International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Technological and Deployment Challenges: Wireless Hotspots

Anil Kumar Pandey

Computer Centre, Banaras Hindu University

Abstract: ***Hotspots can become a ubiquitous infrastructure. The era of mobile computing has been changed and immerged in new concept. There are several technological and deployment challenges are lingering before. These challenges are authentication, security, coverage, management, location services, billing, and interoperability. There is an emergent need of high speed hotspots in public and working sectors, also the unfolding of technical issues before meeting with advancement related goals should be taken into consideration. This paper explores the challenges related to the authentication issues, security, management, location services which will be further helps in improving ability of computer system and software's with respect to wireless hotspot.***

Keywords: Deployment, WISP, Wireless Hotspots, Technology, Authentication

1. Introduction

Nowadays Internet is part of daily routine where multiple tasks are being done online such as banking, purchasing and social networking as well. Sphere of internet is speeded widely in educational institutions, corporate sectors and in accessing knowledge across the world. As estimated there are four million hotspots in the world are used at present (Venkataramana & Jayasri, 2016). To extend connectivity of networks areas (WLANs) Wireless Local Area Network is emerged as a reliable platform for networking and enhanced connectivity of internet(Bahletal. 2002).In modern era in order to provide strong connectivity "WI-FI" hotspots wireless LAN based on IEEE 802.11b technology at 11 Mb/s are used. In upcoming years the extension of the data rates is expected to be enhanced and popularized. Wireless Internet service providers (WISPs) have evolved extensive wireless networking across public synods to provide convenient facility for users during travelling (R.V. Nee, 1999). In addition to enhanced wireless Wi-Fi hotspots connectivity emergence of software oriented goals are made due to challenging conditions in security and authentication. Extensive mental view point in computing has been altered in two forms i.e. numbers and types respectively. There are abundance of challenges to be tackled while implementing the wireless hotspot system.

Recent advancements are great predictor that is upcoming generation, wide coverage of internet connectivity and cellular data, which will help to achieve greater success by introducing various strategies. This wide area network having several limitation and also overlaid voice traffic. There is an emergent need of high speed hotspots in public and working sectors. There is also a need to unfold technical issues before meeting with advancement related goals. This unfolding includes authentication issues, security, management, location services, improving ability of computer system and software's.

2. Technological Challenges

Authentication is one of the key step in establishing wireless hotspot network and this task is challenging too. Other related challenges are security ratio frequency range, preference to the network, management of the network, and require support for context aware services. In current situation, hotspots are Wi-Fi network where authentication procedure is applied by wireless-hop security.In modern era CHOICE and SPINACH attempted topresent the use utilisation authentication techniques based on third party (G. Appenzelleretal.1999, Bahletal. 2001). Metz. Haller and Kerberos has experienced the requirement of sophisticated hardware for the identity verification of hotspot provider with the ease of accessibility, there is an emergent requirement to know the procedure and nature of public environment to enhance the network accessibility (N. Haller and C. Metz, 1996,). It is also required to recognise the mechanism of authenticationfor automated network system using the techniques of one time user and password (OTP). In the whole setup sophisticated hardware is compulsory including, authentication latency can used in wireless LANs. The user can be facilitated by user identity using their e-mail and contact details. A login and password also enables easy identification of location of users who are travelling.

Other than these technological threats to the wireless networks there are several other safety threats i.e. lack of encryption, the evil twin, session hijacking, session side jacking and eaves dropping (Venkataramana&Jayasri, 2016). Despite the many efforts in estimating mobile user location (Bahl&Padmanabhan, 2000), it is still not clear how this location is best represented and used. Every location aware system desiresthe capability to translate geographic location information into a more usable. Bootstrap the creation ofa universal location database that applications can leverage for the user acceptance the hotspot operators has currently provided connectivity through viable model to encourage the connectivity up to user satisfaction (Schilitetal., 2003).

Multi-hop hotspots initiate many challenges to the network and protocol designer because of their inherent dynamic nature as node mobility in which user may constantly enter or leave the network or mobile when in communication. In this process number of active nodes in thead hoc network takes places and the volume of network traffic is changing constantly. All nodes work within adhocnetwork within RF range of access point they may not be able to hear the access

point transmission Channel. In these hotspots network may be transmitting information on behalf of other nodes it may be power constrained than nodes in infrastructure networks. These constraints inspire more power aware channel access protocols and more effective power saving algorithms For the use of Multiple Network Access, nodes in the multi-hop are just one hop away from the access point work as a access router or gateway between two network such as ad hoc network of user odes and the infrastructure mode network with respect to the access point simultaneously. Hotspot network is beneficial to wireless user and hotspot operators due to cellular network have better coverage otherwise when cellular users enter in a building they can be awarded high bandwidth Wi-Fi connectivity which reduces the load on cellular network. The ability of software catalysed the hardware through switch sensing up to the most resource efficient mode of accessibility (Gustafsson&Jonsson, 2003). For access of the network there is an alternative way to migrate the connection across the devices at the medium of interoperability. The industry and research efforts are in the process to meet out the challenges of interoperability in roaming relationship and effective packet routing agreement is needed between network operators.

In the process of effort has been proposed and working of WLAN with CDMA2000 based 3G and 4G network using a special gateway to bridge the two networks and special mobile software .It is an integrated authentication, security with financial billing over the common platform. In this process, multiple challenges of occurs, Handoff Mechanism, Location assisted Roaming, system support for Handoff and billing of the services provided by the network operation and cellular network operators. It was found that to meet out the problems and challenges IOTA gateway having RADIUS server in the implementation of agreement between two operators there is need to manage Interoperability, Authentication, security, coverage, network management (Buddhikotetal., 2003).

3. Conclusions

Technological deployment challengesof Hotspot can be handled with the support of following conservable and effective points found in the study:

1) Interoperability, Authentication, security, coverage, network management are the key challenges in the development of the wireless hotspots.
2) The growing requirement for high-speed connectivity in public areas.
3) A mechanism that is easy to use, economically attractive, and provides fast access in a transparent in independent manner.
4) The hotspot network providers to benefit robust third party authenticating entity establish peering agreements with other providers.
5) Establishment of business agreements with hotspot network providers is required for installation, maintenance, monitoring, and support and make network access an everyday utility for the end user.

References

[1] B. Aboba, IEEE 802.1X pre-authentication, *Presentation to 802.11WGi*(July 2002).
[2] A. Ahmad, R. Chandler, A.A. Dharmadhikari and U. Sengupta, SIM-based WLAN authentication for open platforms. Technology at Intel *Magazine* (August 2003).
[3] J. Ala-Laurila, J. Mikkonen and J. Rinnemaa, Wireless LAN access net-work architecture for mobile operators, IEEE Communications Maga-zine 39(11) (2001).
[4] G. Appenzeller, M. Roussopoulos and M. Baker, User-friendly ac-cess control for public network ports, in: *Proc. IEEE INFOCOM'99* (1999).
[5] W.A. Arbaugh, N. Shankar and J. Wang, Your 802.11 network has no clothes, in: *Proc. IEEE International Conference on Wireless LANs andHome Networks* (Dec. 2001) pp. 131–144.
[6] Aruba Networks. www.arubanetworks.com.
[7] P. Bahl, A. Balachandran, A. Miu, W. Russell, G.M. Voelker and Y.-M. Wang, PAWNs: Satisfying the need for secure ubiquitous connectiv-ity and location services. IEEE Wireless Communications Magazine, Special Issue on Future Wireless Applications (2002) pp. 40–48.
[8] P. Bahl, A. Balachandran and S. Venkatachary, Secure wireless internet access in public places, in: *Proc. IEEE ICC'01* (June 2001) pp. 3271– 3275.
[9] P. Bahl and V. N. Padmanabhan, RADAR: An in-building RF-based user location and tracking system, in: *Proc. IEEE INFOCOM'00* (April 2000).
[10] V. Bahl, P. Bahl and R. Chandra, MultiNet: Connecting to Multiple IEEE 802.11 networks using a single wireless card, Technical Report MSR-TR-2003-46, Microsoft Research (July 2003).
[11] A. Balachandran, G.M. Voelker and P. Bahl, Hot-spot congestion relief in public-area wireless networks, in: *Proc. Workshop on Mobile Com-puting Systems and Applications, WMCSA'02* (June 2002) pp. 70–80.
[12] A. Balachandran, G.M. Voelker, P. Bahl and P.V. Rangan, Characteriz-ing user behavior and network performance in a public wireless lan, in: *Proc. ACM SIGMETRICS'02* (June 2002) pp. 195–205.
[13] M. Balazinska and P. Castro, Characterizing mobility and network us-age in a corporate wireless local-area network, in: *Proc. MobiSys'03*, (May 2003) pp. 303–316.
[14] J. Bellardo and S. Savage, 802.11 Denial-of-service attacks: Real vul-nerabilities and practical solutions, in: *Proc. USENIX Security Sympo-sium*, (Aug. 2003).
[15] N. Borisov, I. Goldberg and D. Wagner, Intercepting mobile com-munications: The insecurity of 802.11, (Jan 2001). *www.isaac.cs.berkeley.edu/isaac/wep-faq.html*
[16] M. Buddhikot, G. Chandramenon, S. Han, Y.W. Lee, S. Miller and L.Salgarelli, Integration of 802.11 and third-generation wireless data networks, in: *Proc. IEEE Infocom 2003* (April 2003).
[17] M. Buddhikot, G. Chandramenon, S. Han, Y.W. Lee, S. Miller and L.Salgarelli, Design and implementation of a WLAN/CDMA2000 interworking architecture, in: *IEEE Communications Magazine*, (Nov. 2003).
[18] S.C. Chan, An overview of smart card security, White Paper (Aug. 1997).

[19] Cometa Networks, www.cometanetworks.com.
[20] D. Deville, A. Galland, G. Grimaud and S. Jean, Smart card operating systems: Past, present, and future, in: *Fifth USENIX/NordU Conference* (Feb. 2003).
[21] M. Gruteser and D. Grunwald, Anonymous usage of location-based services through spatial and temporal cloaking, in: *Proc. First Inter-national Conference on Mobile Systems, Applications, and Services (MobiSys'03)* (May 2003) pp. 31–42.
[22] E. Gustafsson and A. Jonsson, Always best connected, in: *IEEE Wire-less Communications Magazine* (Feb. 2003).
[23] H.L. Van Trees, *Optimum Array Processing* (John Wiley & Sons, 2002).
[24] H. Haverinen, J. Mikkonen and T. Takamki, Cellular access control and charging for mobile operator wireless local area networks, in: IEEE Wireless Communications 9(6) (2002).
[25] J. Hightower and G. Boriello, The location stack: A layered model for location in ubiquitous computing, in: *Proc. Workshop on MobileComputing Systems and Applications, WMCSA'02* (June 2002).
[26] G. Hyman. Wi-Fi, Wherefore Art Thou? Wireless Online (April 2002).
[27] IEEE, 802.11b/d3.0 Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specification (Aug. 1999).
[28] IEEE, P802.11 http://grouper.ieee.org/groups/802/11 (May 2000).
[29] IEEE 802.1X-2001, IEEE Standards for Local Area Networks: Port-Based Network Access Control, 1999.
[30] ITU-R Rec. M. 1225, Guidelines for Evaluation of Radio Transmission Technologies for IMT-2000.
[31] E.-S. Jung and N. Vaidya, A power control mac protocol for ad hoc networks, in: *Proc. ACM MobiCom'02* (Sept. 2002).
[32] D. Kotz and K. Essien, Characterizing usage of a campus-wide wireless network, in: *Proc. ACM MobiCom'02*, (March 2002) pp. 107–118.
[33] L. Qiu, P. Bahl and A. Adya, The effect of first-hop wireless bandwidth allocation on end-to-end network performance, in: *Proc. NOSSDAV'02* (May 2002).
[34] J. Lansford and P. Bahl. The design and implementation of HomeRF: A radio-frequency wireless networking standard for the connected home, in: *Proceedings of the IEEE* (Nov. 2000).
[35] S. Lu, V. Bhargavan and R. Srikant, Fair scheduling in wireless packet networks, in: *Proc. ACM Sigcomm'97* (Aug. 1997) pp. 63–74.
[36] H. Luo, R. Ramjee, P. Sinha, L. Li and S. Lu, UCAN: A unified cellular and ad-hoc network architecture, in: *Proc. ACM MobiCom'03* (Sept. 2003).
[37] A. Mishra and W. A. Arbaugh, An initial security analysis of the IEEE 802.1x standard, technical report CS-TR-4328, University of Maryland (Feb. 2002).
[38] Mobilian, http://www.mobilian.com.
[39] N. Haller and C. Metz, A one-time password system, *IETF RFC 1938* (May 1996).
[40] E.A. Napjus, Netbar–Carnegie Mellon's solution to authenticated ac-cess for mobile machines, White Paper (August 1989).
[41] R.V. Nee, New high rate wireless LAN standards, IEEE Communications Magazine (1999) 82–88.
[42] E. Ng, I. Stoica and H. Zhang, Packet fair queuing algorithms for wireless networks with location-dependent errors, in: *Proc. IEEE Info-com'98* (March 1998).
[43] NYC Wireless, www.nycwireless.net.
[44] N.B. Priyantha, A. Chakraborty and H. Balakrishnan, The cricket location-support system, in: *Proc. ACM MobiCom'00* (July 2000).
[45] C. Rigney, A.C. Rubens, W.A. Simpson and S. Willens, Remote au-thentication dial-in user service (RADIUS), *IETF RFC 2138* (April 1997).
[46] A.K. Salkintzis, C. Fors and R. Pazhyannur, WLAN-GPRS integration for next-generation mobile data networks, IEEE Wireless Communica-tions 9(5) (2002).
[47] M. Satyanarayanan, Pervasive computing: Vision and challenges, IEEE Personal Communications (Aug. 2001).
[48] B. Schilit, G. Boriello, W.G. Griswold, D. McDonald, E. Lazowska, A. Balachandran and V. Iverson, Ubiquitous location-aware computing – the place lab initiative, in: *Proc. First ACM Workshop onWireless Mobile Applications and Services on WLAN Hotspots* (Sept.2003). Seattle Wireless, www.seattlewireless.com.
[49] J.G. Steiner, G. Neuman and J.I. Schiller, Kerberos: An authentica-tion service for open network systems, in: *Proc. Winter 1998 USENIXTechnical Conference* (Feb. 1988).
[50] T-Mobile, www.tmobile.com.
[51] TOGEWAnet AG, http://www.togewanet.com (July 2002). Vivato Systems, www.vivato.net.