Open Issues in Secure Vertical Handoff Techniques for Next Generation Wireless Networks

Nagesha A. G., Mahesh G., Gowrishankar

***Abstract:** The 4G Wireless Networks (WN) have not only provided seamless connection; they also strive to provide Quality of Service (QoS) to the users. However, providing efficient QoS to the users is quite often challenging due to large number of users and significant traffic load. One of the popular techniques to provide consistent QoS to the user is Vertical Handoff (VH). The main concept of VH is to migrate the user to another WN which can provide the requested QoS. Even though substantial contribution has been made in the literature for VH techniques, security oriented VH techniques are limited in number. Security aspect has become critical in Next Generation WN, due to new form of threats which are being introduced, and VH techniques also need to focus on security issues to provide safe and robust communication. In the literature, survey on different security threats, secure VH techniques and future issues has not been effectively presented; in this work, comprehensive survey on all these aspects is presented to aid future research in secure VH.*

***Keywords:** Next Generation Wireless Networks, Vertical Handoff, Security.*

I. INTRODUCTION

The Next generation WN evolution has led to the emergence of Heterogeneous Networks (HNs). The main concept of HNs is that, a particular WN can be integrated with other different types of WNs inorder to provide better QoS to the users. For example, different WN technologies such as: WiFi, 3G, 4G and WiMax can be integrated through HNs, and efficient QoS to the user can be provided.

Implementing integrated security protocol for HNs is challenging, because of different security protocols used by participating WNs, and many of these different security mechanisms might not agree with other mechanisms. The topology of different participating WNs might also create bottlenecks in creating unified security protocol. For example, WiFi is usually installed in homes and other personal spaces; in companies, femto cells are installed to provide cellular connectivity. Hence, each WN might utilize highly specific security mechanism–based on user usage–which can be extremely tedious in integrating with other security mechanisms.

The concept of HNs gave rise to interesting network mechanism called VH. For example, suppose a particular user is accessing WiFi connection from his home. The user expects certain QoS from WiFi for the intended activity. However, due to traffic issues, the WiFi service provider is unable to provide the expected QoS; in such situations, the user can be provided with QoS satisfiable connection through–lets say–cellular network. This migration of the end user to different available WNs–having different technologies–inorder to meet the expected QoS demands of the user is known as VH.

Need for Security

VH has become extremely popular mechanism to deliver QoS in HNs, mainly due to its dynamic scheme; wherein, a user can be shifted from one WN to other based on user preferences. Most of the VH techniques focus on multiple QoS parameters such as: bandwidth, noise rate, RSSI etc. However, only limited number of VH techniques focus on providing robust security to users who utilize VH. It must be noted that, security in Next Generation WNs (NGWNs) has become one of the primary factors for effective network communication, mainly due to myriad of new security threats which are being designed contemporarily. Hence, designing secure VH techniques is ever important–contemporarily and in future, inorder to safeguard users from disastrous consequences of network security attacks. Inorder to promote future research in the area of secure VH techniques, it is extremely vital to comprehensively survey the existing secure VH techniques, inorder to understand: utilized security mechanisms, potential design limitations and future scope of action; however, such survey contributions are hardly available in the literature. Hence, in this work, comprehensive survey on: VH techniques, security challenges in HNs and future research scope for secure VH are outlined. It is expected that, based on this survey contribution, future research endeavors in the area of secure VH techniques can be greatly benefited.

Contributions

In this survey work, the following contributions are made.

Similarly, comprehensive survey on secure VH techniques, along with their limitations is outlined. The existing and possible future security challenges in HNs are outlined, which includes multiple security threats due to: malicious nodes, corrupted access points, compromised cryptographic primitives and malicious node cooperation. The future research issues in the area of secure VH techniques are outlined,

Revised Manuscript Received on December 15, 2019.

* Correspondence Author
Nagesha A G, Dept. of ISE ACIT, Bengaluru, India
Dr. Mahesh G, Dept. of CSE BMSIT&M, Bengaluru, India
Dr. Gourishankar S., Department of CSE, BMSCE, Bengaluru, India.

which includes potential issues in integrating QoS aspects with security mechanisms–under various network traffic conditions.

This paper is organized as follows: Section II provides description about HNs architecture; Section III outlines the existing VH techniques; similarly, Section IV describes the contemporary secure VH techniques–along with, existing security threats and other security mechanisms used in WNs; Section V, outlines the identified future security threats in VH; Section VI, outlines the survey summary along with open issues in designing secure VH techniques; finally, the work is concluded in Section VII.

II. OVERVIEW ON HNS ARCHITECTURE

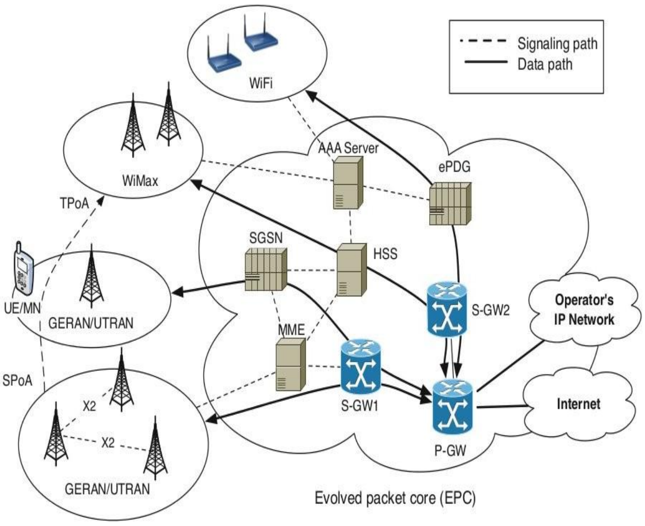

Fig.1 General Architecture of HNs

HNs was conceived due to ever increasing user demands for QoS in NGWNs– including 4G WNs. The general architecture of HNs is illustrated in Figure 1. Here, there are essentially three components in HNs architecture; the network access points for the mobile node; wireless communication component through IP architecture; routing component inside the core network.

The different participating entities in HNs are outlined below:

1. The user device or Mobile Node (MN) is the entity which connects the user to the network.
2. The Point of Access (PoA) is the specific location where the MN connects to the network. For example, in WiFi domain, the PoA is denoted as access point; similarly, in 4G/3G/LTE networks, PoA is denoted as Point of Presence (PoP).
3. Authentication Unit/Center (AuC) is the center through which new MN is verified before being included in the network.
The point of access from which mobile node
4. positions in-order to undergo VH is known as Serving PoA (SPoA).
5. The connection point from which the mobile node connects during VH is known as Transferring PoA (TPoA).

There are different kinds of handoff techniques presented in the literature, and which are outlined below:

1. If a mobile node is migrated from SPoA of one network to TPoA of another; such that, complete disconnection of mobile node is performed from the old PoA; then, this handoff is termed as Hard handoff.
2. If a mobile node is migrated from SPoA of one network to TPoA of another–without disconnection of the mobile node from its old PoA, then, this handoff is termed as Soft handoff.
3. If a handoff is performed between two networks of same technology; then, this handoff is termed as Horizontal handoff. Similarly, if the two networks are having different technologies, the handoff is termed as VH.

III. SURVEY ON VH TECHNIQUES

The existing VH techniques presented in the literature can be broadly classified into five classes: RSSI based VH techniques, Cost Function based VH techniques, Context Aware based VH techniques, Fuzzy Logic based VH techniques and Multiple Criteria based VH techniques.

The RSSI based VH techniques majorly focus on RSSI values provided to the user as signal to invoke VH. If the user expected RSSI is not delivered; then, VH is initiated. In [1, 2], the initial scheme of providing VH through RSSI was presented. In [3], design of RSSI threshold, which ensures efficient VH was outlined. VH technique through RSSI threshold, which considers both the location and velocity of the user, was presented in [4].

The Context Aware based VH techniques consider the context of the user; wherein, the context might refer to: identity of mobile device, environment, time, location and situation. The initial work on Context Aware VH was presented in [5]. In [6], formal definitions of different contexts were presented. The work presented in [7] expanded the work of [6], by including more clearer definition of contexts.

The Cost function based VH techniques consider user specified cost parameters such as: energy consumption, market cost etc. In [8, 9], comprehensive VH techniques using exclusively user specified cost parameters were presented. Some VH techniques [10,11], provide VH on the basis of network cost parameters such as: bandwidth, noise rate etc.

VH techniques presented in [13, 14], gave more emphasis on the second step.

The Multiple Criteria based VH techniques combine the features of RSSI based, Context Aware based and Cost based VH techniques, inorder to outperform these native techniques interms of handoff effectiveness. In [15–17], superior handoff effectiveness of Multiple Criteria based VH techniques over native techniques were presented. In [18], Multiple Criteria based VH technique was based on decision module which was designed through Grey Relational Analysis (GRA) scheme. In [19–21], comprehensive analysis of different Multiple Criteria based VH techniques which utilized different decision making algorithms such as: Simple Additive Weighting, Exponential Weighting, GRA and Similarity to Ideal Solution (TOPSIS), was performed, and it was concluded that, Multiple Criteria based VH techniques can deliver superior effectiveness when compared with native techniques. In [22–24], slight improvement in handoff effectiveness for Multiple Criteria based VH technique, when compared with other contemporary techniques was achieved.

In [25], another Multiple Criteria based VH technique was presented. Here, the HNs had three different WNs: WiMax, WLAN and LTE. Three different kinds of VH algorithms were presented in [25]: network priority, mobile priority and equal priority algorithms; wherein, the first technique prioritizes network parameters, second technique prioritizes mobile node/user parameters and the final technique prioritizes both parameters. It was concluded in [25] that, network priority algorithm performed the best among other techniques. The Multiple Criteria VH technique presented in [26] utilizes Ant Colony Optimization (ACO) meta heuristic scheme for searching the optimal handoff solution. Multiple parameters such as: cost, RSSI, bandwidth and velocity of the mobile node, are utilized to achieve handoff. Here, the mobile nodes are involved in continuous monitoring to detect feasible handoff choices.

In [27], the main focus of Multiple Criteria VH technique was reliability interms of preventing repeated handoffs for a particular user. Here, multiple parameters such as: user device velocity, bandwidth and number of network users, are utilized to achieve handoff; along with, fuzzy classification scheme to select the WN to perform handoff. In [27], reliability is decided interms of number of future users in a particular WN, and this goal is achieved through neural network.

Most of the Multiple Criteria VH techniques can be differentiated on two aspects: utilized parameters and decision component. Raft of parameters are utilized in various VH techniques presented in the literature: RSSI, bandwidth, coverage area, monetary cost, sojourn time, power consumption, device speed, signal to interference ratio, bit error rate, network transmission range, security, traffic intensity, network capacity etc. The decision component represents the component used for making handoff decisions, and multiple techniques such as: neural networks, genetic algorithm, hybrid classification techniques, fuzzy logic classification, are utilized in the literature.

IV. SURVEY ON SECURE VH TECHNIQUES

identified and most prevalent security threats for NGWNs–according to ITU-T X. 800/X. 805–are: *modification attacks*, through illegal modification of network assets; *denial of service attacks*, which is caused due to damage of network assets; *removal attacks*, which is caused due to stealing of network resources or information; *information disclosure attacks*, which is caused due to illegal disclosure of network information; *unavailability attacks*, which results in network services becoming unavailable; *accountability attacks*, which results in charging more to the user than the actual usage.

For the classical 2G WNs, A5/1 and A5/2 cryptographic algorithms were utilized; however, these algorithms could not provide required security for 3G WNs, mainly due to easy breaking of these algorithms, and were substituted by A5/3 algorithm; however, all these cryptographic techniques suffer from vulnerability during session establishment, which can lead to easy malicious node attacks.

In [28], a scheme to integrate 3G security mechanism with 4G WNs was presented; wherein, no significant changes in the security mechanism was proposed; however, the scheme could not overcome the new security threats plaguing 4G. The wireless extension to LANs is provided through IEEE 802.11 standard.

The VH is achieved through a specialized component called *Distribution System*.

The security mechanism proposed for IEEE 802.11 utilizes authentication service such as Radius [29].

One of the initial secure VH techniques were presented in [30, 31]. Here, security during VH is achieved through Radius server, which is inefficient during signaling process. In [32, 33], security mechanisms for both VH and Horizontal Handoff is presented; however, the work fails to resolve uncertainty regarding secure asset management, because both VH and Horizontal Handoff have different goals in secure asset management, and using common security mechanism might be counter predictive. Also, in [32], there is an involvement of third party during authentication, which may increase signaling load.

Media independent handover or VH is achieved through IEEE 802.21 [34]. Here, additional OSI layer is introduced between layer two and three inorder to achieve handoff between different technology WNs. In IEEE 802.21, clear description of integration mechanism inorder to integrate present and future WNs for seamless VH has been outlined. In [35, 36], efficiency evaluation of IEEE 802.21 has been performed; however, security issues have been ignored. In [37], study on security issues for performing VH between WiMax and WiFi has been contributed; however, the security analysis is limited and inaccurate security assumptions are made based on superficial study.

In [38], a new unified security protocol was presented for 4G asset management; however, security analysis is limited and does not address prevalent issues like corruption of base stations. The main focus of 3GPP or 3rd Generation Partnership Project consortium is to design secure VPN channels or tunnels between different MNs inside HNs comprising of core network and WLAN; however, this design is still not adequate to address new security challenges–including from insecure base stations.

V. FUTURE SECURITY THREATS FOR VH

The HNs have achieved next evolution in WNs by attempting to provide consistent QoS for mobile users. However, the achieved merits of HNs have also resulted in significant new security issues due to the gargantuan inclusion of non trusted devices such as WiFi access points or femto cells. Also, the connection between HNs and IP has made HNs extremely vulnerable to IP based network attacks. Some of the identified network threats for HNs in the future are outlined below. Inorder to provide clarity in describing security threats, the generic model for HNs illustrated in Fig 2 is utilized; here, 1, 2, 3 and 4 indicate the corresponding channels between different entities–as illustrated in the Fig 2.

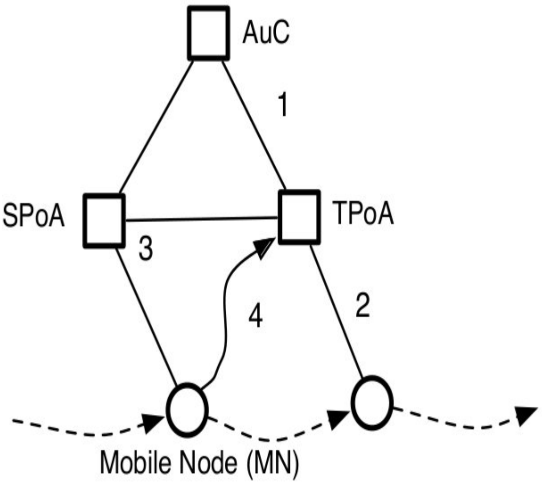

Fig.2 General Model of HNs

Malicious Node Attacks

Here, the malicious node might capture the encrypted packets used during VH. Such malicious node attacks can result in stealing of session keys involved in VH process, and such attacks are usually seen in channel 2 and channel 4. The malicious nodes can also result in denial of service attacks. For example, suppose the handoff process transmits authentication and encryption keys to TPoA through channel 3; however, the sequence number is still not sent. The malicious node might restart the handoff session by using captured session keys and reprogrammed sequence number; due to which, the original mobile node will be prevented handoff due to security screening.

Compromised PoA Attacks

In non-HNs, the network infrastructure is generally considered secure, mainly due to the absence of VH facility. However, in HNs there is a risk that, the security assets could be duplicated by SPoA, and conversation between core network and TPoA could be subjected to eavesdropping. Such kind of attacks is usually seen in channels 3 and 1. Some of the SPoA induced attacks can be considered as Denial of Service attacks–with different variation.

Node Cooperation Attacks

It is possible that, the malicious node in cooperation with SPoA might initiate session cloning which can lead to double handover, and which eventually can lead to overbilling for the user. The session cloning scheme, usually avoids securing authentication information for the cloned node, and its main focus is to create over billing for the customer.

Cryptographic Primitives and Flaw Diffusion

The HNs–due to its legacy and heterogeneity–can create diversity in cryptographic protocols and primitives. For example, handoff might be initiated between two networks having different cryptographic protocols–say 3DES and KASUMI. In such situations, the encryption keys must be transferred with sufficient entropy inorder to prevent flawed diffusion. Otherwise, breakage of any single encryption key can lead to breakage of other keys involved in HNs.

VI. RESULTS AND DISCUSSIONS

The summary of this survey work is outlined in Table 1. The RSSI based VH techniques are essentially suitable for efficient multimedia communication, which requires good RSSI values; however, they are not suitable in applications which stress upon other parameters such as: cost of communication, security etc. The context aware VH techniques are most suitable in critical scenarios; wherein, the user has to establish efficient communication to avoid consequences. These con- text aware VH techniques are unsuitable during normal communication scenarios such as: multimedia communication, and they also lack security mechanisms.

The cost function based VH techniques are well suited to establish economical communication; wherein, the user cannot afford expensive VH costs; however, in some HNs which contain largely expensive networks, these techniques might fail to deliver effective handoff due to limited choices. Also, these cost function based VH techniques lack effective security mechanism.

The Fuzzy logic based VH techniques can model the uncertainty in making handoff decisions. Especially in multi criteria handoff models, uncertainties in making favorable handoff decisions can be seen, because many options to perform handoff might be available; however, each choice might provide more merits in some parameter, when compared to other choices, and such scenarios create uncertainty in deciding the optimal handoff. Hence, fuzzy logic is well suited to model uncertainties in making handoff decisions. However, if proper decision module is not designed for these fuzzy logic based VH techniques, it can lead to poor choices in handoff; also, all these techniques have not addressed security issues.

Multi criteria based VH techniques are the most popular. handoff techniques interms of number of work presented in the literature. These techniques can satisfy multiple QoS requirements of the user. For example, a user might demand QoS interms of: bandwidth, noise rate and RSSI. Such multiple QoS demands can easily be modeled through multi criteria based VH techniques. One of the persistent issues of multi criteria based VH techniques is *Curse of Dimensionality* ; wherein, large number of considered parameters for VH can lead to poor decision making in performing optimal handoff. Most of the multi criteria based VH techniques have also ignored security issues in VH.

The Secure VH techniques are essentially aimed at providing robust security during VH. Since, each participating WN inside HN can have different security protocol for node admission and future communication, most of the secure VH techniques aim to integrate different security mechanisms of WNs. The major security issue addressed in most of the secure VH techniques is: preventing malicious node from getting the VH inside required WN.

However, there can be security issues after the VH has been performed. For example, a particular WN might be extremely prone to network attacks–especially through IP. This particular WN might be the most optimal choice to perform handoff to a certain user. If the handoff is performed, the user is in high risk of being subjected to network attack through the corresponding WN. In such scenarios, it would be judicial to avoid this particular WN for VH, inorder to prevent disastrous consequences for the user. The future security issue for VH techniques is to provide some guarantees about security potential or network attack risks for those WNs which are considered for VH. So that, limited security risk WNs can be selected for VH. This future issue–if resolved–can provide holistic and robust security framework for future VH techniques.

The open issues for future investigations in secure VH are summarized below:

1. Designing secure VH techniques which can accomplish: multi criteria based VH, provide strong security cover against malicious nodes from getting required handoff, are able to estimate the future network attack risk associated with performing handoff to a particular WN; so that, the user can be assured about the possible threats in being subjected to handoff, and the limited risk WN–interms of future network attacks–which satisfies the required QoS constraints of the user is selected for handoff.
2. Continuing on the first goal, some of the WNs might exhibit different behavior interms of network attack risks for different traffic patterns. For example, if large number of users are accessing a particular WN, the risks associated with network attacks might be increased. Hence, calculating network attack risk for a particular WN by considering different possible traffic patterns aids in obtaining aggregated network attack risk information for the WN.
3. In some scenarios, the security potential of a WN might be countering its QoS ability. In such scenarios, the user might advocate better security, when compared to effective QoS or it might even be reverse. Such scenarios again create uncertainty in deciding the optimal handoff choice, and they are attractive to be modeled through fuzzy logic or probabilistic models.
4. Some of the specified QoS parameters involved in deciding VH might not be extremely crucial in deciding the final quality of application. For example, for video processing applications, RSSI is more influential in deciding the final quality when compared to power consumption. If factor analysis on different specified QoS parameters is performed to analyze the influence of these parameters on final application quality; then, some of the less influential parameters can be traded for security–if security is countering QoS ability.

VII. CONCLUSION

In this work, comprehensive survey on security issues for NGWNs was presented; along with, survey on different VH techniques presented in the literature. The merits and limitations of surveyed VH techniques, and their security consideration were outlined. The open issues in designing future secure VH techniques were identified and outlined. It is expected that, this work would provide the necessary motivation for designing future secure VH techniques.

Table- I: Summary of Surveyed VH Techniques

VH Techniques	Characteristics	Merits	Limitations
RSSI based techniques [1–4]	Provides consistent RSSI values during communication	Specially required in multi- media communication	Ignores other vital network parameters and security mechanism
Context aware techniques [5–7]	Provides VH depending on the context of user	Helpful in critical situations	Not applicable during multimedia communication and ignores security mechanism
Cost function based techniques [8–11]	Provides VH based on user specified cost parameters	Useful for economical communication	Can fail to deliver effective handoff; not suitable for high cost networks and lacks security mechanism
Fuzzylogic based techniques [12–14]	Utilizes fuzzy logic concept to decide handoff	Can be used to implement multi criteria handoff	Can result in poor handoff effectiveness and lacks security mechanism
Multi criteria based techniques [15–27]	Provides VH based on multiple parameters	Aids in effective handoff	Security mechanisms are ignored
Secure VH techniques [28–38]	Provides security framework in HNs for VH	Provides unified security framework in heterogeneous environment	Security guarantees after handoff are not addressed

REFERENCES

1. Eshanta O M, Ismail M, Jumari J, Yahaya P.: VHO Strategy for QoS-provisioning in the WiMAX/WLAN Interworking System. Asian J. Appl. Sci. (2009).
2. Yan X, Mani N, Sekercioglu Y A.: A Traveling Distance Prediction Based Method to Minimize Unnecessary Handovers from Cellular Networks to WLANs. IEEE Com- mun. Lett. (2008).
3. Mohanty S, Akyildiz I.: A Cross-Layer (Layer 2 + 3) Handoff Management Protocol for Next-Generation Wireless Systems. IEEE Trans. Mob. Comput. (2006).
4. Liu M, Li Z C, Guo X B, Lach H Y.: Design and Evaluation of Vertical Handoff Decision Algorithm in Heterogeneous Wireless Networks. In: Proceedings of the 14th IEEE International Conference on Networks (2006).
5. Zekri M, Jouaber B, Zeghlache D.: Context Aware Vertical Handover Decision Mak- ing in Heterogeneous Wireless Networks. In: Proceedings of the 35th IEEE Confer- ence on Local Computer Networks (2010).
6. Maaloul S, Afif M, Tabbane S.: Context Awareness and Class of Service Satisfaction for Modeling Handover Decision Making. In: Proceedings of the 21st International Conference on Software, Telecommunications and Computer Networks (2013).
7. Ahmed T, Kyamaky K, Ludwig M.: A Context-Aware Vertical Handover Decision Algorithm for Multimode Mobile Terminals and its Performance. In: Proceedings of the IEEE/ACM Euro American Conference on Telematics and Information Systems (2006).
8. Tawil R, Pujolle G, Salazar O.: A Vertical Handoff Decision Scheme in Heteroge- neous Wireless Systems. In: Proceedings of the IEEE Vehicular Technology Confer- ence (2008).
9. Hasswa A, Nasser N, Hassanein H.: Tramcar: A Context-Aware Cross Layer Archi- tecture for Next Generation Heterogeneous Wireless Networks. In: Proceedings of the IEEE International Conference on Communications (2006).
10. Ong E H, Khan J Y.: On Optimal Network Selection in a Dynamic Multi-RAT Environment. IEEE Commun. Lett. (2010).
11. Abdullah R M, Abdullah A, Hamid N A W A, Othman M, Subramaniam S.: A Network Selection Algorithm Based on Enhanced Access Router Discovery in Heterogeneous Wireless Networks. Wirel. Pers. Commun. (2014).
12. Xia L, Jiang L G, He C.: A Novel Fuzzy Logic Vertical Handoff Algorithm with Aid of Differential Prediction and Pre-Decision Method. In: Proceedings of the IEEE International Conference on Communications (2007).
13. Nasser N, Guizani S, Al Masri E.: Middleware Vertical Handoff Manager: A Neural Network Based Solution. In: Proceedings of the IEEE International Conference on Communications (2007).
14. Pahlavan K, Krishnamurthy P, Hatami A, Ylianttila M, Makela J P, Pichna R, Vallstron J.: Handoff in Hybrid Mobile Data Networks. IEEE Pers. Commun. (2000).
15. Alkhawlani M M, Alsalem K A, Hussein A A.: Multi Criteria Vertical Handover by TOPSIS and Fuzzy Logic. In: Proceedings of the International Conference on Communications and Information Technology (2011).
16. Mahardhika G, Ismail M, Nordin R.: Multi Criteria Vertical Handover Decision Algorithm in Heterogeneous Wireless Network. J. Theor. Appl. Inf. Technol. (2013).
17. Mahardhika G, Ismail M, Mat K.: Multi Criteria Vertical Handover Decision in Heterogeneous Network. In: Proceedings of the IEEE Symposium on Wireless Tech- nology & Applications (2012).
18. Manjaiah D, Payaswini P.: A Review of Vertical Handoff Algorithms Based on Multi Attribute Decision Method. Int. J. Adv. Res. Comput. Eng. Technol.(2013).
19. Tai W L, Chang Y F, Chen Y C.: A Fast Handover Supported Authentication Protocol for Vehicular Ad Hoc Networks. J. Inf. Hiding Multimed. Signal Process. (2016).
20. Chang C C, Huang Y C, Tsai H C.: Design and Analysis of Chameleon Hash- ing Based Handover Authentication Scheme for Wireless Networks. J. Inf. Hiding Multimed. Signal Process. (2014).
21. Kassar M, Kervella B, Pujolle G.: An Overview of Vertical Handover Decision Strategies in Heterogeneous Wireless Networks. Comput. Commun. (2008).
22. Savitha K, Chandrasekar C.: Vertical Handover Decision Schemes Using SAW and WPM for Network Selection. in Heterogeneous Wireless Networks. Glob. J. Comput. Sci. Technol.(2011).
23. Stevens Navarro E, Wong V W S.: Comparison Between Vertical Handoff Decision Algorithms for Heterogeneous Wireless Networks. In: Proceedings of the 63rd IEEE Vehicular Technology Conference (2006).
24. Ismail A, Byeong hee R.: Adaptive Handovers in Heterogeneous Networks Using Fuzzy MADM. In: Proceedings of the International Conference on Mobile IT Con- vergence (2011).
25. Radhwan Mohamed Abdullah, Zuriati Ahmad Zukarnain.: Enhanced Handover Decision Algorithm in Heterogeneous Wireless Network. Sensors (2017).
26. Imad El Fachtali, Rachid Saadane, Mohammed El Koutbi.: Vertical Handover De- cision Algorithm Using Ants Colonies for 4G Heterogeneous Wireless Networks. Journal of Computer Networks and Communications (2016).
27. Guo Q, Zhu J, Xu X.: An Adaptive Multi-Criteria Vertical Handoff Decision Al- gorithm for Radio Heterogeneous Network. In: Communications ICC (2005).
28. 3GPP. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (sae); Security Archi- tecture, Release 11 (June 2012).
29. IEEE Standard for Local and Metropolitan Area Networks - part 11: Wireless LANs (2012).
30. Park S, Kim P S.: A New Vertical Handover Mechanism for Convergence of Wired and Wireless Access Networks. In: Proceedings of the 23rd Intl. Conf. on Information Networking (2009).
31. Wang H, Prasad A R.: Security Context Transfer in Vertical Handover. In: 14th IEEE Proceedings on Personal Indoor and Mobile Radio Communications (2003).
32. Marin R, Fernandez P J, Gomez A F.: 3-Party Approach for Fast Handover in EAP-Based Wireless Networks. In: Meersman, R. (ed.) OTM 2007, Part II. LNCS, vol. 4804, pp. 17341751. Springer, Heidelberg (2007).
33. Lim S H, Bang K S, Yi O, Lim J.: A Secure Handover Protocol Design in Wire- less Networks with Formal Verification. In: Boavida, F., Monteiro, E., Mascolo, S., Koucheryavy, Y. (eds.) WWIC 2007. LNCS, vol. 4517, pp. 6778. Springer, Heidel- berg (2007).
34. IEEE Standard for Local and Metropolitan Area Networks - Part 21: Media Inde- pendent Handover Services (2008).
35. Dutta A, Das S, Famolari D, Ohba Y, Taniuchi K, Fajardo V, Lopez R M, Ko- dama T, Schulzrinne H.: Seamless Proactive Handover Across Heterogeneous Access Networks. Wirel. Pers. Commun. 43(3) (November 2007).
36. Lampropoulos G, Salkintzis A K, Passas N.: Media Independent Handover for Seamless Service Provision in Heterogeneous Networks. IEEE Communications Magazine 46(1), 6471 (2008).
37. Sun H M, Chen S M, Chen Y H, Chung H J, Lin I H.: Secure and Efficient Handover Schemes for Heterogeneous Networks. In: Proceedings of the IEEE Asia- Pacific Services Computing Conference, APSCC 2008, pp. 205210. IEEE Computer Society, Washington, DC (2008).
38. Krichene N, Boudriga N.: Securing Roaming and Vertical Handover in Fourth Generation Networks. In: Proceedings of the Third International Conference on Network and System Security, NSS 2009, pp. 225231. IEEE Computer Society Press, Washington, DC (2009).

AUTHORS PROFILE

Nagesha A. G. - working as Associate Professor at Acharya Institute of Technology, Bengaluru and a research scholar, pursuing PhD under VTU Belagavi at BMSCE Research Centre, Bengaluru. His area of interests includes sensor networks, wireless networks and security

Dr. Mahesh G, holds B.E., M.Tech and Ph.D in Computer Science & Engineering from VTU. He was a 2nd Rank holder in M.Tech. He is currently working with Department of CSE, BMSIT. He has 15 years of professional experience, which spans from academics, research and consultancy. He has published around 20 papers in reputed International Journals / Conferences. His current research interests include stochastic and Petrinets modeling of wireless networks. He is a member of Society of Digital Information & Wireless Communication, International Association of Engineers and Indian Society for Technical Education. Cognizant Technology Solutions has honored him with the Best Faculty Award in 2017.

Dr. Gowrishankar S. - working as Professor in Computer Science and Engineering Departent at BMSCE, Bengaluru. He has more than 50 research publications into his credit. His area of interests includes ubiquitous computing,sensor networks, wireless networks and security