. Existing VPLS Architectures

Internet Engineering Task Force (IETF) has initially standardized two frameworks to build a VPLS network based on Border Gateway Protocol (BGP) [1] and Label Distribution Protocol (LDP) [2]. Thereafter, several VPLS architectures were proposed to improve the performance of these frameworks [3]–[9].

In [7], authors intensely discussed the deployment aspects of BGP and LDP based VPLS frameworks. A VPLS like service exclusively for IP traffic was proposed as IP only LAN Service (IPLS) [3]. Authors explained the possible simplifications in an all-IP environment. A hierarchical VPLS architecture is proposed in [2] to increase the control plane scalability. In [8], authors proposed a hub and spoke connectivity model as a hierarchical VPLS architecture to establish a scalable VPLS network.

The very first secure VPLS architecture was proposed as Host Identity Protocol (HIP)-enabled virtual private LAN Service (HIPLS) [4]. Authors proposed a use-case of HIP to provide a secure VPLS over an untrusted network. HIPLS provides the demanded level of security features for the VPLS network. However, the initial HIPLS architecture is lacking of control, data and security plane scalability.

Two advanced versions of HIPLS are proposed as Session key based HIP VPLS architecture (S-HIPLS) [5] [10] and Hierarchical HIP VPLS architecture (H-HIPLS) [6]. Similar to the original HIPLS, S-HIPLS is also a flat VPLS architecture. Here, authors proposed to use a session key based security mechanism to achieve forwarding and security plane scalability for HIPLS. Later, a hierarchical version of S-HIPLS is proposed as H-HIPLS to increase the control plane scalability as well. The development of secure VPLS solutions for SCADA networks is a very new research topic

TABLE I: A comparison of different VPLS architectures

	Non Secure Flat VPLS [1] [2]	Non Secure Hierarchical VPLS [2] [8]	HIPLS [4]	S-HIPLS [5]	H-HIPLS [6]
PE Authentication	No	No	Yes	Yes	Yes
Payload Encryption	No	No	Yes	Yes	Yes
Secure Control Protocol	No	No	Yes	Yes	Yes
IP Attack Protection	No	No	Yes	Yes	Yes
Scalability	Medium	High	Low	Medium	High

and not many secure VPLS architectures are proposed for the moment. To the best of our knowledge, HIP based VPLS architectures are the only proposed secure VPLS architectures for the moment.

Table I contains a comparison of the security features of different VPLS architectures.

D. HIP-based Virtual Private LAN Service (HIPLS)

HIPLS is the very first secure VPLS architecture which has provided the required level of security for a VPLS network. HIPLS proposed a use-case of HIP to establish a secure VPLS over a standard IP based provider network [4]. It uses HIP enabled PEs as the edge devices and establishes a full mesh of IPsec BEET (Bounded-End-to-End Tunnels) mode tunnels between these PEs. These tunnels are established by using HIP BEX procedure [11]. Later, these tunnels are managed by using HIP signaling. Figure 2 illustrates the network topology and protocol stack of a simple HIPLS network.

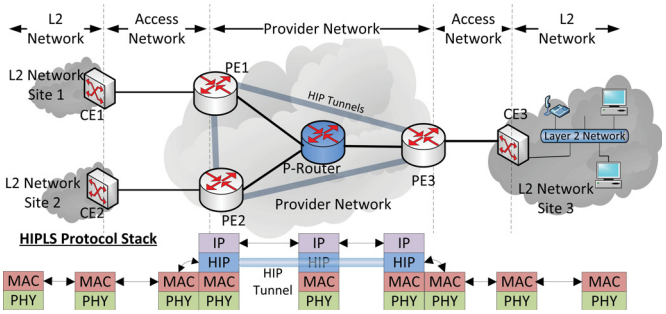


Fig. 2: The network topology of a HIPLS architecture

There are two main differences of HIPLS from the traditional HIP implementation. First, HIP is here implemented as a "bump-in-the-wire" implementation in the middleboxes instead of the end nodes. Second, HIP payload is now layer 2 frames instead of the transport layer Protocol Data Units (PDUs) [4]. However, HIPLS is still able to inherit all the advanced security services which are offered by a traditional HIP implementation.

III. The Experiment Testbed

We model a SCADA network which uses the existing WiFi network to interconnect L2 legacy devices via a VPLS network. Here, the existing Wi-Fi network is provisioning as the provider network of VPLS.

The experiment testbed consists of two User Equipments (UEs) which are placed in two different locations. Two laptops with Ubuntu 12.04 LTS (Long Term Support) operating system are used as two UEs.Here, the provider network is a WiFi 802.11g standard wireless network which supports a maximum speed of 54 Mpbs. Figure 3 illustrates the experiment testbed.

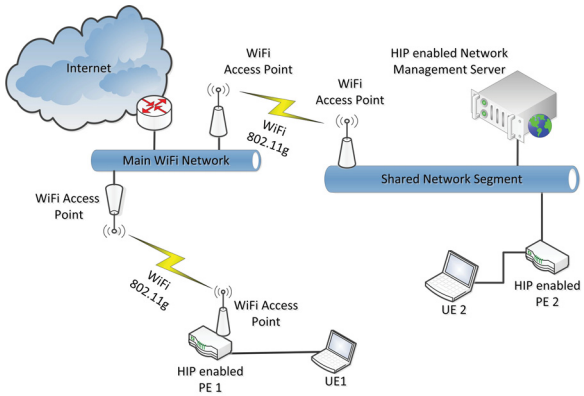


Fig. 3: The experiment testbed

Two HIP enabled PEs are used at the edge of the Wi-Fi network. PE1 has the wireless connectivity to the campus network. A wired shared network is established by using a WiFi router with four Ethernet ports. PE2 has a wired connection to the WiFi router via an Ethernet port. Two customized Industrial Security Appliances (ISAs) are used as PE devices. These ISA devices are developed by Tempered Networks [12]. Each PE uses a unique public/private RSA-2048 bit key pair as its HI.

Furthermore, a HIP enabled network management server is attached to the shared wired network. This server is responsible for the VPLS provisioning functions. It is used to assign network addresses to PEs, key management, VPN tunnel management and distribution of cryptographic credentials. Also, it supports the auto discovery functions of PEs. All customer data traffic is encrypted before transporting them over the provider network. HIP uses Advanced Encryption Standard (AES) - Cipher-block chaining (CBC) encryption. The key size of AES is 128 bits in this experiment.

To the best of our knowledge, HIP based VPLS architectures are the only secure VPLS architectures proposed yet. None of the other VPLS architectures have any dedicated security mechanisms. Thus, it is not possible to study the security penalty of other architectures. We analyze only the HIPLS

architecture in our experiments. Both S-HIPLS and H-HIPLS architectures are proposed only to tackle the scalability issues by proposing a key distribution and tunnel establishment mechanisms. These changes impact only the operation of the control plane. In the steady state operation (once the VPLS network is established), both S-HIPLS and H-HIPLS architectures have exactly the same behavior as the original HIPLS [5] [6]. All three architectures use HIP tunnels to secure the data plane traffic. Thus, we present the experiment results based on original HIPLS architecture only. However, other secure VPLS architectures such as S-HIPLS and H-HIPLS also have the same behavior in this experiment setup.

In this experiment, we analyze the performance penalty of security on throughput, jitter and latency. We measure the performance against no VPLS scenario and with non secure VPLS (LDP VPLS [2]) scenario. The throughput and latency is measured by using the IPERF networking tool [13]. Table II contains the simulation settings for IPERF testing tool.

TABLE II: The simulation settings for the IPERF

Parameter	Value	Value
Protocol	UDP	TCP
Port	5004	5004
Buffer size	default (1470 kB)	default (1470 kB)
Packet size	default (1470 B)	default (1470 B)
TCP window size	-	21.0 KByte
Report interval	1 s	1 s

IV. Performance Evaluation Results

A. Performance Penalty of Security on Latency

In the first set of experiments, we measure the performance penalty of security on latency due to the secure VPLS architecture. The Round Trip Time (RTT) of a packet is measured by using the basic ping test. Each experiment is run for 100 packets in both directions.

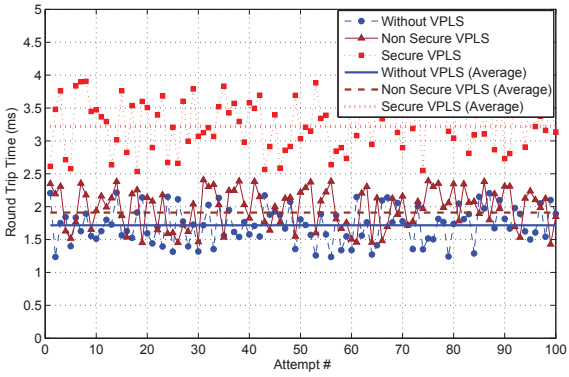


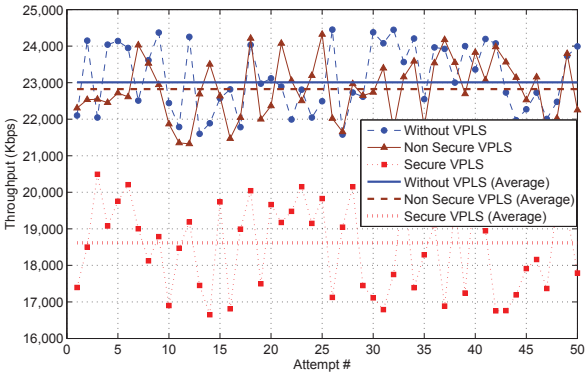
Fig. 4: The performance penalty of security on latency

Figure 4 contains the actual and average latency from the experiments. Based on average RTT values, the secure VPLS architecture increases the latency approximately by 87% than the non VPLS scenario and by 68% than the non secure VPLS scenario. Similarly, non secure VPLS increases the latency approximately by 11% than the non VPLS scenario. The main reason to increase the latency is the delay in both the packet encryption and tunnel encapsulation.

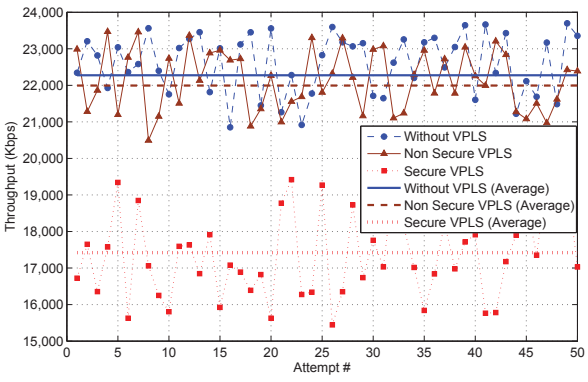
B. Performance Penalty of Security on Throughput

In the second set of experiments, we measure the performance penalty of security on throughput. Both TCP and UDP sessions are considered here.

1) Performance Penalty of Security on TCP Throughput: First, we consider TCP sessions. The throughput is measured by using the IPERF networking tool. We measured the throughput of both short and long TCP sessions. A short TCP session runs for 10 s and a long TCP session runs for 500 s. Each experiment is repeated 50 times in both directions.



(a) Short TCP session



(b) Long TCP session

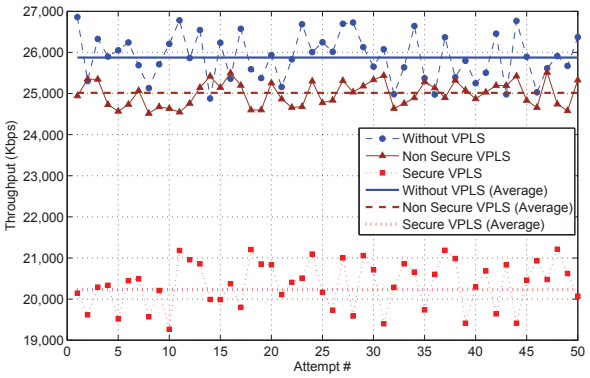
Fig. 5: The performance penalty of security on TCP throughput

According to experiment results in Figure 5, the performance penalty of security on throughput is about 19% for a short TCP session and 21% for a long TCP session compared to the non VPLS scenario. Moreover, the performance penalty of security on throughput is about 18% for a short TCP session and 20% for a long TCP session compared to the non secure VPLS architecture. Thus, we conclude that the

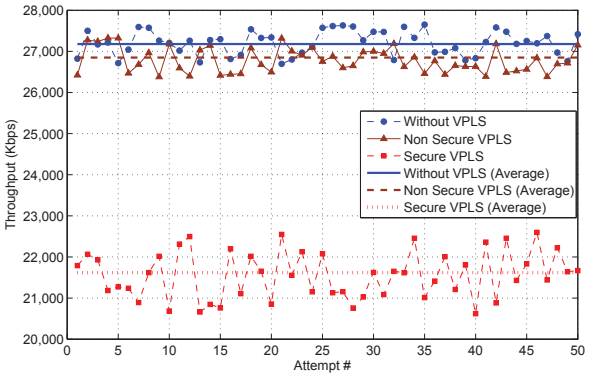
performance penalty of security on throughput is independent of the duration of a TCP session.

On the other hand, non secure VPLS reduces the throughput only by 1% than the non VPLS scenario in both short and long TCP sessions. Therefore, the impact of VPLS tunnel encapsulation on TCP throughput is very low. The additional layer of encryption is the main reasons to reduce the average throughput of the secure VPLS architecture.

2) Performance Penalty of Security on UDP Throughput: In the next experiment, we consider UDP sessions. The throughput is measured by using the IPERF networking tool. The UDP bandwidth of IPERF is set to 54 Mbps which is equal to the bandwidth of the network. In this experiment also, we measure the throughput for both short and long UDP sessions. A short UDP session runs for 10 s and long UDP session runs for 500 s. Each experiment repeated 50 times in both directions.



(a) Short UDP session



(b) Long UDP session

Fig. 6: The performance penalty of security on UDP throughput

According to the experiment results in Figure 6, the performance penalty of security on throughput is about 20% for a short UDP session and 21% for a long UDP session compared to the non VPLS scenario. Moreover, the performance penalty of security on throughput is about 19% for both for short and long UDP sessions compared to the non secure VPLS architecture. Thus, we conclude that the performance penalty of security on throughput is independent of the duration of a UDP session.

On the other hand, non secure VPLS the latency increment is below 2% in compared with the non VPLS scenario in both short and long TCP session. Therefore, the impact of VPLS tunnel encapsulation on TCP throughput is very low. Similar to the TCP experiment, the additional layer of encryption is the main reasons to reduce the average throughput of the secure VPLS architecture.

Furthermore, the experiment results reveal that UDP throughput is 14% higher for both short and long sessions than TCP throughput for secure VPLS architecture. Similarly, UDP throughput is 15% higher for short sessions and 14% higher for long sessions than TCP throughput for both non secure VPLS and non VPLS architectures.

Moreover, the performance penalty of security on throughput is around 20% for both UDP and TCP sessions in compared with both non VPLS scenario and non secure VPLS architecture. Thus, we can conclude that the performance penalty of security on throughput is independent of the transport layer protocol.

On the other hand, Wijesinha et al. observed that the maximum achievable UDP throughput is well below 50% (less than 27 Mbps) for 802.11g Wi-Fi connection at the maximum data rate of 54 Mbps even under ideal and controlled conditions [14]. In our experiments, the UDP throughput (26.5 Mbps) is almost similar to these findings and it verified the accuracy of our test bed.

C. Performance Penalty of Security on Jitter

In the third set of experiments, we measure the performance penalty of security on the jitter. The jitter of a UDP session is measured by using the IPERF networking tool. Each experiment repeated 50 times in both directions.

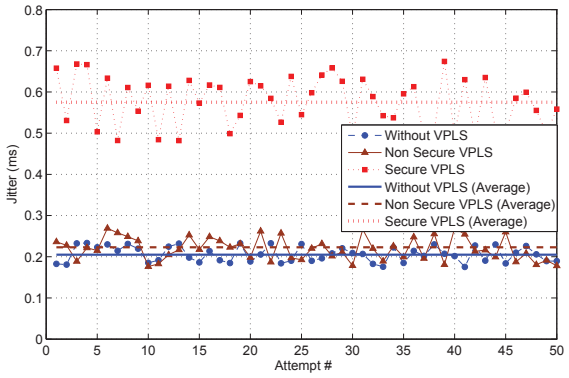
Figure 7 illustrates the experiment results. The UDP bandwidth of IPERF is set to 54 Mbps.

According to the experiment results in Figure 7, the average jitter of the secure VPLS architecture is two times higher than the non-VPLS and non-secure scenarios for both short and long sessions. Thus, we conclude that the performance penalty of security on jitter is independent of the duration of the session. However, the average jitter of secure VPLS is still less than 0.5 ms. Thus, the performance penalty of security on jitter will not affect to the real time application such as VoIP, video streaming in a short range network.

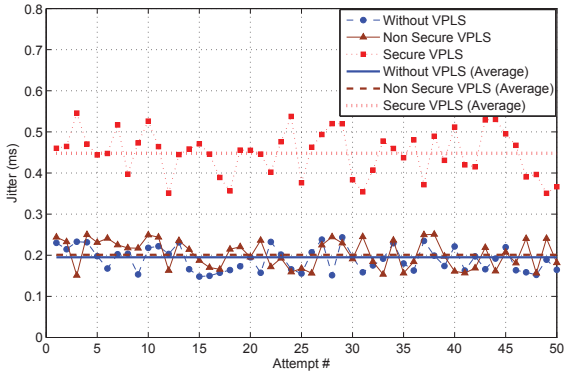
V. Discussion

A. Industrial Applications of Secure VPLS Architectures

HIP based secure VPLS architectures are becoming popular among many industrial enterprises. For instance, Boeing is using HIPLS based VPLS network in the assembly line of Boeing 777 airplanes [15]. On the other hand, two major SCADA network appliance developing companies have already started to develop HIPLS based security solutions. They



(a) Short UDP session



(b) Long UDP session

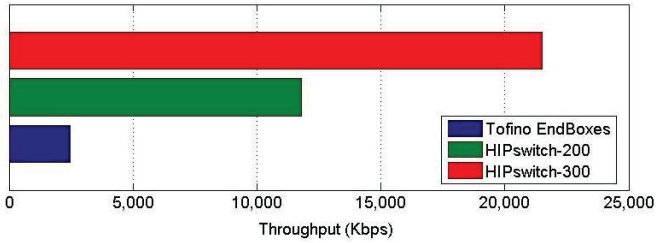
Fig. 7: The performance penalty of security on Jitter

used the OpenHIP project [16] which is an open source software implementation of HIP.

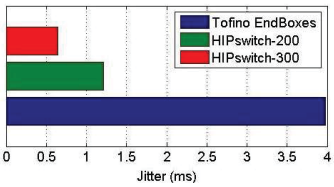
In 2009, a Canadian company Byres Security released the first HIPLS based end-box product called Tofino Endboxes (TEBs) to establish secure VPLS for SCADA and industrial process control systems [17]. However, TEBs are lacking in graphical user interface for the end-box configuration and maintenance. Thus, the configuration and maintenance procedures of TEBs are complex and time consuming tasks.

Later, Tempered Networks released the second HIPLS based network solution called HIPswitches [12]. HIPswitches provide a web based graphical user interface for the device configuration and maintenance. Thus, the configuration process of HIPswitches is simple and user friendly. Moreover, HIPswitches support inbuilt wireless connectivity as well. Tempered HIP switches are used in various use cases such as oil, gas, telecom and production facilities [12].

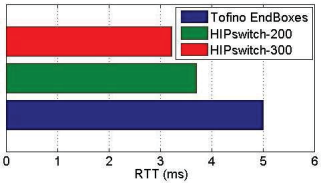
We perform experiments on the same testbed (Figure 3) to compare the performance of TEB and HIPswitches. For each experiment, we replace PEs in the testbed with TEBs and HIPswitches. We use two type of HIPswitches namely HIPswitch-200 and HIPswitch-300. A UDP session with the bandwidth of 54 Mbps is used here. The experiment results are illustrated in Figure 8.



(a) Average Throughput



(b) Average Jitter



(c) Average Latency

Fig. 8: The performance comparison of Tofino and Tempered products

The average throughput, jitter and latency are compared. HIPswitch-300 devices have better performance than TEBs in all three performance metrics. HIPswitch-300 devices reduce the latency by 35% and jitter by 83% and increase the throughput by 8 times than TEB devices. Moreover, HIPswitch-200 devices reduce the latency by 13% and jitter by 46% and increase the throughput by 2 times than TEB devices. HIPswitch-300 devices have higher processing capabilities than TEBs. It is the main reason to improve the performance of VPLS networks. This result opens new opportunities for research. According to a recent Intel's white paper, IPsec acceleration is possible by using external accelerators and/or using new AES instruction sets for processors [18]. Thus, the adaptation of these techniques will further improve the performance of secure VPLS products.

B. Architectural Limitation of Secure VPLS Architectures

In this section, we present the main architectural limitations in existing secure VPLS architectures.

1) Impact on L2 protocols: VPLS architectures allow sharing the same Ethernet broadcast domain over multiple geographically distributed sites. Generally, the legacy user equipments use various L2 network protocols such as STP (Spanning Tree Protocol), RARP Reverse Address Resolution Protocol, ARP (Address Resolution Protocol) in this Ethernet network. However, VPLS based inter-site connectivity links (VPN tunnels) are invisible to L2 devices and L2 protocol.

These hidden links have very different behaviors than typical Ethernet links. Thus, many layer 2 protocols fail to function properly in VPLS based Ethernet network [19]. For instance, STP fails to identify the loops over the provider network. It causes many issues such as broadcast storms, multiple frame transmissions, higher spanning tree convergence time and forwarding table instability.

Secure VPLS architectures is still incapable to provide a

concrete solution for this issue. HIPLS proposed to evade the transmission of L2 PDUs (Protocol Data Units) over VPLS network. However, it is not a perfect solution since many SCADA and process control devices still rely on L2 protocols for their proper operation.

2) Static Tunnel Establishment and Maintenance Procedure: The existing secure VPLS architectures require to establish IPsec tunnels between PEs in the VPLS network. Moreover, authors proposed to maintain these tunnels for a long period to minimize the performance penalty due to the tunnel establishment procedure. The tunnel maintenance duration is static and predefined by the network administrators. However, some of the customer sites have very low traffic intensity between them.

As a result, some of these tunnels will not be used very frequently. The maintenance of a tunnel between such sites not only waste PEs' resources such as memory, CPU and ports but also occupy the network bandwidth for tunnel update messages. Therefore, it is necessary to fine tune the tunnel maintenance duration based on traffic demand. However, the existing secure VPLS architectures do not support dynamic parameter adjustment for IPsec tunnels.

VI. Conclusion and Future Works

In this paper, we evaluated the performance penalty of security of HIP based secure VPLS architectures on throughput, jitter and latency. The performance penalty of security on throughput is around around 20% for both UDP and TCP sessions in compared with both non VPLS scenario and non secure VPLS architecture. Thus, it concludes that the performance penalty of security on throughput is independent of the transport layer protocol. On the other hand, non secure VPLS reduces the throughput only by 1% than the non VPLS scenario in both short and long TCP sessions. Therefore, the impact of VPLS tunnel encapsulation on TCP throughput is very low. The additional layer of encryption is the main reasons to reduce the average throughput of the secure VPLS architecture.

Furthermore, experiments reveal that UDP throughput is 14% higher than TCP throughput for both secure VPLS and non secure VPLS traffic. Thus, UDP based application can obtain a better throughput performance than TCP based applications in a secure VPLS network as well. In general, secure VPLS architectures have relatively poor performance in terms of throughput and it opens new opportunities for research. Thus, the future secure VPLS architectures have to focus on improving the network throughput.

Experiment results revealed that the jitter of the secure VPLS architecture is two times higher than the non-secure and non-VPLS scenarios for both short and long session. However, it is still suitable enough to support many network applications in small scale networks.

The secure VPLS architecture increases the latency approximately by 87% due to encryption and tunneling delays in PE devices. The encryption delay can be reduced by using high performing PE devices or using efficient encryption algorithms. The IPsec acceleration can be achieved by using external accelerators and/or using new AES instruction sets for processors. Thus, the adaptation of these techniques for PEs will improve the performance of secure VPLS networks.

In future, we are planning to extend our experiments beyond SCADA networks such as long-haul and telecommunication networks. For instance, we are working on using the Internet to interconnect two sites which are located at far away locations.

Acknowledgment

This work has been performed in the framework of the CELTIC project CP2012 SIGMONA.

References

[1] K. Kompella and Y. Rekhter, "Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling," RFC 4761, IETF, January 2007.
[2] M. Lasserre and V. Kompella, "Virtual private LAN service (VPLS) using label distribution protocol (LDP) signaling," RFC 4762, IETF, January 2007.
[3] H. Shah, E. Rosen, and G. Heron, "IP-Only LAN Service (IPLS)," IETF, February 2007.
[4] T. Henderson, S. Venema, and D. Mattes, "HIP-based Virtual Private LAN Service (HIPLS)," *Internet Draft*, IETF, December 2013.
[5] M. Liyanage and A. Gurtov, "Securing Virtual Private LAN Service by Efficient Key Management," *Security and Communication Networks*, 2013.
[6] M. Liyanage, M. Ylianttila, and A. Gurtov, "Secure Hierarchical Virtual Private LAN Services for Provider Provisioned Networks," in *Proc. of IEEE Conference on Communications and Network Security: CNS, Washington D.C., USA*, 2013.
[7] R. Gu, J. Dong, M. Chen, Q. Zeng and Z. Liu, "Analysis of Virtual Private LAN Service (VPLS) Deployment," IETF, September 2011.
[8] S. Khandekar, V. Kompella, J. Regan, *et al.*, "Hierarchical Virtual Private LAN Service," *Internet Draft*, IETF, June 2002.
[9] A. Sodder, K. Ramakrishnan, C. DelRegno, , and J. Wils, "Virtual Hierarchical LAN Services," *Internet Draft*, IETF, April 2003.
[10] M. Liyanage and A. Gurtov, "A Scalable and Secure VPLS Architecture for Provider Provisioned Networks," in *Proc. of IEEE Wireless Communication and Networking Conference: WCNC, Shanghai, China*, 2013.
[11] A. Gurtov, *Host Identity Protocol (HIP): Towards the Secure Mobile Internet*. Wiley, 2008.
[12] Tempered networks. [Online]. Available: http://www.temperednetworks.com/
[13] Iperf. [Online]. Available: http://iperf.sourceforge.net/
[14] A. L. Wijesinha, Y.-t. Song, and et al., "Throughput Measurement for UDP Traffic in an IEEE 802.11 g WLAN," in *First ACIS International Workshop on Self-Assembling Wireless Networks, SNPD/SAWN 2005*. IEEE, 2005.
[15] T. Henderson. Boeing HIP Secure Mobile Architecture. [Online]. Available: http://www.ietf.org/proceedings/73/slides/HIPRG-0.pdf
[16] "The OpenHIP project," http://www.openhip.org/.
[17] Tofino Security Appliance. [Online]. Available: http://www.tofinosecurity.com/products/tofino-security-appliance
[18] "Carrier Cloud Telecoms - Exploring the Challenges of Deploying Virtualisation and SDN in Telecom Networks," Intel Cooperation, Tech. Rep., 2013.
[19] M. Liyanage, M. Ylianttila, and A. Gurtov, "A novel distributed spanning tree protocol for provider provisioned VPLS networks," in *IEEE International Conference on Communications (ICC)*. IEEE, 2014, pp. 2982–2988.