Analysis of Deployment Challenges of Host Identity Protocol

Ijaz Ahmad*, Madhusanka Liyanage†, Mika Ylianttila‡ and Andrei Gurtov§
*†‡Centre for Wireless Communications (CWC), University of Oulu, Finland
§Department of Computer and Information Science, Linköping University, SE-581 83 Linköping, Sweden
Email: [*ijaz.ahmad,† madhusanka.liyanage, ‡mika.ylianttila]@oulu.fi, §gurtov@acm.org

***Abstract*—Host Identity Protocol (HIP), a novel internetworking technology proposes separation of the identity-location roles of the Internet Protocol (IP). HIP has been successful from the technological perspectives for network security and mobility, however, it has very limited deployment. In this paper we assess HIP to find the reasons behind its limited deployment and highlight the challenges faced by HIP for its commercial use. We propose technological development and outline deployment strategies for the wide use of HIP. Furthermore, this paper investigates the use of HIP in Software Defined Networks (SDN) to evaluate its performance in new disruptive networking technologies. In a nutshell, this paper presents revealing challenges for the deployment of innovative networking protocols and a way ahead for successful and large scale deployment.**

***Index Terms*—Host Identity Protocol, Mobile VPN, Security, Mobility, SDN**

I. Introduction

The TCP/IP suite uses IP addresses along with domain names for hosts' communication over the Internet. These IP addresses serve as both location identifiers and network interface identifiers at the same time [1]. The IP namespace worked well for stationary hosts but has serious limitations for mobile nodes and their security. These limitations give rise to three grave problems; first, changing the host address directly is not possible without interrupting transport layer connections. Second, there is no consistent and trust-able anonymity or privacy over the Internet. Third, the lack of proper authentication of datagrams and systems that leads to IP spoofing [2]. Therefore, various proposals have been put forward for proper host identification over the Internet.

Host Identity Protocol (HIP) [3], an internetworking architecture with the associated set of protocols enhances mobility and security by adding a namespace used between the IP layer and the transport protocols. The new namespace consists of a cryptographically derived host identifier which is also the public key of an asymmetric key-pair. Each host has at least one such host identity or more, though two hosts cannot have the same identity. The host identity can be public or unpublished and clients can have both public and unpublished identities at the same time. In few words, with the new namespace architecture HIP integrates IP Layer mobility, multi-homing and multi access, security, NAT traversal, and interoperability between IPv4 and IPv6.

As described in [2][3], HIP provides mobility, multi-homing and end-to-end security in a unanimous way by adding a host identity layer between the network and transport layers. With the use of cryptographic identifiers, accountability with building trust, privacy, and location anonymity to the trusted peers is assured. The protocols are carefully designed so that the currently deployed middle boxes work with the new architecture. These features make HIP based solutions foolproof against security breaches, assure mobility technologically, and minimize the involvement of network administrators. Indeed, HIP assures mobility and security, yet it has a limited deployment outside of the Virtual Private LAN (VPLS) segment.

Therefore, in this paper we explore the challenges that are on the forefront for the deployment and integration of HIP in current and new networking technologies. First, we make a comparative analysis of HIP with a competitive technology such as mobile Virtual Private Networks (VPNs) using legacy security and mobility technologies such as IPSec and mobile IP respectively. The reason why we chose mobile VPNs is described in Section II. Second, we integrate HIP in the OpenFlow [4] variant of Software Defined Network (SDN) to see its feasibility in future networks. This paper is organized as follows: Section II provides the comparative analysis of HIP with mobile VPNs. Section III studies the feasibility and integration of HIP into SDNs. Section IV presents the conclusion and future directions.

II. Comparative Analysis of HIP and Mobile VPN

To find the competitive shortcoming of HIP, we conduct a web-based survey from the experts of HIP and mobile VPNs for comparative analysis among the two. There are two reasons why we used mobile VPNs in the comparative analysis. First, mobile VPNs are widely used commercially that use IPsec or Mobile IP to provide secure and mobile connectivity to its users. Second, the same features could be competently provided by HIP-based solutions (e.g. HIP-based VPNs [5][6]).

VPNs provide secure communication to members of a company through the public telecommunication infrastructure while maintaining user privacy and security by utilizing encryption techniques, tunneling protocols and security procedures. In fact it provides an illusion of a complete private network which provides the same capabilities as a private network at comparatively low costs. Mobile VPN in theory

extends the authentication, access control procedures, confidentiality, and data integrity of VPNs to mobile users moving from one geographic location to another [7]. Moreover, mobile VPNs must provide continuous services to the mobile users by seamlessly switching across multiple connections regardless of the underlying heterogeneous technologies over different private and public networks [8].

Since mobile VPNs rely on Mobile IP for mobility, those have many challenges such as corruption of routing tables, replaying and blocking binding updates, bombing the Care-of-Address (CoA) and home agent with unwanted traffic [9], and triangulation problems [3] [10]. Albeit with these challenges, mobile VPNs are highly used for secure and remote connectivity. Therefore, we compare HIP as a mobility and Internet security solution with mobile VPN. The comparative assessment of HIP and mobile VPNs is aimed at finding the weaknesses of HIP which obstruct its adoption and hence commercial success.

A. Comparative Assessment

HIP and mobile VPN are compared in four carefully selected areas. These are mobility, security, costs and facilitating conditions. Mobility and security are the two main features of these technologies, whereas, cost of deployment and use, and facilitating conditions are the driving forces behind adopting any technology. Therefore, these four areas are considered as the main criteria for comparative assessment. Furthermore, these criteria are divided into sub-criteria as shown in Fig. 1 for thorough comparative analysis.

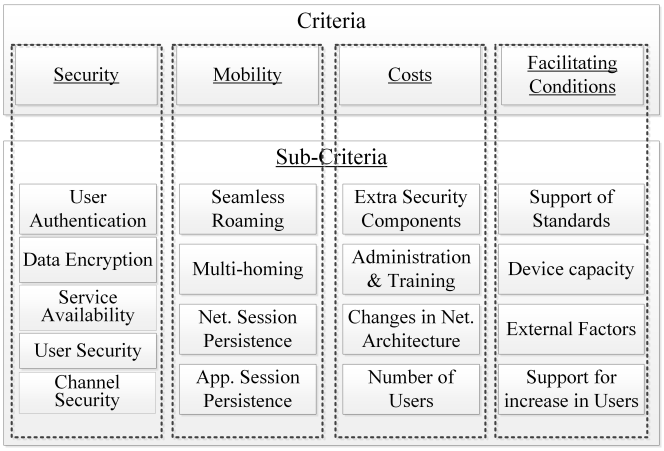

Fig. 1. Criteria and sub-criteria used in the comparative analysis.

The assessment of both solutions is based on a web-based survey that consists of questionnaire on mobility, security, costs and facilitating conditions with their important constituents shown in Fig. 1. The survey was conducted from the target group of technology experts in mobile VPNs and HIP products. We used Analytic Hierarchy Process (AHP) [11] which is a theory of measurement through pair-wise comparisons used to solve complex decision making problems. AHP is a method of Multi-Criteria Decision Making (MCDM) that helps decision makers to solve complex problems having multiple conflicting and subjective criteria.

The AHP model can be completely expressed in a hierarchical structure which shows the relationships of a goal, objectives or criteria and the alternatives. In our case, the goal, criteria and alternatives are as follows:

- ***Goal:*** Secure and seamless mobile communication system.
- ***Criteria:*** Security, mobility, costs and facilitating conditions with their sub-criteria shown in Fig. 1.
- ***Alternatives:*** HIP-based secure mobility solution and IP-based mobile VPNs.

AHP involves structuring multiple choice criteria into hierarchies to assess the relative importance of those criteria by comparing alternatives for each criterion and determining the overall rankings of the alternatives. The process is described below.

B. Relative ranking of Criteria and Sub-Criteria

In this study, the relative ranking comprises two steps. First, hierarchical ranking of the principle criteria. Second, hierarchical ranking of the sub-criteria under each principle criterion. All the rankings of principle and sub-criteria are based on the experts opinion. The AHP Saaty scale [11] given in Table 1, is used for the mathematical development of the hierarchical ranking of the criteria. A top down approach is used for proper ranking where the respondents were asked to provide relative importance of one criterion over the other and henceforth, for its sub-criteria.

TABLE I
SAATY SCALE USED FOR PAIR-WISE COMPARISON

Number	Description
1	Equal Importance, e.g. contribute equally to the objective
3	Moderate importance, e.g. slightly favor one activity over another
5	Strong importance, e.g. strongly favor one activity over another
7	Very strong importance, e.g. favor very strongly one activity over another
9	Extreme importance, e.g. the strongest favor of one activity over another
2,4,6,8	Intermediate values
Decimals	If the activities are very close and the difference may be small

Respondents of the survey were asked to choose numerical values as shown in Table 1, to prioritize/de-prioritize the four choices over each other. The average responses for each of the four principle criteria for relative ranking are:

- Security (*P1*) = 4.275
- Mobility (*P2*) = 3.875
- Facilitating Conditions (*P3*) = 3.125
- Costs (*P4*) = 2.625

We used the eigenvector method suggested by Thomas L. Saaty [11] to calculate the relative ranking. The judgment

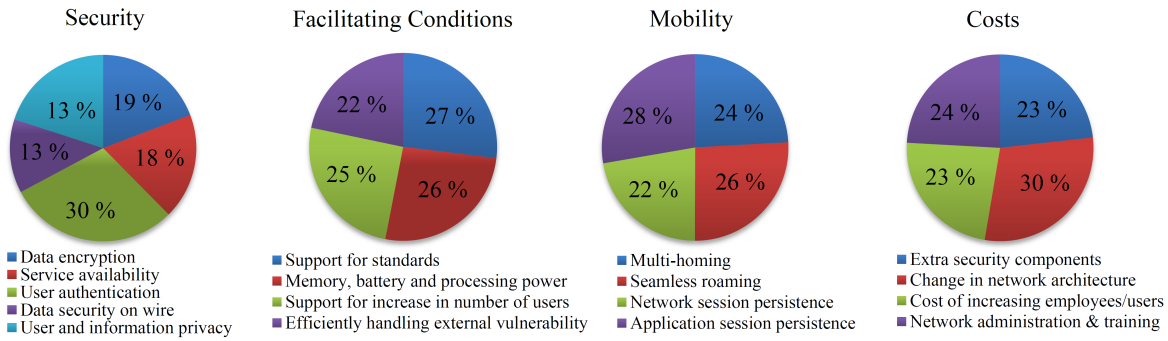

Fig. 2. Relative ranking of sub-criteria according to AHP

	Security	Mobility	Facilitating Conditions	Costs
Security	1	P_1/P_2	P_1/P_3	P_1/P_4
Mobility	P_2/P_1	1	P_2/P_3	P_2/P_4
Facilitating Conditions	P_3/P_1	P_3/P_2	1	P_3/P_4
Costs	P_4/P_1	P_4/P_2	P_4/P_3	1

Fig. 3. Judgment matrix of the four principle criteria.

matrix — giving the relative importance of one criterion over the other, is presented in Fig. 3.

Removing the fractions into decimals, the judgment matrix can be represented as

$$X_{ij} = \begin{pmatrix} 1.000 & 1.142 & 1.420 & 1.690 \\ 0.875 & 1.000 & 1.240 & 1.476 \\ 0.706 & 0.804 & 1.000 & 1.191 \\ 0.593 & 0.677 & 0.840 & 1.000 \end{pmatrix}. \quad (1)$$

The judgment matrix ***Xij*** can be row-wise normalized by following the row normalization as follows,

$$D_i = \frac{\sum_{j=1}^{n} X_{ij}}{\sum_{i=1}^{n}\sum_{j=1}^{n} X_{ij}}, \quad (2)$$

where n is the order of the matrix. Hence, the normalized eigenvector is,

$$D_i = [D_1, D_2, D_3, D_4]^T = [0.3150.2760.2220.186]^T. \quad (3)$$

To remove the possible inconsistency from the matrix, we have calculated the consistency check of the AHP process [20] as follows

$$CR = \frac{CI}{RI}, \quad (4)$$

where, *CR* is the consistency ratio, *CI* is the consistency index and *RI* is the random index, i.e. the average *CI* of randomly generated matrix of the same order. *CI* can be represented by the following formula,

$$CI = \frac{\lambda - n}{n - 1}, \quad (5)$$

where, λ is the dominant eigenvalue of n order matrix and calculated as

$$\lambda = \sum_{i=1}^{n} \frac{(XD)_i}{nD_i}, \quad (6)$$

Where, n = 4, and i = 1, 2, .. , 4.

After finding consistency with the help of equation 4, the normalized eigenvector ***D*** gives the priority ranking as follows,

$$D = \begin{pmatrix} Security \\ Mobility \\ FacilitatingConditions \\ Costs \end{pmatrix} = \begin{pmatrix} 0.315 \\ 0.276 \\ 0.222 \\ 0.187 \end{pmatrix}. \quad (7)$$

In AHP, the relative ranking is always in fractions and sums to one. The ranking can also be represented in terms of percentage and the sum must be 100%. A difference in fractions up to three decimal places can result in difference in percentage of above 1% in the principle criteria. Therefore, the decimal fractions are rounded up to three decimal digits resulting in clear ranking of the criteria. Equation 7 shows that security is the most important criterion followed by mobility and facilitating conditions. Cost is the last important criterion among the two to consider for choosing a solution or technology for Internet security and mobility.

The relative ranking of the sub-criteria is also calculated with the same procedure as described for the four principle criteria. For the sub-criteria fractions up to three decimal places are used, since the relative ranking is clear with sufficient percentage differences in three decimal digits. The percentile relative ranking for the sub-criteria in each of the principle criteria is shown in Fig. 2.

C. Pair-wise Comparison and Results

The next step was to evaluate the performance of both technologies in the criteria and sub-criteria. The comparison

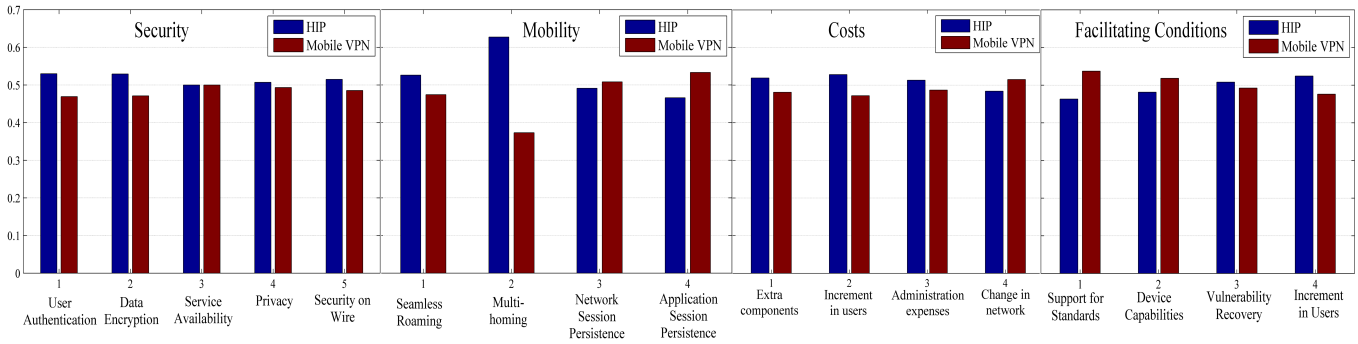

Fig. 4. Security of HIP and mobile VPNs

is based on the relative ranking of criteria, sub-criteria and the competence of both technologies in each of the sub-criteria. In the survey questionnaire, the experts had to provide numerical values for performance of both alternatives in each criterion and sub-criterion from the Saaty Scale[11]. Henceforth, we gathered the weights in numerical values for the relative hierarchical ranking and efficiency of both solutions.

The end results of the efficiency of both technologies can be found by multiplying the pair-wise comparison results of the alternatives with its ranking. The results of the experts' opinion for the pair-wise comparison of the alternatives is presented in Fig. 4. The output of the whole comparison process is presented in Table II.

To summarize, the results of the comparative analysis of HIP with mobile VPN solutions suggest that HIP-based solutions provide better security and mobility. In few words, HIP performs better in security by 3.58 %, in mobility by 5.260 %, and are cost effective by 1.940 %. The only criterion in which HIP based solutions lag by 1.940 % behind mobile VPN solutions is the facilitating conditions. Furthermore, HIP also lags behind mobile VPNs in some of the constituents of mobility and costs as shown in Table II.

The results suggest that HIP has better support for security and mobility. However, facilitating conditions are not favorable for its deployment. Knowing that HIP has comparatively less commercial use, one can conclude that facilitating conditions play a vital role in the deployment of networking protocols, and in our case, HIP. There is higher support of industry standards for mobile VPNS and the devices are more suitable for mobile VPNs than HIP. This means that the broad use of HIP will be possible after its acceptance by the vendors, operators, ISPs and the public to strengthen the availability of resources required for its deployment and usage.

D. Reservations

In the relative ranking, high comparative ranking (e.g. security and mobility in our case) causes bigger impact on the overall results, making one alternative lead over the other with high margin (HIP in our case). This could cause unintentional bias towards a particular alternative or feature. Furthermore, respondents of the survey are expert professionals who have experience with both technologies i.e, HIP and mobile VPNs.

TABLE II
OUTPUT OF THE COMPARISON OF HIP AND MOBILE VPNS

Criteria/ Sub-criteria	Preferred Alternative	Percentile Difference
Security	**HIP**	**3.58** %
Sub-criteria		
Data encryption	HIP	1.12 %
Service availability	HIP, mobile VPN	0.00 %
User Authentication	HIP	1.80 %
Security on wire	HIP	0.38 %
Privacy	HIP	0.28 %
Mobility	**HIP**	**5.26** %
Sub-criteria		
Multi-homing	HIP	6.13 %
Seamless roaming	HIP	1.36 %
Network session persistence	mobile VPN	0.38 %
Application session persistence	mobile VPN	1.85 %
Facilitating Conditions	**mobile VPN**	**1.41** %
Sub-criteria		
Support for standards	mobile VPN	2.00 %
Device capabilities	mobile VPN	0.97 %
Increment in users	HIP	1.20 %
Vulnerability recovery	HIP	0.36 %
Costs	**HIP**	**1.94** %
Sub-criteria		
Extra security components	HIP	0.90 %
Change in network architecture	mobile VPN	0.91 %
Increment in users	HIP	1.32 %
Administration costs	HIP	0.63 %
Total Performance	**HIP**	**2.63** %

Having experience in IPSec-based security, mobile IP-based mobility, HIP, and commercial values of protocols at the same time restricts the number of respondents (11 respondents). However, we were able to draw some conclusions regarding limitations of HIP in terms of requirements for successful deployment and commercial use.

III. HIP IN FUTURE TECHNOLOGIES

A. HIP in Disruptive Technologies

We believe that HIP has the potential to be used in current and emerging networking technologies. HIP solves the basic architectural flaw related to identity by making a split in the identity/location roles of IP addresses while providing secure and unique identity to users. It refurbishes the identity concept such that it does not eliminate the use of IP addresses but

rather enhances it, making HIP backward and forward compatible [3]. The difference which HIP brings to the network security and mobility arena is huge while its technical design brings it much closer to the existing solutions in terms of least pain in changing the existing platforms and updating them [3]. A strong advantage of HIP architecture when compared with other technologies is its capability to function without changes to existing IP routers [2].

HIP has been implemented for Linux based systems [12], Microsoft systems [13], sensor networks [14], mobile platforms [15], lightweight hardware [16], RFIDs [17], and has been used in mobile ad hoc networks (MANETs) [18]. The InfraHIP project was devoted to develop the infrastructure for the wide utility of HIP. The Development of Tofino Endbox solution for SCADA networks [19] is one of the major breakthroughs of HIP-based solutions. Boeing Inc. had been keen in developing secure communication infrastructure for its production and operation lines and is using HIP based Endboxes in the Secure Mobile Architecture (SMA) [20]. Similarly, Tampared Networks used HIP in their network security products such as the Conductor and HIPswitch to provide security to critical infrastructures. The devices have successfully reduced the cyber attack surface by about 90% [21].

Since HIP cleanly separates host-to-host signaling and data traffic into separate planes, it has the appeal to be used in architectures where data is separated from the control. Therefore, HIP can be used in the new architectures of the Internet such as SDN. We discuss the use of HIP in SDN in the following section.

B. SDN and HIP

SDN separates the network control plane from the data forwarding plane [22]. The control plane is logically centralized in software-based SDN controllers that maintain global view of the network. This offers greater flexibility, control, programmability and automation of the network equipment. The SDN architecture uses two communication channels, i.e. control and data channels. The control channel is used for control signaling between the control and data planes, whereas, user communication is transported via the data channel. However, SDN faces a number of security challenges in which the controller-datapath communication is on the forefront [23].

The most widely used standard of SDN, i.e. the OpenFlow [4], uses Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) for the controller switch communication. However, the configuration of TLS is so complex that its use left optional leaving the control channel open to security vulnerabilities [23]. Furthermore, it is demonstrated in [24] that TLS cannot provide protection against TCP-level attacks. We believe that HIP can solve the security challenges of the control-data planes communication in SDN as demonstrated in [25], [26], [27]. Therefore, we integrate HIP in OpenFlow and perform experiments using HIP as a control channel between the OpenFlow controller and OpenFlow switch to show the feasibility of HIP in SDNs.

C. Performance of HIP in OpenFlow Networks

To evaluate the performance of HIP in OpenFlow, we integrated HIP with OpenFlow in a testbed comprising two OpenFlow switches controlled by the SDN controller. We Implemented OpenVswitch version 1.10.0 in two laptops to work as virtual OpenFlow switches. In a third laptop, the Python based POX controller [28] is implemented that controls the OpenVswitches. The controller and OpenVswitches are connected by using one D-LINK DSR-250N router and another D-LINK DSR-250N router is used to establish data channel communication between OpenVswitches. Moreover, the OpenHIP implementation [29] is used to establish HIP tunnels for both control and data channels. Furthermore, we connect attackers to each router according to the experiment scenarios. The attacker is a laptop with an i5-3210M CPU of 2.5GHz processor that performed IP based attacks such as TCP DoS and TCP reset attacks. We measured the performance by using the IPERF network measurement tool [30].

In the first experiment, we measure the impact of TCP reset attack on control channel connection establishment delay between the OpenFlow controller and the OpenFlow switch in different settings for establishing the existing secure connection with SSL and secure control channel with HIP. The attack is performed for 50% of the simulation time. The results shown in Fig. 5 reveal that secure control channel with HIP is secured from TCP reset attacks. However, the existing SDN control channel with TLSv1 is vulnerable to TCP reset attack.

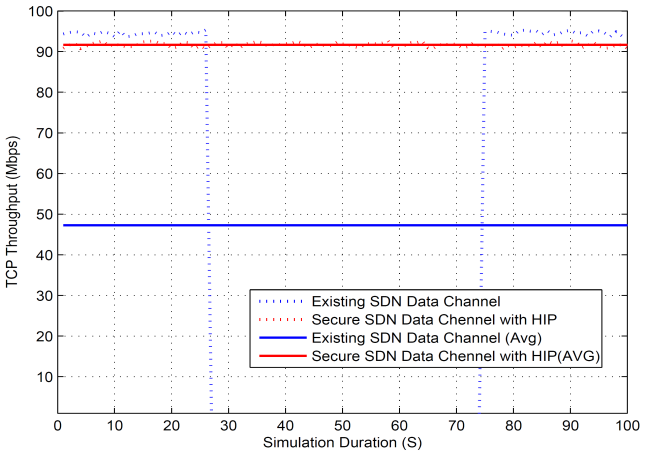

Fig. 5. Impact of TCP DoS attack

In the second experiment, we measure the impact of TCP DoS attack on data channel between two OpenFlow switches in different settings for establishing the existing SDN data channel and secure data channel with HIP. The attack is performed for 50% of the simulation time. The results shown in Fig. 6 reveal that secure data channel with HIP is secured from TCP DoS attacks. However, the existing SDN data channel is vulnerable to TCP DoS attack.

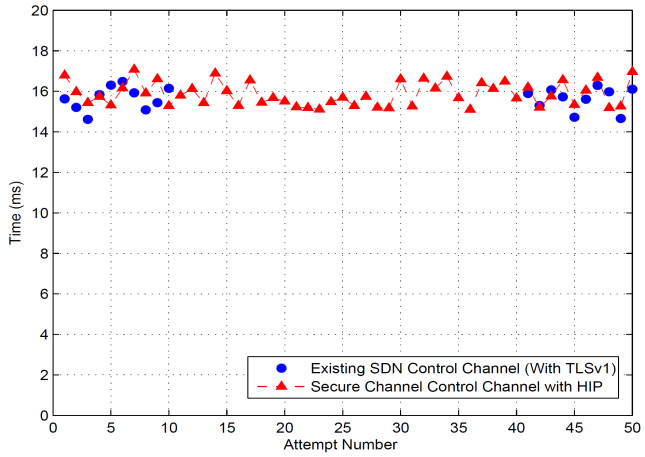

Fig. 6. Impact of TCP reset attack

IV. Conclusions

This paper investigates the weaknesses and strengths of HIP for deployment in current and future networking technologies. To find the reasons of its limited deployment, we conducted a web-based survey from the experts of HIP and IP-based mobile VPNs to make a comparative assessment. The results show that HIP has better technological features to solve the challenges of Internet security and mobility with less costs. However, facilitating deployment conditions such as industrial support and capabilities of devices for the use of HIP are not as favorable as for its competitors. Nevertheless, HIP can be easily integrated into novel networking technologies such as SDN. To show its feasibility, we integrated HIP for securing the SDN control and data communication channels. Besides easy integration, the results show that HIP provides more security for the control and data channels than the currently used security mechanisms for communication in SDN. Therefore, this paper reveals that network protocol developers need to pay attention to facilitating conditions for the deployment of a protocol besides its useful technological features.

Acknowledgment

This work was supported by TEKES Finland and Academy of Finland under projects: The Naked Approach, Towards Digital Paradise and SecureConnect. Andrei Gurtov was supported by the Center for Industrial Information Technology (CENIIT).

References

[1] R. Moskowitz, "Host Identity Protocol Architecture," 2012.
[2] A. Gurtov, *Host Identity Protocol (HIP): towards the secure mobile internet*. Wiley, 2008, vol. 21.
[3] P. Nikander, A. Gurtov, and T. R. Henderson, "Host Identity Protocol (HIP): Connectivity, mobility, multi-homing, security, and privacy over IPv4 and IPv6 networks," *Communications Surveys & Tutorials, IEEE*, vol. 12, no. 2, pp. 186–204, 2010.
[4] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "OpenFlow: Enabling innovation in campus networks," *ACM SIGCOMM Computer Communication Review*, vol. 38, no. 2, pp. 69–74, 2008.
[5] T. Henderson, S. Venema, and D. Mattes, "HIP-based Virtual Private LAN Service (HIPLS)," *Internet Draft*, IETF, November 2014.
[6] M. Liyanage and A. Gurvov, "Securing Virtual Private LAN Service by Efficient Key Management," *Security and Communication Networks*, 2013.
[7] A. A. Jaha, F. Ben Shatwan, and M. Ashibani, "Proper Virtual Private Network (VPN) Solution," in *Next Generation Mobile Applications, Services and Technologies, 2008. NGMAST'08. The Second International Conference on*. IEEE, 2008, pp. 309–314.
[8] A. V. Uskov, "Information security of mobile VPN: Conceptual models and design methodology," in *Electro/Information Technology (EIT), 2012 IEEE International Conference on*. IEEE, 2012, pp. 1–6.
[9] B. Hayat and S. Alam, "Mobile IP: enabling user mobility," *Ubiquity*, vol. 2006, no. December, p. 2, 2006.
[10] J. Chandrasekaran, "Mobile IP: Issues, Challenges and Solutions," Ph.D. dissertation, Master's thesis, Department of Electrical and Computer Engineering Rutgers University, 2009.
[11] T. L. Saaty, "Decision making with the Analytic Hierarchy Process," *International Journal of Services Sciences*, vol. 1, no. 1, pp. 83–98, 2008.
[12] L. Journals, "Host Identity Protocol for Linux." [Online]. Available: http://www.linuxjournal.com/magazine/host-identity-protocol-linux
[13] OpenHIP, "Host Identity Protocol for Windows." [Online]. Available: http://www.openhip.org/wiki/index.php?title=Windows_Installation
[14] A. Khurri, D. Kuptsov, and A. Gurtov, "On application of host identity protocol in wireless sensor networks," in *7th International Conference on Mobile Adhoc and Sensor Systems (MASS)*. IEEE, 2010, pp. 358–345.
[15] A. Khurri, D. Kuptsov, and A. Gurtov, "Performance of Host Identity Protocol on Symbian OS," in *Communications 2009. ICC'09. IEEE International Conference on*. IEEE, 2009, pp. 1–6.
[16] A. Khurri, E. Vorobyeva, and A. Gurtov, "Performance of Host Identity Protocol on lightweight hardware," in *Proceedings of 2nd ACM/IEEE international workshop on Mobility in the evolving internet architecture*. ACM, 2007, p. 4.
[17] P. Urien, H. Chabanne, M. Bouet, D. De Cunha, V. Guyot, G. Pujolle, P. Paradinas, E. Gressier, and J.-F. Susini, "HIP-based RFID networking architecture," in *Wireless and Optical Communications Networks, 2007. WOCN'07. IFIP International Conference on*. IEEE, 2007, pp. 1–5.
[18] J. Campos, C. T. Calafate, M. Nácher, P. Manzoni, and J.-C. Cano, "HOP: achieving efficient anonymity in MANETs by combining HIP, OLSR, and pseudonyms," *EURASIP J. Wirel. Commun. Netw.*, vol. 2011, pp. 975–985, jan 2011.
[19] TofinoSecurity, "Security For SCADA and Industrial Process Control System," Portable Tofino. [Online]. Available: http://tofinosecurity.com
[20] R. H. Paine, "Secure Mobile Architecture (SMA)–A way to fix the broken Internet," *Information Security Technical Report*, vol. 12, no. 2, pp. 85–89, 2007.
[21] Tampered Networks products. [Online]. Available: http://www.temperednetworks.com/
[22] M. Liyanage, A. Gurtov, and M. Ylianttila, *Software Defined Mobile Networks (SDMN): Beyond LTE Network Architecture*. John Wiley & Sons, 2015.
[23] I. Ahmad, S. Namal, M. Ylianttila, and A. Gurtov, "Security in Software Defined Networks: A Survey," *Communications Surveys Tutorials, IEEE*, vol. PP, no. 99, pp. 1–1, 2015.
[24] M. Liyanage, A. Abro, M. Ylianttila, and A. Gurtov, "Opportunities and Challenges of Software-Defined Mobile Networks in Network Security Perspective," *IEEE Security and Privacy Magazine*, 2015.
[25] S. Namal, I. Ahmad, A. Gurtov, and M. Ylianttila, "Enabling Secure Mobility with OpenFlow," in *Future Networks and Services (SDN4FNS), 2013 IEEE SDN for*, Nov 2013, pp. 1–5.
[26] M. Liyanage, I. Ahmed, M. Ylianttila, J. L. Santos, R. Kantola, O. L. Perez, M. U. Itzazelaia, E. M. d. Oca, A. Valtierra, and C. Jimenez, "Security for future software defined mobile networks," in *2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies*, Sept 2015, pp. 256–264.
[27] M. Liyanage, A. Braeken, A. D. Jurcut, M. Ylianttila, and A. Gurtov, "Secure communication channel architecture for software defined mobile networks," *Computer Networks*, vol. 114, pp. 32 – 50, 2017.
[28] noxrep. (2009, Nov.) POX: OpenFlow Controller. [Online]. Available: http://www.noxrepo.org/pox/about-pox/
[29] The OpenHIP project. [Online]. Available: http://www.openhip.org/
[30] A. Tirumala, F. Qin, J. Dugan, J. Ferguson, and K. Gibbs, "Iperf: The TCP/UDP bandwidth measurement tool," *http://dast.nlanr.net/Projects*, 2005.