

A New Secure Algorithm for Upcoming Sensitive Connection between Heterogeneous Mobile Networks

Omar Khattab

Department of Computer Science and Engineering
Kuwait College of Science and Technology (KCST), Doha, Kuwait

Abstract—One of the most important concepts in the heterogeneous mobile networks is Vertical Handover (VHO). The VHO is a vital process taken place by Mobile Users (MUs) in order to satisfy their preferences of security and cost, in addition to the rest of parameters of network and terminal such as latency and velocity, respectively. However, a proactive security for upcoming sensitive connection and performing VHO between heterogeneous mobile networks have not been considered. This paper therefore comes up with a new secure algorithm to address this issue: Proactive Security for Upcoming Sensitive Connection (PSUSC). Analysis of the PSUSC algorithm proves reducing potential attacks extremely compared with previous works which rely on using less secure RAT.

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

I. INTRODUCTION

The Mobile Users (MUs) are always keen for using all available communication services anywhere, anytime regardless of any potential technical issue and/or technological constraint might associated with the different Radio Access Technologies (RATs): Wi-Fi, 2G (GSM), 3G (UMTS), 4G (WiMAX and LTE) and 5G.

In fact, a RAT itself is not able to satisfy MUs' preferences all the time as each RAT has its own restricted capabilities in terms of security, data rate, coverage, etc. For example, the 5G itself is not sufficient for providing ubiquitous wireless access without cooperating with the rest of RATs [1].

The VHO performance is measured by different factors such as latency, packet loss, cost signaling, connection failure and security. However, this paper focuses on the security as one of the most crucial factors for the MU to secure upcoming sensitive connection.

Although there are hundreds VHO approaches have been proposed in the literature, it is noticed that a proactive security for upcoming sensitive connection and performing VHO between heterogeneous mobile networks have not been considered. Therefore, this paper presents a new secure algorithm to address this issue: Proactive Security for Upcoming Sensitive Connection (PSUSC).

The rest of the paper is organized as follows: Section II presents related works in securing roaming issues. In Section III, a design of the proposed algorithm is presented. Section IV presents an analysis of the proposed algorithm. Finally, a conclusion and future work are given in Section V.

II. RELATED WORK

In [2], 132 VHO approaches have been reviewed and classified into two categories: VHO security based category and VHO non-security based category for which their characteristics have been discussed. It has been concluded in [2] that the VHO non-security based category takes a large portion of previous works (93%) compared with the VHO security based category (7%). Where, the majority works of this modest percentage of VHO security based category have mainly focused on the role of security parameter in selecting the best available RAT [3].

In [4-11] multi-criteria input parameters considered are (delays, user satisfactions), (Received Signal Strength (RSS), bandwidth, network, coverage, Quality of Service (QoS)), (RSS, Signal to Noise Ratio (SNR), bandwidth), (RSS, bandwidth, cost, velocity of the user), (user speed, RSS, network), (RSS, QoS, bandwidth, network coverage and current and predicted optical link status, traffic rate, active Access Points (APs), and traffic load of adjacent APs), respectively.

However, a proactive security for upcoming sensitive connection and performing VHO between heterogeneous mobile networks has not been considered.

III. DESIGN OF PSUSC ALGORITHM

The VHO consists of three phases: Initiation (Collecting Information), Decision and Execution [12-19]. The proposed secure algorithm takes into account the critical phases of decision and execution in order to secure upcoming sensitive connection between heterogeneous mobile networks. This is shown in Fig. 1.

A. Decision Phase

Unlike previous works which only focus on the role of security parameter in selecting the best available RAT for an imminent VHO, this proactive phase is responsible for selecting the best available secure RAT for the upcoming sensitive connection. Hence, it extremely reduces any potential attack might be launched due to using a current less secure RAT.

Based on Table I, the PSUSC algorithm descendingly orders all available RATs in terms of security into two levels [2]: L1: higher security for 5G (M=5), L2: high security for LTE (M=4), less high security for UMTS (M=3), medium security for WiMAX & GSM (M=2) and low security for Wi-Fi (M=1).

HrS: Higher Security
HS: High Security
LHS: Less High Security
MS: Medium Security
LS: Low Security
Decision Phase ———
Execution Phase - - - - -

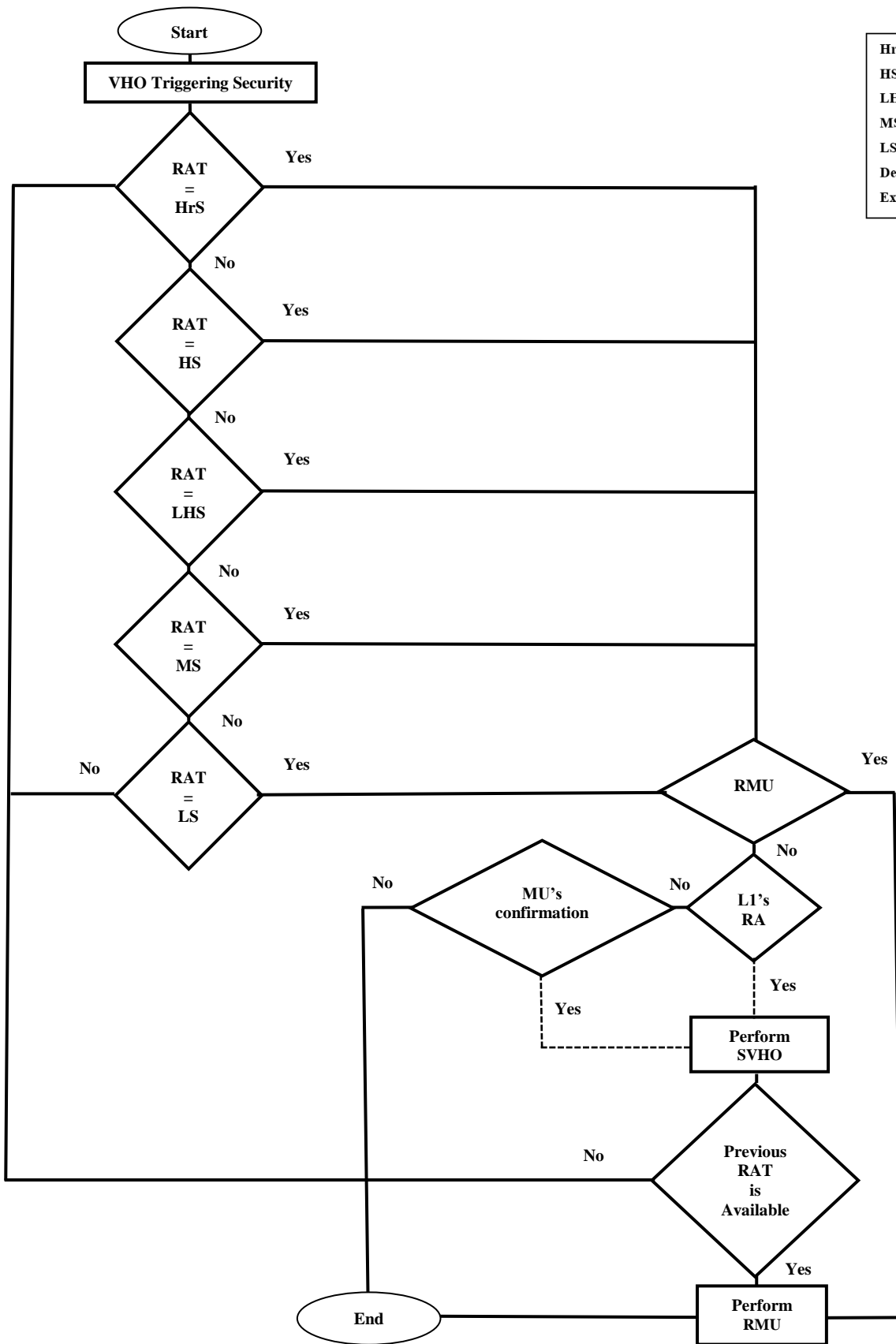


Fig. 1. The PSUSC Algorithm.

TABLE I. SECURITY COMPARISON OF RATs

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	

Once the VHO is triggered for a security session, the algorithm's precedence is to secure the upcoming sensitive session and it therefore selects the best available secure RAT, taking into account that the sole VHO to 5G (L1) is automatically taken place without MUs' confirmation. Otherwise, the MU could confirm whether proceeding VHO from available L2's RATs or not. Finally, when the VHO ongoing sensitive session is successfully performed, the MU is returned back to a previous RAT as long as it is still available. Otherwise, the MU is connected to the best available secure RAT.

B. Execution Phase

This phase is responsible for securing roaming between heterogeneous mobile networks. The critical moment during

the phase is that the VHO between any two RATs (from a source RAT to a destination RAT) might face attackers who exploit such a process for achieving their malicious goals.

MIPv4 and MIPv6 are the best mobility management protocols used to maintain VHO ongoing sessions [20]. However, the MIPv6 is more secure than MIPv4 as it provides Internet Protocol Security (IPSec) for all security requirements [21].

IV. ANALYSIS OF PSUSC ALGORITHM

In this analysis, there are five available RATs: 5G, LTE, UMTS, GSM and Wi-Fi, as shown in Fig. 2. The MU is currently connected with Wi-Fi at office and intending to make online bank transactions. Once the MU proceeds to fill sensitive information, the VHO is triggered in order to secure the upcoming sensitive session by selecting the best available secure RAT. It is obvious in this scenario that the transactions' session is handedover to the most available secure RAT and therefore the security is effectively improved compared with using Wi-Fi as a less secure RAT.

Where the PSUSC algorithm guarantees ordering all available RATs descendingly in terms of security: higher security for 5G, high security for LTE, less high security for UMTS, medium security for GSM and low security for Wi-Fi. This is shown in Fig. 3 to Fig. 6.

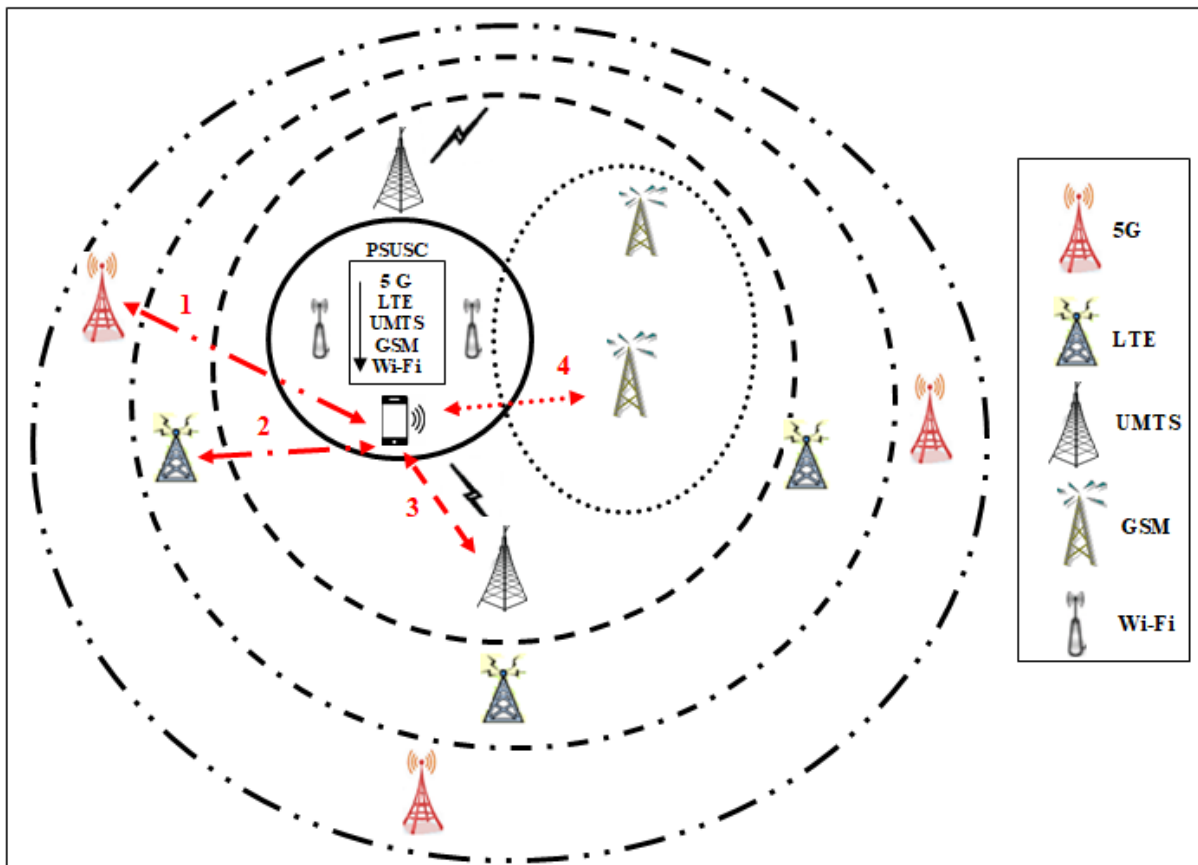


Fig. 2. Scenario of PSUSC Algorithm.

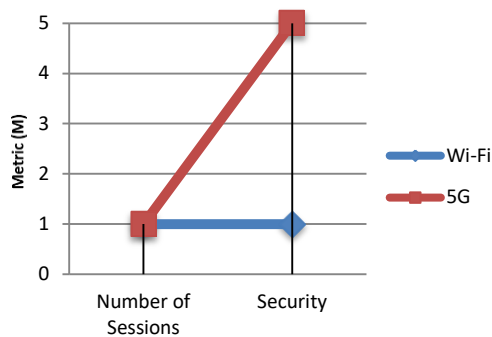


Fig. 3. 5G vs. Wi-Fi.

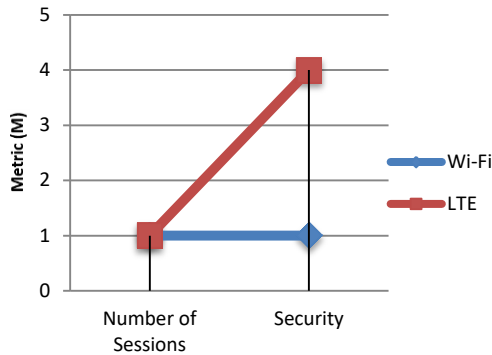


Fig. 4. LTE vs. Wi-Fi.

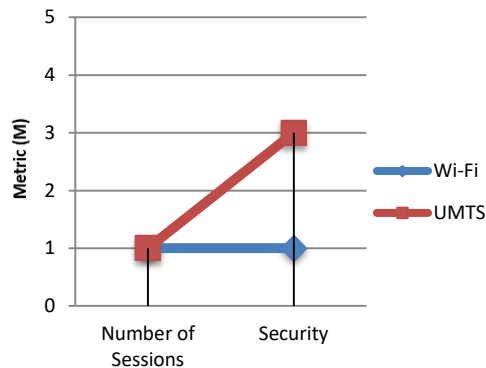


Fig. 5. UMTS vs. Wi-Fi.

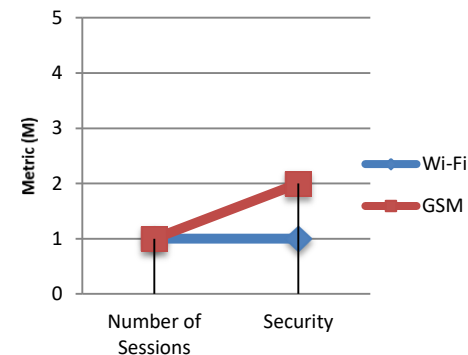


Fig. 6. GSM vs. Wi-Fi.

V. CONCLUSION

This paper has presented design and analysis of new proactive security algorithm for upcoming sensitive connection and performing VHO between heterogeneous mobile networks. The analysis has noticeably showed reducing potential attacks compared with previous works which rely on using less secure RAT. However, we intend to perform more analysis as well as simulation on the proposed algorithm to address security issues, which might face the execution phase as a result of using mobility management protocols during VHO.

REFERENCES

- [1] O. Khattab, "Vertical handover study on 4G category vs. 5G category for 3GPP generation mobile systems and non-3GPP wireless network", *Transactions on Networks and Communications*, vol. 6, no. 2, pp. 1-9, 2018.
- [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, 2018.
- [3] 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.
- [4] D. Wang, Q. Sun, Y. Wang, X. Han and Y. Chen, "Network-assisted vertical handover scheme in heterogeneous aeronautical network", *Asia-Pacific Conference on Image Processing, Electronics and Computers (IPEC)*, pp. 148-152, 2020.
- [5] S. Goutam and S. Unnikrishnan, "QoS based Vertical Handover Decision Algorithm using Fuzzy Logic", *International Conference on Nascent Technologies in Engineering (ICNTE)*, pp. 1-7, 2019.
- [6] A. Debnath and N. Kumar, "Simple Additive Weighted Algorithm for Vertical Handover in Heterogeneous Network," *2nd PhD Colloquium on Ethically Driven Innovation and Technology for Society (PhD EDITS)*, pp. 1-2, 2020.
- [7] S. Goutam, S. Unnikrishnan and A. Karandikar, "Algorithm for Vertical Handover using Multi Attribute Decision Making Techniques," *IEEE International Conference on Communication, Networks and Satellite (Comnetsat)*, pp. 306-313, 2020.
- [8] N. A. Ezz-Eldien, M. F. Abdelkader, M. I. Abdalla and H. M. Abdel-Atty, "Handover Performance Improvement in Heterogeneous Wireless Network," *11th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, pp. 821-830, 2020.
- [9] S. Goutam, S. Unnikrishnan and N. Kudu, "Decision for Vertical Handover using k-Means Clustering Algorithm," *IEEE Bombay Section Signature Conference (IBSSC)*, pp. 31-35, 2020.
- [10] 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*, pp. 1-7, 2021.
- [11] H. T. Yew, A. Chekima, A. Kiring, A. I. Mbulwa, J. A. Dargham and S. K. Chung, "RSS Based Vertical Handover Schemes in Heterogeneous Wireless Networks: Past, Present & Future," *IEEE 2nd International Conference on Artificial Intelligence in Engineering and Technology (IICAET)*, pp. 1-5, 2020.
- [12] M. Zekri, B. Jouaber and D. Zeghlache, "Context aware vertical handover decision making in heterogeneous wireless networks", *IEEE 35th Conference on Local Computer Networks (LCN)*, pp. 764-768, 2010.
- [13] 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.
- [14] E. Stevens-Navarro and V.W.S. Wong, "Comparison between vertical handoff decision algorithms for heterogeneous wireless networks", *IEEE 63rd Vehicular Technology Conference (VTC)*, vol. 2, pp. 947-951, 2006.
- [15] 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.

- [16] W.T. Chen, J.C. Liu, and H.K. Huang, "An adaptive scheme for vertical handoff in wireless overlay networks", Tenth International Conference on Parallel and Distributed Systems (ICPADS), pp. 541- 548, 2004.
- [17] J. McNair and F. Zhu, "Vertical handoffs in fourth-generation multinet network environments", IEEE Wireless Communications, vol. 11, no. 3, pp. 8- 15, 2004.
- [18] Y. Gyekye-Nkansah and J. Agbinya, "Vertical handoffs decision algorithms using fuzzy logic", International Conference on Wireless Broadband and Ultra Wideband Communications, pp. 1-5, 2006.
- [19] D. Sourav, R. Amitava and B. Rabindranath, "Design and simulation of vertical handover algorithm for vehicular communication", International Journal of Engineering Science and Technology, vol. 2. no. 10, pp. 5509-5525, 2010.
- [20] J. Rodriguez, M. Tsagaropoulos, I. Politis, S. Kotsopoulos and T. Dagiuklas, "A middleware architecture supporting seamless and secure multimedia services across an intertechnology radio access network", IEEE Wireless Communications, vol. 16, no. 5, pp. 24-31, 2009.
- [21] Nokia Networks (2001). White paper on introducing mobile IPv6 in 2G and 3G mobile networks, (pp. 1-16): Finland.