ISSN 2278-3091
Volume 8, No.5, September - October 2019
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse20852019.pdf
https://doi.org/10.30534/ijatcse/2019/20852019

A Comprehensive Survey on Vertical Handover Security Attacks during Execution Phase

Dr. Omar Khattab
Assistant Professor, Dept. of Computer Science & Engineering, Kuwait College of Science and Technology
Doha, Kuwait

ABSTRACT

The Mobile Users' demand (MUs) in getting Always Best Connected (ABC) is on the increase by using different Radio Access Technologies (RATs): Wi-Fi, GSM (2G), UMTS (3G), LTE (4G) and 5G. To fulfill the ABC, three phases of Vertical Handover (VHO) are required: Initiation, Decision and Execution. The importance of the security factor particularly arises during the execution phase where the mobility management protocols are taken place: Mobile IPv4 (MIPv4) and Mobile IPv6 (MIPv6). This paper therefore surveys the current research initiatives on VHO security attacks during execution phase in order to precisely identify the active security challenges.

Key words: Heterogeneous Wireless, Mobile Networks, Vertical Handover Security, Wireless Networks

1. INTRODUCTION

The procedure which permits Mobile Users (MUs) to maintain their ongoing sessions when either moving within the same Radio Access Technology (RAT) or traversing different RATs, is named Horizontal Handover (HHO) and Vertical Handover (VHO), respectively. This is shown in Figure 1. As there is no one RAT can satisfy MUs' preferences in securing Always Best Connected (ABC) anywhere anytime, both of HHO and VHO are highly important to complement each other in order to enhance continuing MUs growth, as shown in Figure 2.

During MUs' movements to new locations, the VHO might be triggered and therefore using mobility management protocols in this case are required to securely and seamlessly maintain the ongoing session during execution phase. This paper surveys the current research initiatives on VHO security attacks during execution phase in order to precisely identify the active security challenges.

The rest of the paper is organized as follows: Section 2 presents related works of VHO security attacks. Section 3 presents a background of mobility management: Mobile IPv4 (MIPv4) and Mobile (MIPv6).

In section 4, a comparison of VHO security attacks during execution phase is presented. Finally, a conclusion work is given in section 5.

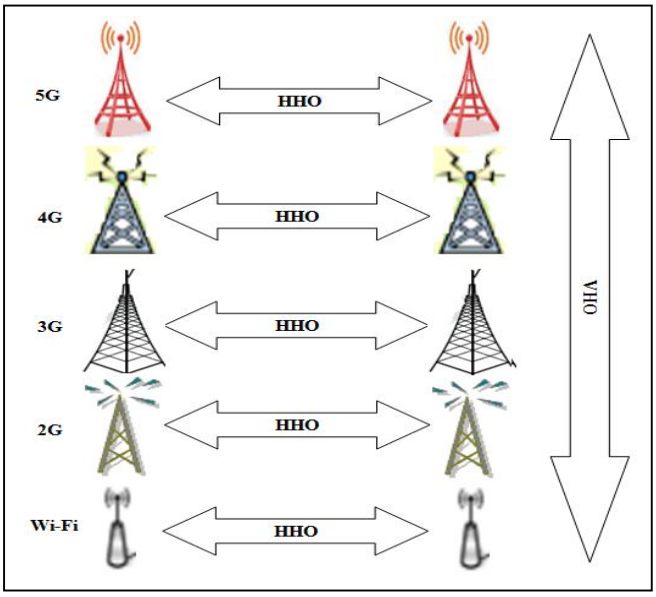

Figure 1: HHO vs. VHO

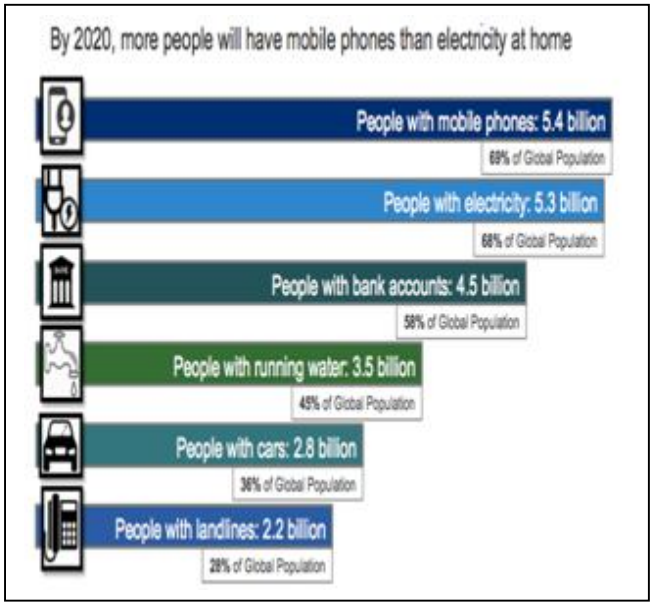

Figure 2: Mobile Growth Continues through 2020 [1]

2. RELATED WORKS OF VHO SECURITY ATTACKS

Although in [2] there are 132 VHO approaches have been reviewed, only (7%) of them have considered the VHO security. However, we conclude that the majority works of this modest percentage of VHO security have mainly focused on the role of security parameter in selecting the best available RAT for decision phase (i.e., 5%), whereas the rest of works have mainly confined on the Denial of Service (DoS) attack for execution phase (i.e., 2%). This is shown in Figure 3.

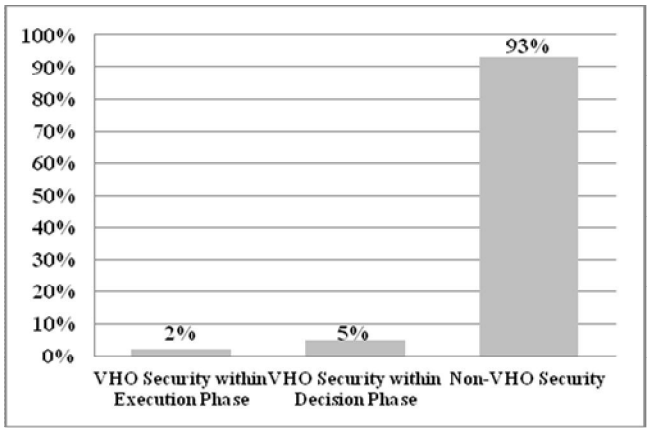

Figure 3: Previous Works Percentage of VHO Security vs. Non-VHO Security

3. BACKGROUND OF MOBILITY MANAGEMENT

There are two main types of mobility scenarios during MU's movements:

- *HHO (Homogeneous, Intra-System, Micro Mobility)*

The HHO is typically taken place when the Radio Signal Strength (RSS) of the active access point becomes unavailable to the MU as a result of its degradation.

- *VHO (Heterogeneous, Inter-System, Macro Mobility)*

Unlike homogeneous, the RSS is insufficient for making handover in the heterogeneous RATs as it relies on RSS besides several parameters such as coverage area, data rate, security and cost. The VHO procedure includes three main phases: Initiation (Collecting Information), Decision and Execution [3, 4, 5, 6 and 7], as explained below.

A. Handover Initiation

This phase is responsible to collect all necessary information for decision phase which is classified in terms of the following parameters: (a) network (e.g., latency and coverage area), (b) user's preferences (e.g., cost and security) and (c) terminal (e.g., battery and velocity).

B. Handover Decision

This phase is responsible for selecting the most suitable RAT among all available RATs and informing the next phase accordingly. The selected RAT will be based on the collected parameters from the initiation phase.

C. Handover Execution

Once a VHO decision is made and a new RAT is selected, this phase will be responsible to securely and seamlessly keep ongoing session (i.e., packets) for the MU on the new RAT taking into consideration the MU's authentication. Finally, the resources of the old RAT are eventually released.

Security is the major drawback during the execution phase. It is particularly arose when the MUs move between different RATs while the hackers strive to steal their confidential information (e.g., passwords and bank account details) during their handover to the new RAT. This is shown in Figure 4. The execution phase can be implemented by mobility management protocols such as MIPv4 and MIPv6.

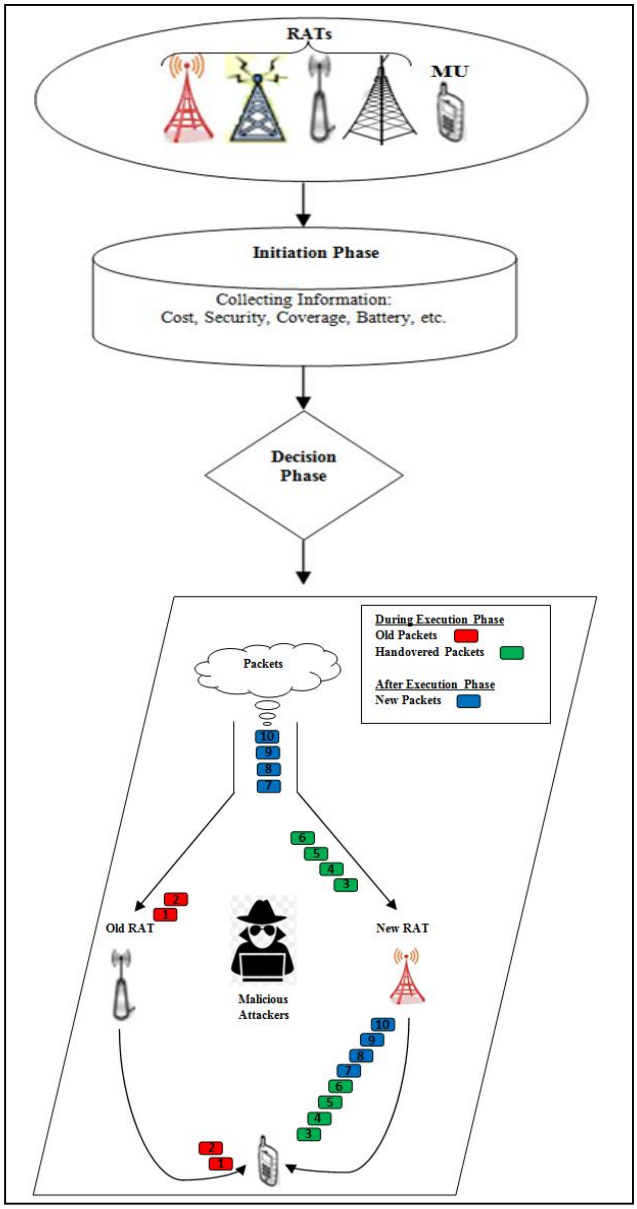

Figure 4: Diagram of Vertical Handover Security Attacks during Execution Phase

1. MIPv4

The most Internet traffic these days relies on the IPv4 as it is the first version of Internet protocol [8]. Although IPv4 provides over than 4 billion addresses, it is not able to accommodate the future requirements in increasing number of devices (e.g., Personal Computers (PCs), laptops, mobiles, Personal Digital Assistants (PDAs)).

The IPv4 does not provide any built-in security mechanism which results in exploiting such a drawback in order to start malicious attacks: sniffing attacks, flooding attacks, application layer attacks and man-in-the-middle attacks [8].

2. MIPv6

The IPv6 is the expected successor to the IPv4 where the main goal of the IPv6 is to offer larger addressing space compared with the IPv4 [9]. Although IPv6 provides built-in security mechanism via IP Security (IPSec), the IPv6 is still vulnerable to the security threats: firewall evasion by fragmentation, header manipulation, smurf attack (broadcast amplification attack), host initialisation attack and reconnaissance attack [8].

4. COMPARISON OF VHO SECURITY ATTACKS

The Public key is one of the most available methods to address the security of RATs [10]. In Section 2, we have reviewed 132 VHO recent approaches found in the literature which have been classified into two categories: VHO security works and non-VHO security works. In Section 3, we have presented security threats posed to IPv4 and IPv6 which make VHO execution phase at risk.

To offer a systematic survey in this paper, we present a fair comparison between MIPv4 and MIPv6 in terms of the following criteria: Security, VHO Security Attacks in the Previous Works, Previous Works Percentage of VHO Security Attacks, Identifying the Current Types of VHO Security Attacks and Active Research Area. This is shown in Table 1.

As for the "Security" criteria, it is obvious that MIPv6 is more secure than MIPv4 as it provides built-in security mechanism via IPSec.

For "VHO Security Attacks in the Previous Works" criteria, the DoS is the sole attack which has been considered under MIPv6. Whereas there is no attack has been considered under MIPv4.

In terms of "Previous Works Percentage of VHO Security Attacks" criteria, it is noticed that there is a shortage of VHO security works as the VHO security attacks under MIPv6 score 2% (out of 7%). Whereas there is no previous work of VHO security attacks has been considered under MIPv4. This is shown in Figure 5.

For "Identifying the Current Types of VHO Security Attacks" criteria, The MIPv6 encounters various attacks: fragmentation, header manipulation, smurf (broadcast amplification), host initialisation and reconnaissance. Whereas the MIPv4 encounters: DoS, sniffing, flooding, application layer and man-in-the-middle.

Table 1: A Comparative Summary of the VHO Security Attacks during Execution Phase: MIPv4 vs. MIPv6

Mobility Management Protocols	Security	VHO Security Attacks in the Previous Works	Previous Works Percentage of VHO Security Attacks	Identifying the Current Types of VHO Security Attacks	Active Research Area
MIPv6	High	DoS	2%	1. Fragmentation 2. Header Manipulation 3. Smurf (Broadcast Amplification) 4. Host Initialisation 5. Reconnaissance	Yes
MIPv4	Less	-	0%	1. DoS 2. Sniffing 3. Flooding 4. Application Layer 5. Man-in-the-Middle	Yes

Finally, in the "Active Research Area" criteria, the MIPv6 requires future work improvements for addressing the current types of attacks before using it during VHO execution phase. Whereas, the MIPv4 is also an active research area as it is still widely used.

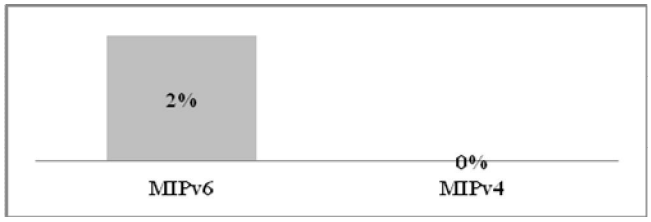

Figure 5: Previous Works Percentage of VHO Security Attacks: MIPv4 vs. MIPv6

5. CONCLUSION

This paper has surveyed the current research initiatives on VHO security attacks during execution phase in order to precisely identify the active security challenges. We have discussed plenty VHO approaches found in the literature which have been classified into two categories: VHO security works and non-VHO security works. Then, we have presented security threats posed to IPv4 and IPv6 which make VHO execution phase at risk. It is concluded that there is a shortage of VHO security works for addressing the current types of attacks during execution phase. This makes VHO security an active research area.

REFERENCES

1. Growth in Smart Devices, Mobile Video, and 4G Networks to Drive Eight-Fold Increase in Mobile Data Traffic over the Next Five Years. https://newsroom.cisco.com/press-release-content?articleId=1741352. Accessed on Aug 26, 2019.
2. O. Khattab, **An Overview of VHO Security vs. VHO Non-Security in Mobile Networks: Approaches**, *IOSR Journal of Electronics and Communication Engineering*, vol. 13, no. 2, Ver. I, pp. 72-75, Mar 2018.
3. M. Zekri, B. Jouaber and D. Zeghlache, **Context Aware Vertical Handover Decision Making in Heterogeneous Wireless Networks**, *35th Conference on Local Computer Networks 2010 (LCN 2010)*, 10-14 Oct 2010, pp. 764-768. https://doi.org/10.1109/LCN.2010.5735809
4. K. Meriem, K. Brigitte and P. Guy, **An Overview of Vertical Handover Decision Strategies in Heterogeneous Wireless Networks**, *Computer Communications*, vol. 31, no. 10, pp. 2607-2620, 25 Jun 2008. https://doi.org/10.1016/j.comcom.2008.01.044
5. E. Stevens-Navarro and V.W.S. Wong, **Comparison between Vertical Handoff Decision Algorithms for Heterogeneous Wireless Networks**, *63rd Vehicular Technology Conference (VTC 2006)*, vol. 2, 7-10 May 2006, pp. 947-951. https://doi.org/10.1109/35.968811
6. P.M.L. Chan, R.E. Sheriff, Y.F. Hu, P. Conforto and C. Tocci, **Mobility Management Incorporating Fuzzy Logic for Heterogeneous a IP Environmen**, *IEEE Communications Magazine*, vol. 39, no. 12, Dec 2001, pp. 42-51.
7. W.T. Chen, J.C. Liu and H.K. Huang, **An Adaptive Scheme for Vertical Handoff in Wireless Overlay Networks**, *10th International Conference on Parallel and Distributed Systems 2004 (ICPADS 2004)*, 7-9 Jul 2004, pp. 541-548.
8. A. Ahmed and H. Hasan, **A Comparative Study on IPV4 and IPV6**, *International Journal of Advanced Research (IJAR)*, vol. 6, no. 4, pp. 1073-1083, Apr 2018. https://doi.org/10.21474/IJAR01/6953
9. H. Steffen and F. Benjamin, **A Comparison of Internet Protocol (IPv6) Security Guidelines**, *Future Internet*, vol. 6, no. 1, pp. 1-60, Apr 2015. https://doi.org/10.3390/fi6010001
10. P. Singh and N.S. Gill, **A Secure and Power-Aware Protocol for Wireless Ad Hoc Networks**, *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 8, no. 1, pp. 34-41, Jan-Feb 2019. https://doi.org/10.30534/ijatcse/2019/07812019