Computers, Materials & Continua
DOI: 10.32604/cmc.2022.026102
Article

Tech Science Press

Enhance Vertical Handover Security During Execution Phase in Mobile Networks

Omar Khattab*

Department of Computer Science and Engineering, Kuwait College of Science and Technology (KCST), Kuwait
*Corresponding Author: Omar Khattab. Email: o.khattab@edu.salford.ac.uk
Received: 15 December 2021; Accepted: 22 February 2022

Abstract: The Vertical Handover (VHO) is one of the most vital features provided for the heterogeneous mobile networks. It allows Mobile Users (MUs) to keep ongoing sessions without disruption while they continuously move between different Radio Access Technologies (RATs) such as Wireless Fidelity (Wi-Fi), Global System for Mobile Communication (GSM), Universal Mobile Telecommunications System (UMTS), Long Term Evolution (LTE) and Fifth Generation (5G). In order to fulfill this goal, the VHO must comply to three main phases: starting of collecting the required information and then passing it for decision phase to obtain the best available RAT for performing VHO by execution phase eventually. However, the execution phase still encounters some security issues which are exploited by hackers in launching malicious attacks such as ransomware, fragmentation, header manipulation, smurf, host initialization, reconnaissance, eavesdropping, Denial of Service (DoS), spoofing, Man in the Middle (MITM) and falsification. This paper thoroughly studies the recent security issues for hundreds VHO approaches found in the literature and comes up with a secure procedure to enhance VHO security during execution phase. A numerical analysis results of the proposed procedure are effectively evaluated in terms of security and signaling cost. Compared with the recent related work found in literature, the analysis demonstrates that the security is successfully improved by 20% whereas signaling cost is maintained as in non-proposed procedure.

Keywords: Vertical handover security; mobile networks; wireless networks; heterogeneous wireless networks

1 Introduction

Maintaining ongoing sessions over heterogeneous mobile networks is becoming an essential demand for the MUs during their movements. This process of switching between different RATs is referred to as VHO which is implemented via Initiation Phase (IP), Decision Phase (DP) and Execution Phase (EP) [1–8]. There are three main types of information which should be considered for securing seamless VHO, as shown in Fig. 1: a) network's parameters such as latency and coverage area, b) MU's preferences parameters such as cost of service and security and c) terminal's parameters such as battery

and velocity. The operators always strive to make a balance between MU's preferences and optimum use of the network by making a seamless VHO as much as possible. This helps operators in attracting more number of subscribers and hence increasing their profit accordingly. However, the security as one of the most critical parameters from MU's side must be considered carefully by the operators. Therefore, this paper thoroughly studies the recent security issues for hundreds VHO approaches found in the literature and proposes a secure procedure to enhance VHO security during execution phase. The rest of the paper is organized as follows: In Section 2, related works are presented. In Section 3, a design of the proposed procedure is presented. In Section 4, a numerical analysis is presented. In Section 5, performance evaluation and results discussion are presented. Finally, a conclusion is given in Section 6.

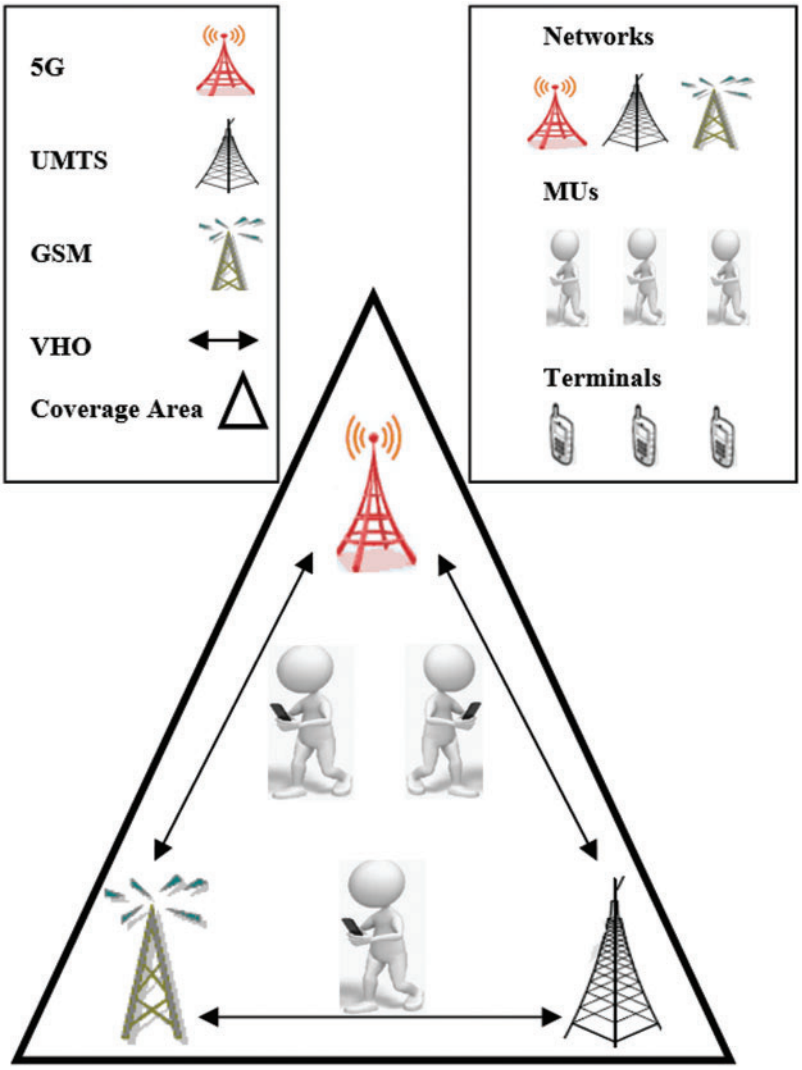

Figure 1: Main VHO parameters: networks, MUs and terminals

2 Related Works

In this section, 174 previous works have been considered. In [9], 132 VHO research works have been classified into two main categories: VHO security based category and VHO non-security based category. It has been concluded in [9] that the VHO non-security category presented a modest number of previous works (7%). In [10–21], many recent VHO research works have been proposed which also have not considered VHO security. In [22], 22 security mechanisms proposed on securing the Mobile IPv6 handover have been surveyed [23–44]. It has been concluded in [22] that it is still vulnerable to various malicious activities. In [45], a new proactive security algorithm for upcoming sensitive connection between heterogeneous mobile networks was proposed: Proactive Security for Upcoming Sensitive Connection (PSUSC). The PSUSC algorithm descendingly orders all available RATs in terms of security into two levels [2], as shown in Tab. 1. When the VHO is triggered for a security session, the PSUSC's priority is to secure the upcoming sensitive session and it therefore selects the best available secure RAT, taking into consideration that the sole VHO to 5G (L1) is dynamically taken place without MUs' confirmation. Otherwise, the MU could confirm proceeding VHO from available L2's RATs. An analysis of the PSUSC algorithm for the decision phase has proved reducing potential attacks compared with previous works which rely on using less secure RAT. However, no performance evaluation or validation provided about the execution phase where attackers may lunch their malicious attacks due to using less secure RAT in sending sensitive date, as shown in Fig. 2. Some security issues have been surveyed in [46]: fragmentation, header manipulation, smurf (broadcast amplification), host initialization and reconnaissance. Besides eavesdropping, DoS, spoofing, MITM, falsification and ransomware in [47–51] and [52], respectively.

Table 1: Security comparison of RATs [45]

RAT	Generation	Security	Metric (M)	Level (L)
5G	Fifth	Higher	5	One
LTE	Fourth	High	4	Two
UMTS	Third	Less high	3	
WiMAX	Fourth	Medium	2	
GSM	Second			
Wi-Fi	–	Low	1	

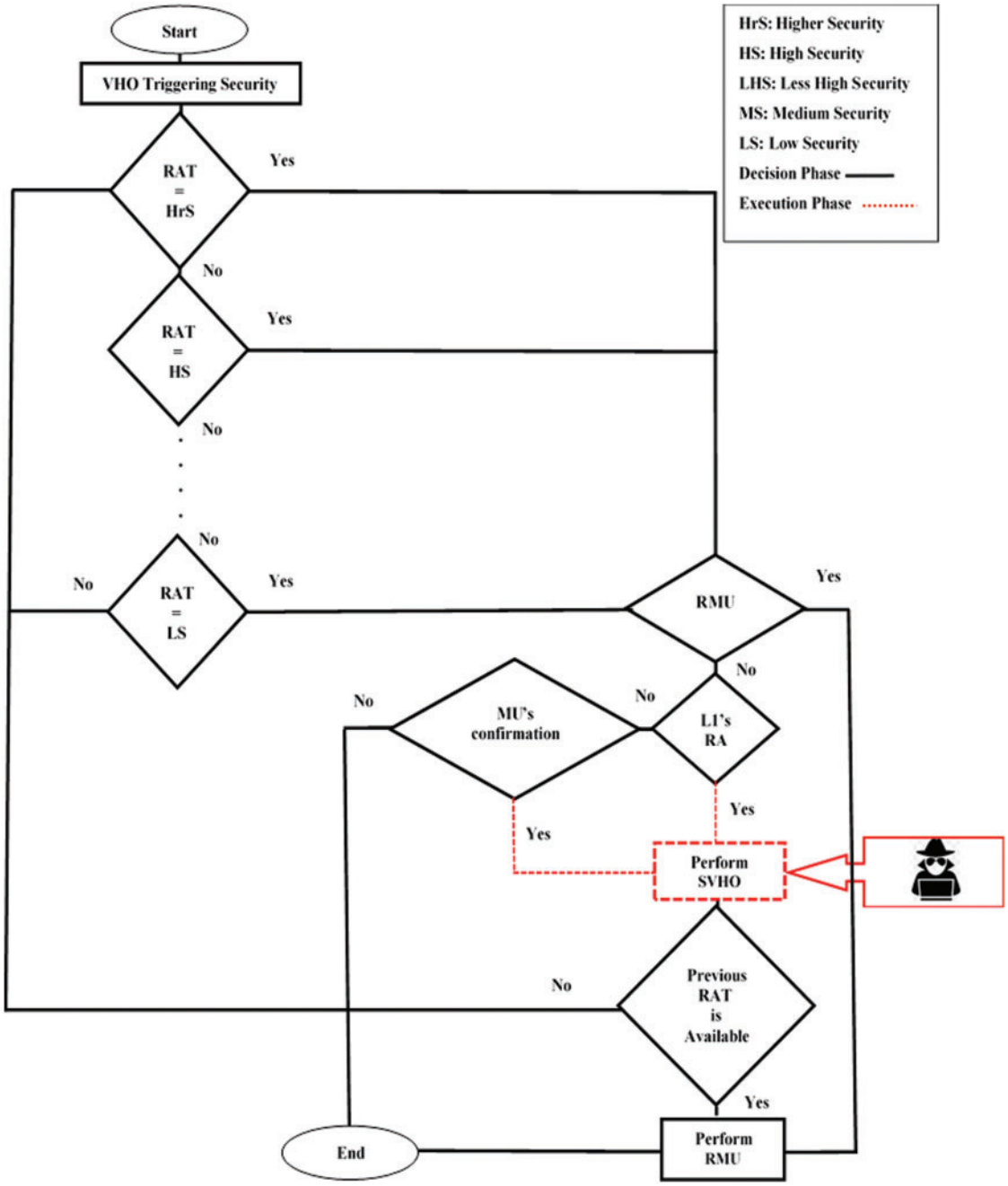

Figure 2: The penetrated PSUSC algorithm [45]

3 Design of Proposed Procedure

In Section 2, hundreds VHO approaches have been surveyed. It has been noticed that only [45] has considered a proactive security for upcoming sensitive connection in decision phase. However, no performance evaluation or validation provided about the execution phase where attackers may lunch

their malicious attacks due to using less secure RAT in sending sensitive date. Therefore, for VHO execution phase, this section proposes a secure procedure compared with non-proposed procedure [45] which relies on using less secure RAT. This is shown Fig. 3, where the green arrows are referred to the proposed procedure and the orange arrows are referred to the non-proposed procedure. Once the VHO is triggered for a security session, instead of sending MU's sensitive packets over old less secure RAT (steps: 2, 3, 4: MU-Old RAT-Internet-Corresponding Node (CN)), while VHO is taking place (step: 1: Old RAT-New RAT), the proposed procedure sends concurrent signals to inform both of VHO to start its phases (step: 1a: Old RAT-New RAT) and MU to make use of the VHO period to start buffering MU's sensitive packets (step: 1b: MU). After that the MU starts to sending its sensitive packets over secure RAT to the CN (steps: 2, 3, 4: MU-New RAT-Internet-CN).

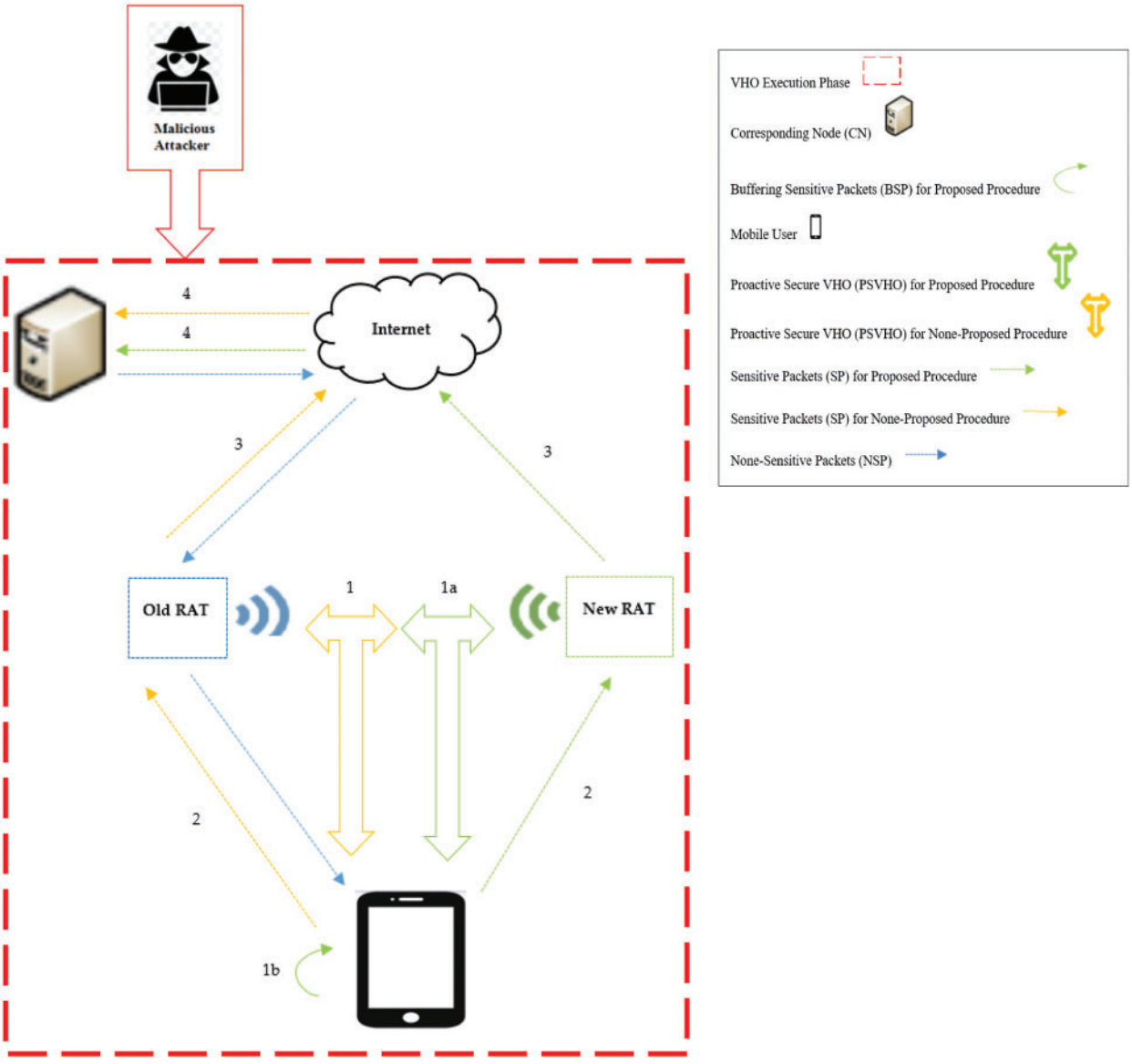

Figure 3: The design of proposed procedure

4 Numerical Analysis

In this section, a numerical analysis for security and signaling cost is presented in order to evaluate the performance of the proposed procedure during the VHO execution phase compared with non-proposed procedure. This is shown in Fig. 4.

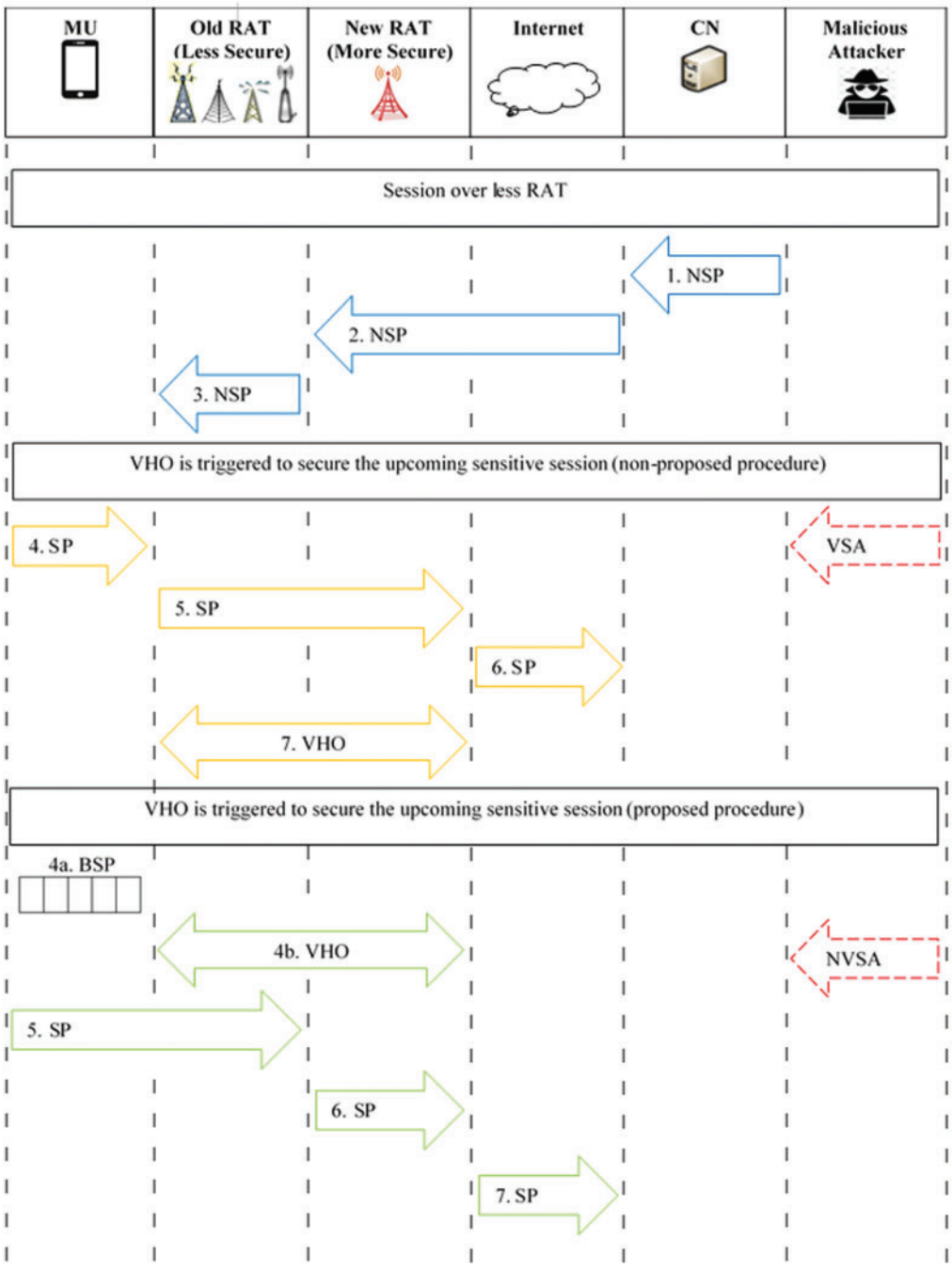

Figure 4: The analysis of proposed procedure *vs.* non-proposed procedure

The signaling cost of each of two procedures is as follows:

a. None-proposed procedure

$$VSA\_sc = SP + SP + SP + IP + DP + EP \tag{1}$$

where VSA_sc, SP, IP, DP and EP are referred to signaling cost of Vulnerable Session Attacks, Sensitive Packet, Initiation Phase, Decision Phase and Execution Phase, respectively.
From (1),

$$VSA\_sc = 3SP + 3Ps \tag{2}$$

where Ps is referred to Phases
From (2),

$$VSA\_sc = 3SP + VHO \tag{3}$$

b. Proposed procedure

$$NVSA\_sc = IP + DP + EP + SP + SP + SP \tag{4}$$

where $NVSA\_{sc}$ is referred to signaling cost of None-Vulnerable Session Attacks.
From (4),

$$NVSA\_sc = 3Ps + 3SP \tag{5}$$

From (5),

$$NVSA\_sc = VHO + 3SP \tag{6}$$

The security of each of two procedures is as follows:

a. None-proposed procedure

$$VSA\_sec = (VHOxM) - PSVHO \tag{7}$$

where VSA_sec is referred to security of Vulnerable Session Attacks. M is referred to Metric (5, 4, 3, 2, 1 to 5G, LTE, UMTS, (WiMAX, GSM) and WiFi, respectively). $PSVHO$ is referred to Proactive Secure VHO and it is assumed to be 3 (VHO phases).

b. Proposed procedure

$$NVSA\_sec = (VHOxM) \tag{8}$$

where $NVSA\_sec$ is referred to security of None-Vulnerable Session Attacks.

5 Performance Evaluation and Results Discussion

In this section, the performance of security and signaling cost of the two procedures: proposed procedure and none-proposed procedure are evaluated where four VHO scenarios between RATs are considered: Wi-Fi to 5G, Wi-Fi to LTE, Wi-Fi to UMTS and Wi-Fi to WiMAX/GSM.

From Tab. 2, it can be seen that the security is successfully improved by 20% compared with none-proposed procedure, as shown in Figs. 5–8. This obviously due to early buffering sensitive packets. From Tab. 3, it can be seen that the signaling cost is maintained as in non-proposed procedure, as shown in Fig. 9.

Table 2: Parameters of VHO security

	RATs	VHO	M	PSVHO
Proposed procedure $NVSA\_sec = (VHO \times M)$	Wi-Fi to 5G	3	5	–
	Wi-Fi to LTE	3	4	–
	Wi-Fi to UMTS	3	3	–
	Wi-Fi to WiMAX/GSM	3	2	–
None-proposed procedure $VSA\_sec = (VHO \times M) - PSVHO$	Wi-Fi to 5G	3	5	3
	Wi-Fi to LTE	3	4	3
	Wi-Fi to UMTS	3	3	3
	Wi-Fi to WiMAX/GSM	3	2	3

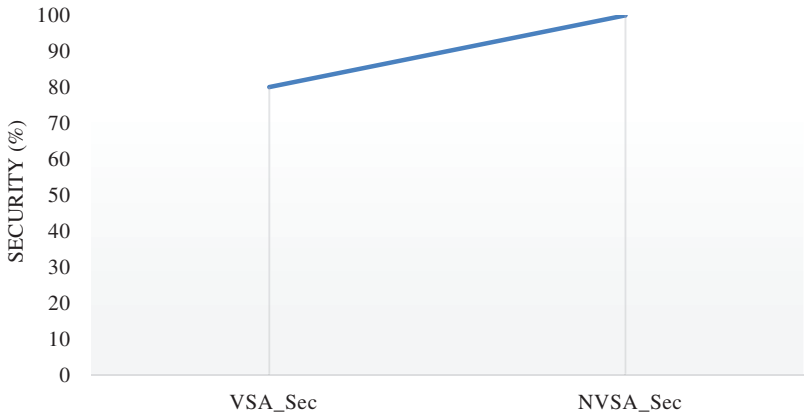

Figure 5: VHO from Wi-Fi to 5G

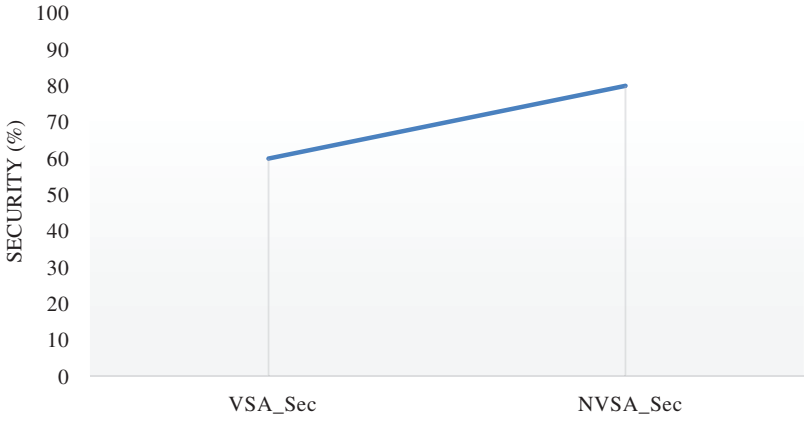

Figure 6: VHO from Wi-Fi to LTE

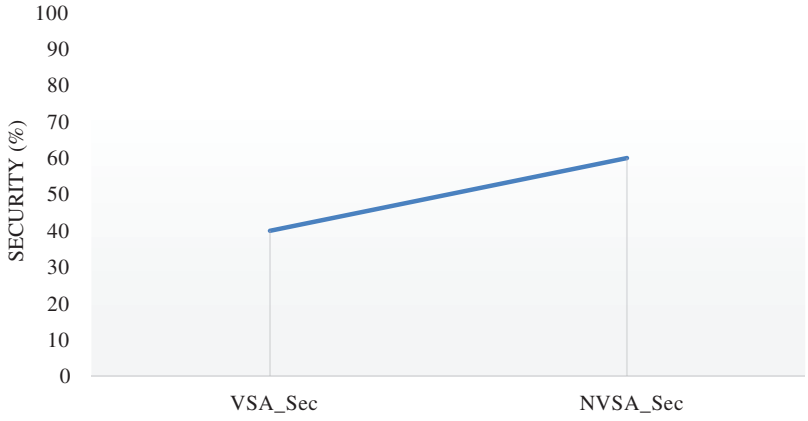

Figure 7: VHO from Wi-Fi to UMTS

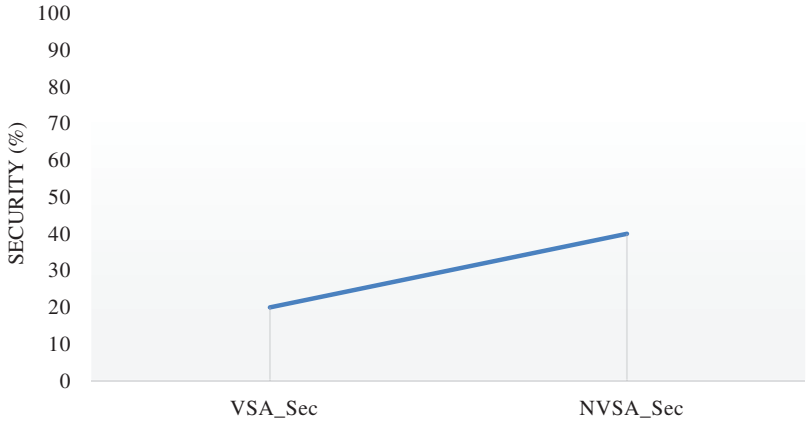

Figure 8: VHO from Wi-Fi to WiMAX/GSM

Table 3: Parameters of VHO signaling cost

	RATs	VHO	SP
Proposed procedure $NVSA\_sc = VHO + 3SP$	Wi-Fi to 5G	3	3
	Wi-Fi to LTE	3	3
	Wi-Fi to UMTS	3	3
	Wi-Fi to WiMAX/GSM	3	3
None-proposed procedure $VSA\_sc = 3SP + VHO$	Wi-Fi to 5G	3	3
	Wi-Fi to LTE	3	3
	Wi-Fi to UMTS	3	3
	Wi-Fi to WiMAX/GSM	3	3

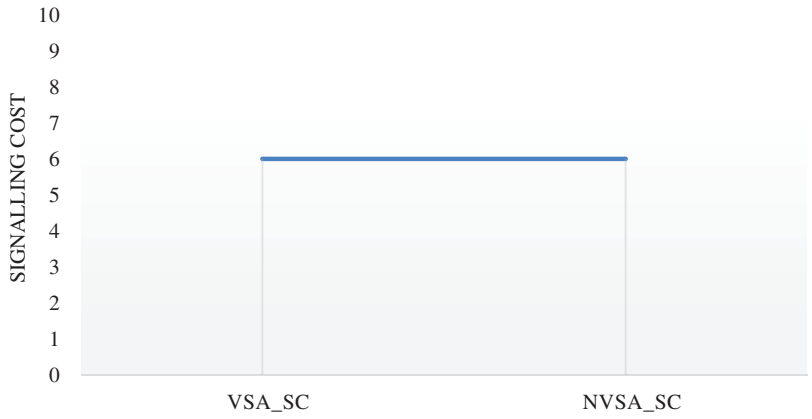

Figure 9: Signaling cost: proposed procedure *vs.* non-proposed procedure

6 Conclusion

In this paper, the recent security issues for hundreds VHO approaches have been surveyed thoroughly. It has been noticed that the VHO execution phase still encounters some security issues which are exploited by hackers in launching malicious attacks due to using less secure RAT in sending sensitive date. Therefore, the paper came up with a secure procedure to enhance VHO security during execution phase. A numerical analysis results of the proposed procedure were effectively evaluated against non-proposed procedure in terms of security and signaling cost. The results showed that the security was successfully improved by 20% whereas signaling cost was maintained as in non-proposed procedure.

Funding Statement: The author received no specific funding for this study.

Conflicts of Interest: The author declares that he has no conflicts of interest to report regarding the present study.

References

[1] M. Zekri, B. Jouaber and D. Zeghlache, "Context ware vertical handover decision making in heterogeneous wireless networks," in *35th Conf. on Local Computer Networks (LCN)*, Denver, CO, USA, pp. 764–768, 2010.

[2] M. Kassar, B. Kervella and G. Pujolle, "An overview of vertical handover decision strategies in heterogeneous wireless networks," *Computer Communications*, vol. 31, no. 10, pp. 2607–2620, 2008.

[3] E. Stevens-Navarro and V. W. S. Wong, "Comparison between vertical handoff decision algorithms for heterogeneous wireless networks," in *63rd VehicularTechnology Conf. (VTC)*, Melbourne, VIC, Australia, pp. 947–951, 2006.

[4] P. M. L. Chan, R. E. Sheriff, Y. F. Hu, P. Conforto and C. Tocci, "Mobility management incorporating fuzzy logic for heterogeneous a IP environment," *IEEE Communications Magazine*, vol. 39, no. 12, pp. 42–51, 2001.

[5] W. T. Chen, J. C. Liu and H. K. Huang, "An adaptive scheme for vertical handoff in wireless overlay networks," in *10th Int. Conf. on Parallel and Distributed Systems (ICPADS)*, Newport Beach, CA, USA, pp. 541–548, 2004.

[6] J. McNair and F. Zhu, "Vertical handoffs in fourth-generation multinetwork environments," *IEEE Wireless Communications*, vol. 11, no. 3, pp. 8–15, 2004.
[7] Y. Gyekye-Nkansah and J. Agbinya, "Vertical handoffs decision algorithms using fuzzy logic," in *Int. Conf. on Wireless Broadband and Ultra Wideband Communications*, Sydney, Australia, pp. 1–5, 2006.
[8] D. Sourav, R. Amitava and B. Rabindranath, "Design and simulation of vertical handover algorithim for vehicular communication," *International Journal of Engineering Science and Technology*, vol. 2, no. 10, pp. 5509–5525, 2010.
[9] 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, pp. 72–75, 2018.
[10] D. Wang, Q. Sun, Y. Wang, X. Han and Y. Chen, "Network-assisted vertical handover scheme in heterogeneous aeronautical network," in *Asia-Pacific Conf. on Image Processing, Electronics and Computers (IPEC)*, Dalian, China, pp. 148–152, 2020.
[11] S. Goutam and S. Unnikrishnan, "QoS based vertical handover decision algorithm using fuzzy logic," in *Int. Conf. on Nascent Technologies in Engineering (ICNTE)*, Navi Mumbai, India, pp. 1–7, 2019.
[12] A. Debnath and N. Kumar, "Simple additive weighted algorithm for vertical handover in heterogeneous network," in *2nd phd Colloquium on Ethically Driven Innovation and Technology for Society (PhD EDITS)*, Bangalore, India, pp. 1–2, 2020.
[13] S. Goutam, S. Unnikrishnan and A. Karandikar, "Algorithm for vertical handover using multi attribute decision making techniques," in *Int. Conf. on Communication, Networks and Satellite (Comnetsat)*, Batam, Indonesia, pp. 306–313, 2020.
[14] N. A. Ezz-Eldien, M. F. Abdelkader, M. I. Abdalla and H. M. Abdel-Atty, "Handover performance improvement in heterogeneous wireless network," in *11th IEEE Annual Information Technology, Electronics and Mobile Communication Conf. (IEMCON)*, Vancouver, BC, Canada, pp. 821–830, 2020.
[15] S. Goutam, S. Unnikrishnan and N. Kudu, "Decision for vertical handover using k-means clustering algorithm," in *Bombay Section Signature Conf. (IBSSC)*, Mumbai, India, pp. 31–35, 2020.
[16] Z. Y. Wu, M. Ismail, E. Serpedin and J. Wang, "Artificial intelligence for smart resource management in multi-user mobile heterogeneous RF-light networks," *IEEE Wireless Communications*, vol. 28, no. 4, pp. 152–158, 2021.
[17] H. T. Yew, A. Chekima, A. Kiring, A. I. Mbulwa, J. A. Dargham *et al.,* "RSS based vertical handover schemes in heterogeneous wireless networks: Past, present & future," in *IEEE 2nd Int. Conf. on Artificial Intelligence in Engineering and Technology (IICAIET)*, Kota Kinabalu, Malaysia, pp. 1–5, 2020.
[18] M. Beshley, N. Kryvinska, O. Yaremko and H. Beshley, "A Self-optimizing technique based on vertical handover for load balancing in heterogeneous wireless networks using Big data analytics," *Applied Sciences*, vol. 11, no. 11, pp. 1–24, 2021.
[19] H. Tong, T. Wang, Y. Zhu, X. Liu, S. Wang *et al.,* "Mobility-aware seamless handover with MPTCP in software-defined HetNets," *IEEE Transactions on Network and Service Management*, vol. 18, no. 1, pp. 498–510, 2021.
[20] X. Tan, G. Chen and H. Sun, "Vertical handover algorithm based on multi-attribute and neural network in heterogeneous integrated network," *EURASIP Journal on Wireless Communications and Networking*, vol. 2020, pp. 1–21, 2021.
[21] L. Tuyisenge, M. Ayaida, S. Tohme and L. E. Afilal, "A mobile internal vertical handover mechanism for distributed mobility management in VANETs," *Vehicular Communications*, vol. 26, pp. 100277, 2020.
[22] S. Praptodiyono, T. Firmansyah, M. Alaydrus, M. Iman Santoso, A. Osman *et al.,* "Mobile IPv6 vertical handover specifications, threats and mitigation methods: A survey," *Security and Communication Networks*, vol. 2020, pp. 1–18, 2020.
[23] R. H. Deng, J. Zhou and F. Bao, "Defending against redirect attacks in mobile IP," in *9th ACM Conf. on Computer and Communications Security*, Berlin, Heidelberg, pp. 59–67, 2002.
[24] K. Ren, "Routing optimization security in mobile IPv6," *Computer Networks*, vol. 50, no. 13, pp. 2401–2419, 2006.

[25] S. K. Mathi and M. Valarmathi, "A secure and decentralized registration scheme for IPv6 network-based mobility," *Computer Networks*, vol. 5, no. 5, pp. 4247–4256, 2013.
[26] S. Rajkumar, M. Ramkumar Prabhu and A. Sivabalan, "Securing binding updates in routing optimizaton of mobile IPv6," *Research Journal of Applied Sciences, Engineering and Technology*, vol. 4, no. 12, pp. 1633–1636, 2012.
[27] J. D. Koo, J. Koo and D. C. Lee, "A new authentication scheme of binding update protocol on handover in mobile IPv6 networks," in *Int. Conf. on Embedded and Ubiquitous Computing*, Korea, pp. 972–978, 2006.
[28] J. D. Koo and D. C. Lee, "Extended ticket-based binding update (ETBU) protocol for mobile IPv6 (MIPv6) networks," *IEICE Transactions on Communications*, vol. 90, no. 4, pp. 777–787, 2007.
[29] D. Kavitha, E. Murthy and S. Hug, "A secure route optimization protocol in mobile IPv6," *International Journal of Computer and Network Security (IJCSNS)*, vol. 9, no. 3, pp. 27–34, 2009.
[30] W. A. A. Alsalihy and M. S. S. Alsayfi, "Integrating identity based encryption in the return routability protocol to enhance signal security in mobile IPv6," *Wireless Personal Communications*, vol. 68, no. 3, pp. 655–669, 2013.
[31] S. Mathi and M. Valarmathi, "An enhanced binding update scheme for next generation internet protocol mobility," *Journal of Engineering Science and Technology*, vol. 13, no. 3, pp. 573–588, 2018.
[32] S. Mathi, "A certificateless public key encryption based return routability protocol for next-generation IP mobility to enhance signalling security and reduce latency," *Sadhana*, vol. 42, no. 12, pp. 1987–1996, 2017.
[33] Y. C. Chen and F. C. Yang, "An efficient MIPv6 return routability scheme based on geometric computing," *International Journal of Electrical and Information Engineering*, vol. 3, no. 3, pp. 437–442, 2009.
[34] G. O'shea and M. Roe, "Child-proof authentication for MIPv6 (CAM)," *ACM SIGCOMM Computer Communication Review*, vol. 31, no. 2, pp. 4–8, 2001.
[35] I. You, J. H. Lee and B. Kim, "CATBUA: Context-aware ticketbased binding update authentication protocol for trust-enabled mobile networks," *International Journal of Communication Systems*, vol. 23, no. 11, pp. 1382–1404, 2010.
[36] C. Vogt, R. Bless, M. Doll and T. Kuffner, "Early binding updates for mobile IPv6," in *Wireless Communications and Networking Conf.*, New Orleans, LA, USA, pp. 1440–1445, 2005.
[37] F. Al Hawi, C. Y. Yeun and K. Salah, "Secure framework for the return routability procedure in MIPv6," in *Int. Conf. on Green Computing and Communications (GreenCom)*, Beijing, China, pp. 1386–1391, 2013.
[38] H. Kim and J. H. Lee, "Diffie-hellman key based authentication in proxy mobile IPv6," *Mobile Information Systems*, vol. 6, no. 1, pp. 107–121, 2010.
[39] H. Modares, "Enhancing security in mobile IPv6," *Electronics and Telecommunications Research Institute (ETRI)*, vol. 36, no. 1, pp. 51–61, 2014.
[40] L. Zhang, L. J. Zhang and S. Pierre, in *Performance Analysis of Seamless Handover in Mobile IPv6-Based Cellular Networks*, Burlingto, USA: InTech, 2011 [Online]. Available https://www.intechopen.com/chapters/14761.
[41] M. Alnas, I. Awan and R. D. W. Holton, "Performance evaluation of fast handover in mobile IPv6 based on linklayer information," *Journal of Systems and Software*, vol. 83, no. 10, pp. 1644–1650, 2010.
[42] L. Wang and G. S. Kuo, "Mathematical modeling for network selection in heterogeneous wireless networks – a tutorial," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 1, pp. 271–292, 2013.
[43] S. Wang, C. Fan, C. H. Hsu, Q. Sun and F. Yang, "A vertical handoff method via self-selection decision tree for internet of vehicles," *IEEE Systems Journal*, vol. 10, no. 3, pp. 1183–1192, 2016.
[44] H. Modares, A. Moravejosharieh, J. Lloret and R. Salleh, "A survey of secure protocols in mobile IPv6," *Journal of Network and Computer Applications*, vol. 39, no. c, pp. 351–368, 2014.
[45] O. Khattab, "A new secure algorithm for upcoming sensitive connection between heterogeneous mobile networks," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 12, no. 7, pp. 705–709, 2021.
[46] O. Khattab, "A comprehensive survey on vertical handover security attacks during execution phase," *International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE)*, vol. 8, no. 5, pp. 1965–1968, 2019.

[47] S. Lakshmanan, C. L. Tsao, R. Sivakumar and K. Sundaresan, "Securing wireless data networks against eavesdropping using smart antennas," in *Int. Conf. on Distributed Computing Systems ICDCS'08*, Bandung, Indonesia, Beijing, China, pp. 19–27, 2008.
[48] D. R. Raymond and S. F. Midkiff, "Denial-of-service in wireless sensor networks: Attacks and defenses," *IEEE Pervasive Computing*, vol. 7, no. 1, pp. 74–81, 2008.
[49] B. Kannhavong, "A survey of routing attacks in mobile ad hoc networks," *IEEE Wireless Communications*, vol. 14, no. 5, pp. 85–91, 2007.
[50] U. Meyer and S. Wetzel, "A Man-in-the-middle attack on UMTS," in *3rd ACM Workshop on Wireless Security*, PA, USA, pp. 90–97, 2004.
[51] T. Ohigashi and M. Morii, "A practical message falsification attack on WPA," *JWIS*, vol. 14, pp. 1–12, 2009.
[52] T. R. Reshmi, "Information security breaches due to ransomware attacks-a systematic literature review," *International Journal of Information Management Data Insights*, vol. 1, no. 2, pp. 100013, 2021.