Fast Transmission Mechanism for Secure VPLS Architectures

Madhusanka Liyanage[1], Mika Ylianttila[2], Andrei Gurtov[3]
[1,2] Centre for Wireless Communications (CWC), University of Oulu, Finland
[3] Department of Computer and Information Science, Linköping University, Sweden
Email: [1]madhusanka.liyanage@oulu.fi, [2]mika.ylianttila@oulu.fi, [3]gurtov@acm.org

***Abstract*—Ethernet based secure VPLS (Virtual Private LAN Services) networks require to establish full mesh of VPLS tunnels between the customer sites. However, the tunnel establishment between geographically distant customer sites introduces a significantly high delay to the user traffic transportation.**

In this article, we propose a novel fast transmission mechanism for secure VPLS architectures to reduce the waiting time before transmitting the data and the average data transmission delay between geographically distant customer sites. The performance of proposed mechanism is analyzed by using a simulation model and a testbed implementation.

***Index Terms*—VPLS, Delay, SDN, Security, IPsec, HIP**

I. Introduction

Ethernet based VPLS networks are initially designed for industrial networks to interconnect the premises-wide SCADA (Supervisory Control and Data Acquisition) and process control devices. It provides transparent, protocol independent, multipoint-to-multipoint Ethernet connectivity over (Internet Protocol) or MPLS (Multiprotocol Label Switching) based provider networks. Due to the simple, protocol-independent and cost efficient operation, VPLS networks are now becoming attractive in many Enterprise applications such as Telecommunication networks, Industrial Internet, DCI (data center interconnect), voice over IP (VoIP) and videoconferencing services. Thus, VPLS networks are now interconnecting customer sites across the countries and even across the globe.

Existing secure VPLS architectures establish a full mesh of IPsec tunnels between the customer sites. Each tunnel establishment requires to exchange several round of message exchanges. As a result, the tunnel establishment delay is highly depending on the communication link quality and the distance between the sites. For instance, the tunnel establishment delay between geographically distant sites is very high. This will effect the performance of delay sensitive applications. However, legacy secure VPLS networks do not consider communication link characteristics and follow the same procedure for all the tunnel establishment instances. Thus, some tunnel establishment instances are suffering from significantly high tunnel establishment delays (E.g. tunnels with satellite hops) and not able to provide required level of service quality.

- Our Contribution

In this article, we propose a novel Fast Transmission Mechanism (FTM) to reduce the waiting time of the user data transmission. It ultimately reduces the average data transmission delay between geographically distant customer sites and increases the Quality of Service (QoS). We analyze the performance of the proposed architecture by using a simulation model. Finally, the feasibility of proposed mechanism is verified by using a testbed implementation.

The rest of the paper is organized as follows. Section II contains the background of existing secure VPLS architectures and their limitations. Related works are presented in Section III. The proposed FTM is described in Section IV. The simulation and testbed experiment results are presented in Section V. Section VI contains the conclusion of the paper.

II. Background

A. Virtual Private LAN Service (VPLS)

VPLS provides the multipoint-to-multipoint Ethernet communication over IP/MPLS (Multiprotocol Label Switching) based provider networks. It expands the Ethernet broadcast domain to multiple sites which are geographically dispersed across the country or even the globe. Figure 1 illustrates a simple VPLS architecture.

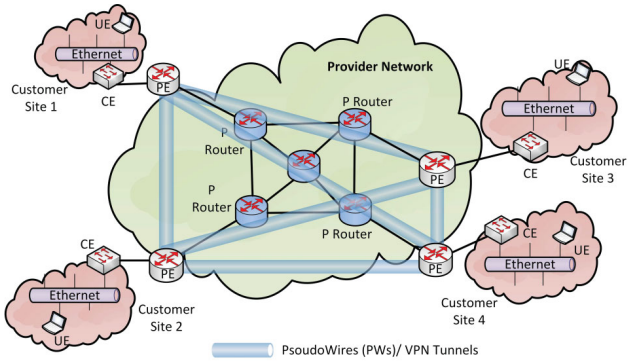

Fig. 1: The network topology of a VPLS network

A VPLS network consists of different components such as Customer edge Equipment (CE), Provider edge Equipment (PE), Provider (P) routers, PWs (Pseudo Wires)/tunnels and a provider network. CEs are the middleboxes between the customer sites and provider network. PEs are belonged to the service provider and they have all the VPLS intelligence. A full mesh of PWs/tunnels are established over the provider

network to interconnect these PEs. The provider network can be operated on the basis of several network protocols, such as IPv4, IPv6, and MPLS. Different variety of tunnels such as IPsec, L2TPv3 (Layer 2 Tunneling Protocol Version 3) and MPLS are used to establish these links. However, the existing secure VPLS architectures [**?**], [1]–[3] and commercial products [4], [5] utilize IPsec tunnels. Provider network contains other P routers to provide the connectivity between PEs. The existence of the overlay VPLS network is hidden from P routers.

B. Limitations in Legacy Secure VPLS Architectures

In [6], authors listed the most of the limitations (i.e. N-square scalability problem, static tunnel parameters, long tunnel establishment delay and lack of traffic engineering features) related to the secure VPLS tunnel establishment mechanism. In addition to the list above, legacy secure VPLS architectures are suffering form additional limitations when they are used to interconnect the distant sites.

1) Long Waiting Time: When the long distant customer sites are communicating, Customer sites have to face a waiting time due to the long tunnel establishment delays. The tunnel establishment delay is highly depending on communication link quality and distance between PEs. Legacy secure VPLS networks do not consider these physical layer constraints and all the tunnel establishments follow the same procedure. As a result, some tunnel establishment instances are suffering from significantly high tunnel establishment delays (e.g. tunnels with satellite hops).

In [6], authors have proposed a tunnel resumption mechanism to reduce the tunnel establishment delay of subsequent tunnel establishments between previously authorized PEs. However, it does not reduces the tunnel establishment delay which occurs during the initial tunnel establishment phase. Moreover, this tunnel resumption mechanism can be supported only for a limited amount of sites due to the network resources limitation in PEs.

2) Reduced Quality of Service (QoS): The tunnel establishment delay between geographically distant sites is very high. For instance, the tunnel establishment of legacy secure VPLS architectures [1]–[3] can take at least 2000 ms between the VPLS sites which have 500 ms transmission delay. However, communication sessions between are very short (e.g. less than 50 ms [7]) in many cases. If the session between sites lasts only a short duration (e.g. 50 ms), then VPLS users have to wait long (e.g. 2000 ms) just to communicate very short duration (e.g.50 ms). This reduces the QoS of short sessions.

III. Related work

Internet Engineering Task Force (IETF) had standardized two basic frameworks for VPLS networks by using Border Gateway Protocol (BGP) [8] and Label Distribution Protocol (LDP) [9]. Thereafter, several VPLS architectures were proposed to improve the performance of these frameworks [1], [3], [10], [11]. The very first secure VPLS architecture was proposed as Host Identity Protocol (HIP)-enabled virtual private LAN Service (HIPLS) [1]. Later, two advanced HIP based VPLS architectures were proposed as Session key based HIP VPLS architecture (S-HIPLS) [2] and Hierarchical HIP VPLS architecture (H-HIPLS) [3]. S-HIPLS is a flat VPLS architecture which proposes to use a session key based security mechanism to achieve forwarding and security plane scalability. A hierarchical architecture of S-HIPLS is proposed as H-HIPLS to increase the control plane scalability as well.

Secure VPLS architectures are using in many industrial applications as well. For instance, Boeing is using HIPLS based VPLS network in the assembly line of Boeing 777 airplanes [12]. Moreover, two major SCADA network appliance developing companies [4], [5] have already started to develop HIPLS based security solutions. The performance of secure VPLS architectures and the commercial products are analyzed in [13].

However, all above stated secure VPLS architectures use static tunnel establishment procedures and they are suffering from limitations such as underutilized network resources, high tunnel management overhead and lack of flexibility. Despite the H-HIPLS architecture, all other secure VPLS architectures are suffering from N-square scalability problem as well. Recently, the utilization of SDN to improve the tunnel management performance of legacy secure VPLS architectures is presented in [6].

All these secure VPLS architectures require to establish IPsec tunnels between PEs. However, none of these architectures proposes a mechanism to overcome the high tunnel establishment delay due to link level limitations.

IV. Fast Transmission Mechanism (FTM)

We propose a novel Fast Transmission Mechanism (FTM) to reduce the waiting time of the user data transmission and the average data transmission delay between geographically distant customer sites. The proposed FTM can be used with existing secure VPLS architecture. However, some some modifications are required in the tunnel establishment mechanism of secure VPLS architectures. Here, we use the tunnel establishment procedure presented in [1]–[3], [6] as the reference model. The proposed FTM is illustrated in Figure 2.

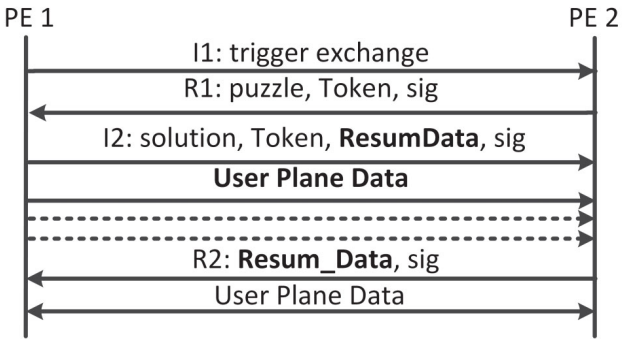

Fig. 2: Fast Transmission Mechanism (FTM)

Similar to legacy secure VPLS architectures, PE1 or the initiator triggers the registration procedure by sending I1

message. Then, PE2 or the responder sends pre-generated R1 message which contains cryptographic puzzle, security token and a signature. This security token is available only for the registered PEs in the VPLS network. During the PE registration phase either Authentication Server [1]–[3] or the centralized controller [6] securely distributes the security token to each PE. The security token is mandatory to establish tunnels with other registered PEs in the VPLS network.

Upon the arrival of RI message, the initiator (PE1) checks the signature and the security token. After the verification of these fields, the initiator sends I2 message which contains the solution of the puzzle, a security token and a signature. Upon the arrival of I2 message, the responder (PE2) subsequently checks the signature, the solution of the puzzle and the security token. Now, the responder (PE2) has received all the necessary information to establish the tunnel and it initiates the tunnel from its side. Moreover, it sends the R2 message to complete tunnel establishment procedure.

The existing VPLS architectures wait until the completion of all four steps of the tunnel establishment mechanism to transmit the user data. However, the tunnel establishment is already completed for the responder (PE2), once it receives the I2 message. Our FTM proposes to transmit the user data from the initiator's (PE1's) end, after it sends the I2 message. Therefore, the tunnel establishment delay will be reduced by 1 RTT (Round Trip Time). However, the initiator (PE1) is still expecting the R2 message. If it does not receive the R2 message before the timeout, it will terminate the further transmission of user data and terminate the tunnel establishment with the responder (PE2).

A. Selective FTM (SFTM) for SDN enabled VPLS networks

It is not necessary to support fast transmission for every tunnel in a VPLS network. For instance, not all tunnels are transporting delay critical user data or not all the tunnels are facing long transport delay. For SDN enabled VPLS networks [6], we can propose a Selective FTM (STFM) mechanism. Here, the SDN controller has the opportunity to select which tunnels are allowed to use FTM by considering following factors.

1) Traffic Transport Delay between end PEs (D) : By measuring the transport delay, we can eliminate the short tunnels. In SDN networks, transport delay can be calculated by using flow information from PEs.
2) QoS requirement of traffic flow (P) : The priority is given for delay sensitive traffic flows. Priorities and QoS levels can be set by using SLAs (Service Level Agreements) between customer and provider networks.

However, SFTM can not use with other legacy secure VPLS architectures [1]–[3] since there is no mechanism available to get real-time network and traffic information. Such information is available only for SDN enabled VPLS networks.

B. Fast Transmission Mechanism (FTM) with Tunnel Resumption Procedure (TRP)

In [6], authors proposed a Tunnel Resumption Procedure (TRP) to reduce the tunnel establishment delay of subsequent tunnel establishments between already authorized and communicated PEs. For already registered PEs, the proposed FTM mechanism can be used with TRP as well. The proposed FTM with TRP is illustrated in Figure 3.

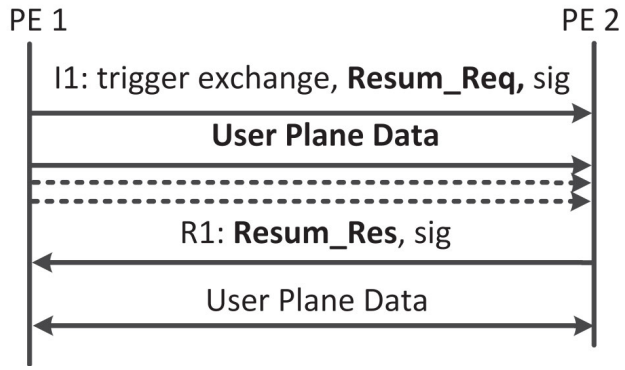

Fig. 3: Fast Transmission Mechanism (FTM) with Tunnel Resumption Procedure (TRP)

Here, user data are transmitted right after the sending the I1 message. In this case, PEs are not experiencing any tunnel establishment delay. The user data are transmitting as they are transmitted in a tunnel free environment. However, both PEs should satisfy both FTM and TRP criteria to use FTM with TRP.

V. Performance Evaluation

The performance of proposed FTM analyzed with simulation and testbed experiments.

A. Simulation Results

A network with 100 PEs is used as our reference network. The model network is generated by using stochastic Kronecker graphs [14]. We compared performance of FTM by integrating into existing secure VPLS architectures, namely HIPLS [1], S-HIPLS [11] and SDN VPLS [6] architectures.

In this experiment, we measured the average waiting time before starting the user traffic transmission. We selected two PEs and gradually increase the RTT (Round Trip Time) between the PEs. We measure the waiting time at the session initiating PE before transmitting the user data. Figure 4 illustrates the simulation results.

The simulation results (Figure 4) verify that proposed FTM has reduced the waiting time for all VPLS architectures. The reduction of waiting by one RTT helps to achieve at-least 50% performance advantage in all scenarios. As we expected, PEs are not experiencing any tunnel establishment delay for FTM with TRP in SDN VPLS scenario (Figure 3).

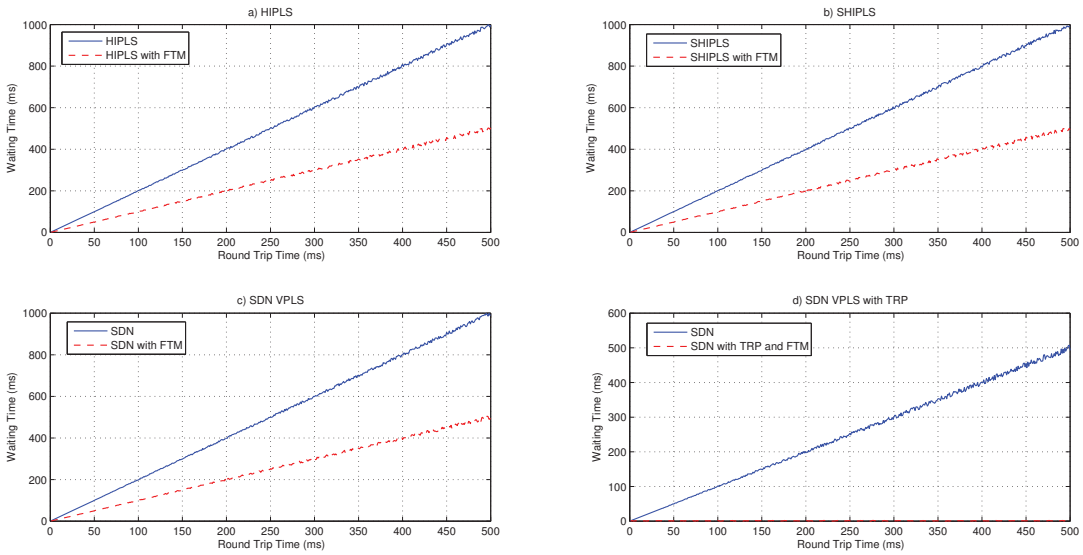

Fig. 4: The average waiting time before starting the file transmission

B. *Testbed Implementation*

The proposed solution was implemented in a testbed to analyze the real world performance and verify the feasibility of proposed mechanism. The experiment testbed is illustrated in Figure 5.

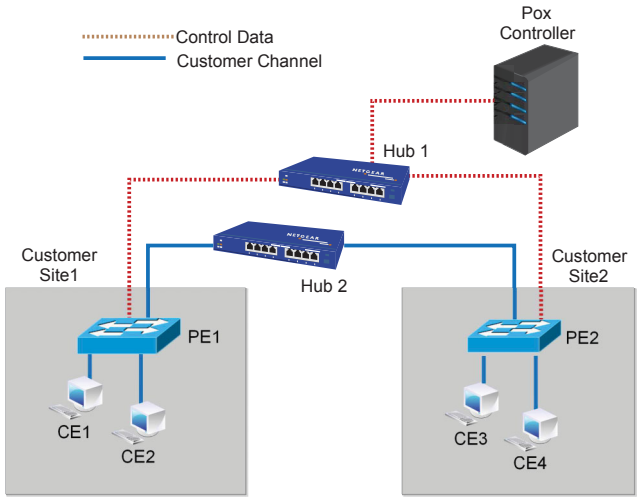

Fig. 5: The experiment testbed

We use three laptops and two Ethernet hubs in the testbed. In first two laptops, OpenVswitch (OVS) version 1.10.0 [15] is installed. These OpenFlow switches act as PE and each laptop has Intel i5-3210M CPU of 2.5GHz. Moreover, we implement two CEs in each of these laptops and each OVS represents PE for two customer sites. Moreover, we use OpenHIP implementation [16] to establish IPsec tunnels between PEs.

TABLE I: The Performance Comparison

	Average waiting time (ms)	**Performance Advantage of FTM**
HIPLS [1]	80.6578	
HIPLS [1] with FTM	42.6752	47.0910%
SHIPLS [11]	81.3541	
SHIPLS [11] with FTM	43.1254	46.9905%
SDN VPLS [6]	80.5457	
SDN VPLS [6] with FTM	41.9552	47.9113%
SDN VPLS [6] with TRP	44.5646	
SDN VPLS [6] with TRP and FTM	1.8545	95.8386%

The third laptop with a L2400 CPU of 1.66GHz works as the SDN controller. We used POX controller [17] as our controller and the latest POX controller [17] runs on this laptop. POX controller uses OpenFlow version 1.1.0 [18] to control SDN enabled PEs. A network with 100 Mbps bandwidth had established by using two D-LINK DSR-250N routers. Finally, we use OpenHIP implementation [16] to establish IPsec tunnels between PEs.

In the testbed experiment, we established communication sessions between CE1 and CE3 via the VPLS network. We measured the waiting time before transmitting the data. We compared the performance with other secure VPLS architectures, namely HIPLS [1], S-HIPLS [11] and SDN VPLS [6]. We ran the experiment for 100 times and average values are calculated. The experiment results are presented in Table I.

The experiment results verify that proposed FTM reduced

the waiting time of existing VPLS architectures by 46% - 47%. Moreover, FTM with TRP has almost zero waiting time and waiting time reduction is about 96%. Here, user data transmission can be started right after the transmission of first tunnel establishment message (i.e. I1 in Figure 3).

VI. Conclusion and Future Works

Ethernet based secure VPLS (Virtual Private LAN Services) networks require to establish a full mesh of VPLS tunnels between customer sites. However, the tunnel establishment between geographically distant customer sites introduces a significantly high waiting time to the user traffic transportation. Such long waiting times increase the traffic transport delay as well as reduces the QoS of short communication sessions. In this article, we proposed a novel Fast Transmission Mechanism (FTM) for secure VPLS architectures to reduce the waiting of user data transmission. It ultimately reduces the average data transmission delay between geographically distant customer sites.

The performance of proposed mechanism is analyzed with existing VPLS architectures by using a simulation model. Simulation results verified that proposed FTM reduced the waiting time of all the secure VPLS architectures. The reduction of waiting by one RTT helps to achieve at-least 50% performance advantage in all scenarios. Moreover, the proposed FTM was implemented in a testbed to analyze the real world performance and verify the feasibility of the proposed mechanism. The experiment results verified that proposed FTM reduced the waiting time of existing VPLS architectures by 46% - 47%. Moreover, FTM with Tunnel Resumption Procedure (TRP) has almost zero waiting time for SDN enabled VPLS networks.

Acknowledgment

This work has been performed in the framework of the SECUREConnect (Secure Connectivity of Future Cyber-Physical Systems), Naked Approach, Towards Digital Paradise and CENIIT 17.01 projects. This research is funded by Academy of Finland and TEKES, Finland.

References

[1] T. Henderson, S. Venema, and D. Mattes, "HIP-based Virtual Private LAN Service (HIPLS)," *Internet Draft*, IETF, December 2013.

[2] 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.

[3] 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.

[4] Tempered networks. [Online]. Available: http://www.temperednetworks.com/

[5] Tofino Security Appliance. [Online]. Available: http://www.tofinosecurity.com/products/tofino-security-appliance

[6] M. Liyanage, A. Gurtov, and M. Ylianttila, "Improving the Tunnel Management Performance of Secure VPLS Architectures with SDN," in *Proc. of IEEE Consumer Communications and Networking Conference (CCNC), Las Vegas, USA. IEEE.* IEEE, 2016.

[7] G. Keller and A. Beylot, "Improving flow level fairness and interactivity in WLANs using size-based scheduling policies," in *Proc. of the 11th international symposium on Modeling, analysis and simulation of wireless and mobile system*, 2008.

[8] K. Kompella and Y. Rekhter, "Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling," RFC 4761, IETF, January 2007.

[9] M. Lasserre and V. Kompella, "Virtual private LAN service (VPLS) using label distribution protocol (LDP) signaling," RFC 4762, IETF, January 2007.

[10] A. Sodder, K. Ramakrishnan, C. DelRegno, , and J. Wils, "Virtual Hierarchical LAN Services," *Internet Draft*, IETF, April 2003.

[11] M. Liyanage and A. Gurtov, "Securing Virtual Private LAN Service by Efficient Key Management," *Security and Communication Networks*, 2013.

[12] T. Henderson. Boeing HIP Secure Mobile Architecture. [Online]. Available: http://www.ietf.org/proceedings/73/slides/HIPRG-0.pdf

[13] M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Secure Virtual Private LAN Services: An Overview with Performance Evaluation," in *IEEE ICC 2015 - Workshop on Advanced PHY and MAC Techniques for Super Dense Wireless Networks*. IEEE, 2015, pp. 1–7.

[14] J. Leskovec, D. Chakrabarti, J. Kleinberg, C. Faloutsos, and Z. Ghahramani, "Kronecker graphs: An approach to modeling networks," *The Journal of Machine Learning Research*, vol. 11, pp. 985–1042, 2010.

[15] Open vSwitch: An Open Virtual Switch. [Online]. Available: http://openvswitch.org/

[16] "The OpenHIP project," http://www.openhip.org/.

[17] About POX. [Online]. Available: http://www.noxrepo.org/pox/about-pox/

[18] OpenFlow Switch Specification Version 1.1.0. [Online]. Available: http://archive.openflow.org/documents/openflow-spec-v1.1.0.pdf