TRAFFIC CHARACTERISATION MECHANISM FOR DETECTING ROGUE ACCESS POINT IN LOCAL AREA NETWORK

AMRAN BIN AHMAD

DOCTOR OF PHILOSOPHY
UNIVERSITI UTARA MALAYSIA
2015

Permission to Use

In presenting this thesis in fulfilment of the requirements for a postgraduate degree from Universiti Utara Malaysia, I agree that the Universiti Library may make it freely available for inspection. I further agree that permission for the copying of this thesis in any manner, in whole or in part, for scholarly purpose may be granted by my supervisor(s) or, in their absence, by the Dean of Awang Had Salleh Graduate School of Arts and Sciences. It is understood that any copying or publication or use of this thesis or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to Universiti Utara Malaysia for any scholarly use which may be made of any material from my thesis.

Requests for permission to copy or to make other use of materials in this thesis, in whole or in part, should be addressed to:

Dean of Awang Had Salleh Graduate School of Arts and Sciences
UUM College of Arts and Sciences
Universiti Utara Malaysia
06010 UUM Sintok

Abstrak

Titik Capaian Bangsat (RAP) adalah satu kerentanan rangkaian yang melibatkan penggunaan titik capaian tanpa wayar secara haram di dalam satu persekitaran rangkaian. Kewujudan RAP boleh dikenal pasti melalui pemeriksaan trafik rangkaian. Tesis ini bertujuan untuk membentangkan kajian penggunaan pencirian trafik rangkaian setempat (LAN) bagi mencirikan rangkaian trafik berwayar dan tanpa wayar melalui pemeriksaan pertukaran paket antara pengirim dan penerima, menggunakan penangkapan paket dengan cop masa masuk untuk menunjukkan kewujudan sesuatu RAP. Kajian ini adalah berdasarkan kepada analisis maklumbalas penyegerakan (SYN/ACK), maklumbalas penutupan sambungan (FIN/ACK), maklumbalas tolakan data (PSH/ACK) dan penghantaran data (PAYLOAD) oleh isyarat daripada pembekal yang dikaitkan kepada pasangan penerima akuan (ACK) masing-masing. Cop masa bagi setiap pasangan kemudiannya dikumpulkan menggunakan teknik Kumpulan Setara yang menghasilkan purata kumpulan. Ia kemudiannya dikategorikan kepada tiga zon untuk membentuk purata zon. Kemudiannya, purata zon ini telah digunakan untuk membentuk purata global yang bertindak sebagai nilai ambang dalam mengenal pasti sesuatu RAP. Sebuah tapak uji rangkaian dibangunkan di mana trafik rangkaian sebenar diperoleh dan dianalisis. Satu mekanisma untuk mencirikan trafik rangkaian berwayar dan tanpa wayar LAN menggunakan analisis purata global dalam proses pengesanan RAP telah dicadangkan. Nilai ambang pengesanan RAP bagi protokol rangkaian berwayar (IEEE 802.3) yang telah dikira oleh kajian adalah 0.002 ms manakala protokol tanpa wayar (IEEE 802.11g dan IEEE 802.11n) adalah masing-masing 0.014 ms dan 0.033 ms. Kajian ini menyumbang kepada satu mekanisma baru bagi mengesan sesuatu RAP melalui pencirian trafik dengan penelitian komunikasi paket dalam persekitaran LAN. Pengesanan RAP adalah penting dalam usaha untuk mengurangkan kerentanan dan memastikan integriti pertukaran data dalam LAN.

Kata kunci: Titik capaian bangsat, Cop masa masuk, Penangkapan paket, Penapisan paket, Keselamatan rangkaian.

Abstract

Rogue Access Point (RAP) is a network vulnerability involving illicit usage of wireless access point in a network environment. The existence of RAP can be identified using network traffic inspection. The purpose of this thesis is to present a study on the use of local area network (LAN) traffic characterisation for typifying wired and wireless network traffic through examination of packet exchange between sender and receiver by using inbound packet capturing with time stamping to indicate the existence of a RAP. The research is based on the analysis of synchronisation response (SYN/ACK), close connection respond (FIN/ACK), push respond (PSH/ACK), and data send (PAYLOAD) of the provider's flags which are paired with their respective receiver acknowledgment (ACK). The timestamp of each pair is grouped using the Equal Group technique, which produced group means. These means were then categorised into three zones to form zone means. Subsequently, the zone means were used to generate a global mean that served as a threshold value for identifying RAP. A network testbed was developed from which real network traffic was captured and analysed. A mechanism to typify wired and wireless LAN traffic using the analysis of the global mean used in the RAP detection process has been proposed. The research calculated RAP detection threshold value of 0.002 ms for the wired IEEE 802.3 LAN, while wireless IEEE 802.11g is 0.014 ms and IEEE 802.11n is 0.033 ms respectively. This study has contributed a new mechanism for detecting a RAP through traffic characterisation by examining packet communication in the LAN environment. The detection of RAP is crucial in the effort to reduce vulnerability and to ensure integrity of data exchange in LAN.

Keywords: Rogue access point, Inbound timestamp, Packet capturing, Packet filtering, Network security.

Acknowledgements

In the name of ALLAH, Most Gracious, Most Merciful.

First and foremost, I would like to profoundly praise The Almighty Allah, who has shown me the right path, provided me the strength and knowledge to complete this research.

There are so many wonderful and talented people whom I would like to thank for their help and patience that I am loss to where to begin.

I will start by thanking my supervisors Professor Dr. Suhaidi Hassan and Dr. Mohd Hasbullah Omar for their help, motivation, and encouragement throughout my study. Both of them are extremely talented person, and I have nothing but respect and admiration for them. They have helped me immensely, and I would like them to know that I appreciate all of their efforts and support.

Finally, my heartiest gratitude goes to my family, to my late father who passed away, to my mother who always has faith in me and prays for my success, to my beloved wife Hapizah Hussain for her understanding, support, and love, and last but not least to all my children, Amira, Hafizi, Amanina and Amalia Husna for being so sweet and loving.

Table of Contents

List of Tables

List of Figures

List of Appendices

List of Abbreviations

ACK	Acknowledgement
AP	Access Point
ARP	Address Resolution Protocol
ASN.1	Abstract Syntax Notation One
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service
FIN	No more data from sender
GUI	Graphical User Interface
IETF	Internet Engineering Task Force
IP	Internet Protocol
LAN	Local Area Network
MAC	Medium Access Control
MIB	Management Information Base
ms	Milliseconds
MyCERT	Malaysia Computer Emergency Response Team
NAT	Network Address Translation
NIC	Network Interface Card
NMS	Network Management System
OID	Object Identifier
OS	Operating System

OSI	Open Systems Interconnection model
PC	Personal Computer
PCAP	Packet Capturing
PHY	Physical
PSH	Push function
RADIUS	Remote Authentication Dial-In User Service
RAP	Rogue Access Point
RTT	Round Trip Time
SMI	Structure of Management Information
SNMP	Simple Network Management Protocol
SSID	Service Set Identifier
SYN	Synchronize sequence numbers
TCP	Transfer Control Protocol
UUM	Universiti Utara Malaysia
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA2	Wi-Fi Protected Access 2

CHAPTER ONE
INTRODUCTION

Wireless technology provides users the freedom of mobility, gives network designers more options for connectivity, and gives many new devices the capability to connect to a network [1, 2, 3]. However, wireless technology brings significantly more threats or vulnerability than traditional wired networks. The issue of network vulnerabilities of wireless LAN is very critical in managing computer networks [4, 5, 6, 7, 8]. With increasing faults and attacks on network infrastructure, there is an urgent need to analyse network and service vulnerabilities under an organised fault attack in a more comprehensive manner [9, 10, 11, 12, 13].

Network extensibility can be achieved easily, with less effort, and become more cost effective through an implementation using wireless devices, such as by installing Access Points (APs) [14]. Many organisations spend greater effort in installing APs for widening the LAN coverage to enable greater access for staff, especially those located at various locations in different buildings. However, some staff prefer to access the organisational network through their private AP without realising the possible detrimental effects of doing so with regard to network security and also performance. This kind of private AP or Rogue AP does not belong to the organisation and it is also unmanageable because of the different configurations and without support by a specific tools in local area network. Thus, this has opened up the network and subjected it to many vulnerability related issues, for example intruders.

In relation to the above scenario, there should be a way to rectify the real problem of RAP, which is unknown to the network manager by using a special mechanism that has capabilities to detect RAPs in whatever event or situation [15, 16]. They are two types of LAN, namely wired and wireless. It can be considered that wired

REFERENCES

[1] CISCO, “Five reasons to go wireless,” 2014. [Online]. Available: http://www.cisco.com/cisco/web/solutions/small_business/resource_center/articles/work_from_anywhere/why_go_wireless/index.html

[2] S. Evans, “Wired vs wireless in the enterprise,” 2014. [Online]. Available: http://www.computerweekly.com/feature/Wired-vs-wireless-in-the-enterprise

[3] Bizhelp24, “How can a wireless network benefit your business?” 2010. [Online]. Available: http://www.computerweekly.com/feature/Wired-vs-wireless-in-the-enterprise

[4] S. Plosz, A. Farshad, M. Tauber, C. Lesjak, T. Ruprechter, and N. Pereira, “Security vulnerabilities and risks in industrial usage of wireless communication,” in *Emerging Technology and Factory Automation (ETFA), 2014 IEEE*, 2014, pp. 1–8. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7005129

[5] J. Zhang, L. Fu, and X. Wang, “Asymptotic analysis on secrecy capacity in large-scale wireless networks,” vol. 22, no. 1, pp. 66–79, 2014. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6470734

[6] E. Mckinney, “Disadvantages of wireless networks,” 2014. [Online]. Available: http://www.ehow.com/facts_4809373_disadvantages-wireless-networks.html

[7] G. Francia, III, D. Thornton, and T. Brookshire, “Wireless vulnerability of scada systems,” in *Proceedings of the 50th Annual Southeast Regional Conference*, ser. ACM-SE ’12. New York, NY, USA: ACM, 2012, pp. 331–332. [Online]. Available: http://doi.acm.org/10.1145/2184512.2184590

[8] P. De, Y. Liu, and S. Das, “An epidemic theoretic framework for vulnerability analysis of broadcast protocols in wireless sensor networks,” vol. 8, no. 3, pp. 413–425, 2009. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4591395

[9] T. Stimpson, L. Liu, J. Zhang, R. Hill, W. Liu, and Y. Zhan, “Assessment of security and vulnerability of home wireless networks,” in *Fuzzy Systems and Knowledge Discovery (FSKD), 2012 9th International Conference on*, 2012, pp. 2133–2137. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6233783

[10] T. Walker, M. Tummala, and J. McEachen, “Security vulnerabilities in hybrid flow-specific traffic-adaptive medium access control,” in *System Science (HICSS), 2012 45th Hawaii International Conference on*, 2012, pp. 5649–5658. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6149581

[11] E. Stavrou and A. Pitsillides, “Vulnerability assessment of intrusion recovery countermeasures in wireless sensor networks,” in *Computers and*

Communications (ISCC), 2011 IEEE Symposium on, 2011, pp. 706–712. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5983922

[12] P. Tague, D. Slater, J. Rogers, and R. Poovendran, "Evaluating the vulnerability of network traffic using joint security and routing analysis," vol. 6, no. 2, pp. 111–123, 2009. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4668352

[13] S. Anand, K. Hong, R. Chandramouli, S. Sengupta, and K. Subbalakshmi, "Security vulnerability due to channel aggregation/bonding in LTE and HSPA+ network," in *Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE*, 2011, pp. 1–5. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6134063

[14] S. Reddy, K. Sai Ramani, K. Rijutha, S. Ali, and C. Reddy, "Wireless hacking - a WiFi hack by cracking wep," in *Education Technology and Computer (ICETC), 2010 2nd International Conference on*, vol. 1, 2010. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5529269

[15] Airtight, "Conquering the minefield of soft rogue aps in the enterprise," 2014. [Online]. Available: http://airtightnetworks.com/fileadmin/pdf/whitepaper/Conquering-the-Minefield-of-Soft-Rogue-APs.pdf

[16] AirMagnet, "Best practices for rogue detection and annihilation," 2004. [Online]. Available: http://airmagnet.flukenetworks.com/assets/whitepaper/Rogue_Detection_White_Paper.pdf

[17] C. D. Mano, A. Blaich, Q. Liao, Y. Jiang, D. A. Cieslak, D. C. Salyers, and A. Striegel, "Ripps: Rogue identifying packet payload slicer detecting unauthorized wireless hosts through network traffic conditioning," *ACM Trans. Inf. Syst. Secur.*, vol. 11, no. 2, pp. 1–23, 2008.

[18] K. N. Gopinath and H. Chaskar, "All you wanted to know about wifi rogue access points," 2014. [Online]. Available: http://www.rogueap.com/rogue-ap-docs/RogueAP-FAQ.pdf

[19] R. Beyah, S. Kangude, G. Yu, B. Strickland, and J. Copeland, "Rogue access point detection using temporal traffic characteristics," *Global Telecommunications Conference, 2004. GLOBECOM '04. IEEE*, vol. 4, pp. 2271–2275 Vol.4, 2004.

[20] H. Hou, R. Beyah, and C. Corbett, "A passive approach to rogue access point detection," in *Global Telecommunications Conference, 2007. GLOBECOM '07. IEEE*, 26-30 Nov. 2007, pp. 355–360.

[21] L. Ma, A. Teymorian, and X. Cheng, "A hybrid rogue access point protection framework for commodity wi-fi networks," in *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, 13-18 April 2008, pp. 1220–1228.

[22] D. Schweitzer, W. Brown, and J. Boleng, “Using visualization to locate rogue access points,” *J. Comput. Small Coll.*, vol. 23, no. 1, pp. 134–140, 2007.

[23] CISCO, “Cisco wireless lan controller configuration guide,” 2014. [Online]. Available: http://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED.pdf

[24] C. Liu and J. Yu, “Rogue access point based dos attacks against 802.11 wlans,” in *Telecommunications, 2008. AICT ’08. Fourth Advanced International Conference on*, 8-13 June 2008, pp. 271–276.

[25] S. Srilasak, K. Wongthavarawat, and A. Phonphoem, “Integrated wireless rogue access point detection and counterattack system,” in *Information Security and Assurance, 2008. ISA 2008. International Conference on*, 24-26 April 2008, pp. 326–331.

[26] P. Drake, “Using snmp to manage networks,” in *Proc. IEE Colloquium on Designing Resilient Architectures*, Nov. 15, 1991, pp. 2/1–2/4.

[27] J. Case, M. Fedor, M. Schoffstall, and J. Davin, “Rfc 1157: Simple network management system,” 2012. [Online]. Available: http://datatracker.ietf.org/doc/rfc1157/

[28] Y.-S. Hwang and E. bae Kim, “An architecture of snmp-based network management of the broadband wireless access system,” in *Proc. 9th Asia-Pacific Conference on Communications APCC 2003*, vol. 3, Sep. 21–24, 2003, pp. 1163–1166.

[29] J. Schonwalder, A. Pras, M. Harvan, J. Schippers, and R. van de Meent, “Snmp traffic analysis: Approaches, tools, and first results,” in *Proc. 10th IFIP/IEEE International Symposium on Integrated Network Management IM ’07*, May 2007, pp. 323–332.

[30] A. Ahmad and S. Hassan, “Detecting rogue access point (rap) using simple network management protocol (snmp),” in *International Conference on Network Applicaitons, Protocols and Services NetApps2008)*, November 21 2008–November 22 2008. [Online]. Available: http://www.internetworks.my/NetApps2008/Proceedings/accepted%20paper/Detecting%20Rogue%20Access%20Point%20%28RAP%29%20using%20SNMP.pdf

[31] X. Wang, L. Wang, B. Yu, and G. Dong, “Studies on network management system framework of campus network,” in *Informatics in Control, Automation and Robotics (CAR), 2010 2nd International Asia Conference on*, vol. 2, March 2010, pp. 285–289.

[32] NetSNMP, “Netsnmp,” 2011. [Online]. Available: http://www.net-snmp.org

[33] MYCERT, “Malaysian computer emergency response team,” 2012. [Online]. Available: http://www.mycert.org.my

[34] CyberSecurity, “Cyber999,” 2012. [Online]. Available: http://www.cybersecurity.my

[35] J. Yang, Y. Chen, and W. Trappe, "Detecting spoofing attacks in mobile wireless environments," in *Sensor, Mesh and Ad Hoc Communications and Networks, 2009. SECON '09. 6th Annual IEEE Communications Society Conference on*, 2009, pp. 1–9. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5168926

[36] A. Ahmad and M. A. Hajer, "Spoofing tracking mechanism for eliminating masquerade users," in *The Fifth Social Economic and Information Technology SEiT 2010 Conference*. UUM, 2010, pp. 50–53.

[37] A. Hadid, "Face biometrics under spoofing attacks: Vulnerabilities, countermeasures, open issues, and research directions," in *Computer Vision and Pattern Recognition Workshops (CVPRW), 2014 IEEE Conference on*, 2014, pp. 113–118. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6909967

[38] D. Reising, M. Temple, and J. Jackson, "Authorized and rogue device discrimination using dimensionally reduced rf-dna fingerprints," *Information Forensics and Security, IEEE Transactions on*, vol. PP, no. 99, pp. 1–1, 2015.

[39] R. Henning, "Vulnerability assessment in wireless networks," in *Applications and the Internet Workshops, 2003. Proceedings. 2003 Symposium on*, 2003, pp. 358–362. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1210186

[40] V. Agapov and S. Rahman, "Exploring wireless device driver vulnerabilities," in *Computer and Information Technology, 2008. ICCIT 2008. 11th International Conference on*, 2008, pp. 78–84. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4803130

[41] F. Azzali, A. Ahmad, and A. Daud, "Determining wireless local area network (wlan) vulnerabilities on academic network," in *Proc. International Conference on Computing and Informatic (ICOCI09)*, 2009.

[42] A. Amran, D. Ali Yusny, and A. Fazly, "Determining wireless local area network vulnerabilities on academic network," in *PROSIDING SEMINAR HASIL PENYELIDIKAN SEKTOR PENGAJIAN TINGGI KE-3*, July 2 2013–July 3 2013, pp. 516–527.

[43] SANS, "Security vulnerabilities and wireless lan technology," 2014. [Online]. Available: http://www.sans.org/reading-room/whitepapers/wireless/security-vulnerabilities-wireless-lan-technology-1629

[44] A. K. Gupta, "Wifi vulnerabilities: Advances and incidents in 2010," 2014. [Online]. Available: http://www.networkworld.com/article/2197200/wi-fi/wifi-vulnerabilities--advances-and-incidents-in-2010.html

[45] PCMag, "Encyclopedia," 2014. [Online]. Available: http://www.pcmag.com/encyclopedia/term/50596/rogue-access-point

[46] H. Yin, G. Chen, and J. Wang, "Detecting protected layer-3 rogue aps," in *Proc. Fourth International Conference on Broadband Communications, Networks and Systems BROADNETS 2007*, Sep. 10–14, 2007, pp. 449–458.

[47] X. Zheng, C. Wang, Y. Chen, and J. Yang, "Accurate rogue access point localization leveraging fine-grained channel information," in *Communications and Network Security (CNS), 2014 IEEE Conference on*, 2014, pp. 211–219. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6997488

[48] S. Jadhav, S. Vanjale, and P. Mane, "Illegal access point detection using clock skews method in wireless LAN," in *Computing for Sustainable Global Development (INDIACom), 2014 International Conference on*, 2014, pp. 724–729. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6828057

[49] S. Nikbakhsh, A. Manaf, M. Zamani, and M. Janbeglou, "A novel approach for rogue access point detection on the client-side," in *Advanced Information Networking and Applications Workshops (WAINA), 2012 26th International Conference on*, 2012, pp. 684–687. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6185342

[50] R. Shrestha and S. Y. Nam, "Access point selection mechanism to circumvent rogue access points using voting-based query procedure," *IET Communications*, vol. 8, no. 16, pp. 2943–2951, 2014.

[51] H. Han, F. Xu, C. Tan, Y. Zhang, and Q. Li, "Vr-defender: Self-defense against vehicular rogue aps for drive-thru internet," vol. 63, no. 8, pp. 3927–3934, 2014. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6762935

[52] K. F. Kao, W. C. Chen, J. C. Chang, and H. T. Chu, "An accurate fake access point detection method based on deviation of beacon time interval," in *Software Security and Reliability-Companion (SERE-C), 2014 IEEE Eighth International Conference on*, 2014, pp. 1–2. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6901631

[53] N. Agrawal, B. Pradeepkumar, and S. Tapaswi, "Preventing arp spoofing in WLAN using sha-512," in *Computational Intelligence and Computing Research (ICCIC), 2013 IEEE International Conference on*, 2013, pp. 1–5. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6724145

[54] K. Kyriakopoulos, F. Aparicio-Navarro, and D. Parish, "Detecting misbehaviour in WiFi using multi-layer metric data fusion," in *Measurements and Networking Proceedings (M&N), 2013 IEEE International Workshop on*, 2013, pp. 155–160. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6663795

[55] R. Beyah and A. Venkataraman, "Rogue-access-point detection: Challenges, solutions, and future directions," *IEEE Secur Priv*, vol. 9, no. 5, pp. 56–61, 2011. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5963632

[56] K. Sawicki and Z. Piotrowski, "The proposal of ieee 802.11 network access point authentication mechanism using a covert channel," in *Microwave Radar and Wireless Communications (MIKON), 2012 19th International Conference on*, vol. 2, May 2012, pp. 656–659.

[57] Y. Song, C. Yang, and G. Gu, "Who is peeping at your passwords at starbucks? x2014; to catch an evil twin access point," in *Dependable Systems and Networks (DSN), 2010 IEEE/IFIP International Conference on*, 282010-july1 2010, pp. 323 –332.

[58] M. Wong and A. Clement, *Sharing wireless internet in urban neighbourhoods*. Springer, 2007.

[59] A. Kalbasi, O. Alomar, M. Hajipour, and F. Aloul, "Wireless security in uae: A survey paper," in *Proc. of the IEEE GCC Conference*, 2007.

[60] C.-M. Chuang, C. Tung, H.-L. Lee, and K.-S. Huang, "Distributed wireless security system," Jun. 15 2006, uS Patent App. 11/453,725.

[61] V. Sharma, "Intrusion detection in infrastructure wireless lans," *Bell Labs Technical Journal*, vol. 8, no. 4, pp. 115–119, 2004.

[62] HKGoverment, "Wireless networking security," 2014. [Online]. Available: http://www.infosec.gov.hk/english/technical/files/wireless.pdf

[63] K. Jones and L. Liu, "What where wi: An analysis of millions of wi-fi access points," in *Portable Information Devices, 2007. PORTABLE07. IEEE International Conference on*, 25-29 May 2007, pp. 1–4.

[64] A. Phippen and S. Furnell, "Taking responsibility for online protection–why citizens have their part to play," *Computer Fraud & Security*, vol. 2007, no. 11, pp. 8–13, 2007.

[65] H. Sathu, "Wardriving dilemmas," in *Proceedings of the Nineteenth Annual Conference of the National Advisory Committee on Computing Qualifications, Wellington*, 2006, pp. 237–242.

[66] H. Berghel and J. Uecker, "Wireless infidelity ii: airjacking," *Commun. ACM*, vol. 47, no. 12, pp. 15–20, 2004.

[67] NetStumbler, "The physics of where to put a wi-fi router," 2014. [Online]. Available: http://www.netstumbler.com/2014/09/19/the-physics-of-where-to-put-a-wi-fi-router/

[68] A. Weiss, "Introduction to netstumbler," 2014. [Online]. Available: http://www.wi-fiplanet.com/tutorials/article.php/3589131

[69] A. Sulaiman and M. Hussein, "A modified multi-wall wave propagation model for concrete based building structure," in *Computer and Communication Engineering (ICCCE), 2012 International Conference on*, 2012, pp. 325–330. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6271205

[70] S. Gold, “Hacking on the hoof,” *Engineering & Technology*, vol. 7, no. 3, pp. 80–83, 2012. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6210313

[71] E. S. Aimuanmwosa, “Evaluating kismet and netstumbler as network security tools & solutions,” Ph.D. dissertation, Blekinge Institute of Technology, 2010.

[72] K. R. Foster, “Radiofrequency exposure from wireless lans utilizing wi-fi technology,” *Health Physics*, vol. 92, no. 3, pp. 280–289, 2007.

[73] M. Sajat, S. Hassan, and S. Chit, “An analysis of wi-fi security vulnerabilities in Malaysia: A survey in golden triangle kuala lumpur,” in *Computing & Informatics, 2006. ICOCI ’06. International Conference on*, 2006, pp. 1–6. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5276423

[74] K. Y. Park, Y. S. Kim, and J. Kim, “Security enhanced IEEE 802.1x authentication method for WLAN mobile router,” in *Advanced Communication Technology (ICACT), 2012 14th International Conference on*, 2012, pp. 549–553. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6174728

[75] E.-K. Ryu, G.-J. Lee, and K.-Y. Yoo, “Unlinkable authentication for roaming user in heterogeneous wireless networks,” in *Connected Vehicles and Expo (ICCVE), 2013 International Conference on*, Dec 2013, pp. 629–634.

[76] W. Wei, K. Suh, B. Wang, Y. Gu, J. Kurose, and D. Towsley, “Passive online rogue access point detection using sequential hypothesis testing with tcp ack-pairs,” in *IMC ’07: Proceedings of the 7th ACM SIGCOMM conference on Internet measurement*. New York, NY, USA: ACM, 2007, pp. 365–378.

[77] T. Le, R. P. Liu, and M. Hedley, “Rogue access point detection and localization,” in *Personal Indoor and Mobile Radio Communications (PIMRC), 2012 IEEE 23rd International Symposium on*, 2012, pp. 2489–2493. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6362775

[78] Tcpdump, “Tcpdump and libpcap,” 2014. [Online]. Available: http://www.tcpdump.org

[79] M. Qadeer, M. Zahid, A. Iqbal, and M. Siddiqui, “Network traffic analysis and intrusion detection using packet sniffer,” in *Communication Software and Networks, 2010. ICCSN ’10. Second International Conference on*, Feb 2010, pp. 313–317.

[80] L. Braun, A. Didebulidze, N. Kammenhuber, and G. Carle, “Comparing and improving current packet capturing solutions based on commodity hardware,” in *Proceedings of the 10th ACM SIGCOMM Conference on Internet Measurement*, ser. IMC ’10. New York, NY, USA: ACM, 2010, pp. 206–217. [Online]. Available: http://doi.acm.org/10.1145/1879141.1879168

[81] P. Orosz and T. Skopko, “Software-based packet capturing with high precision timestamping for linux,” in *Systems and Networks Communications (ICSNC), 2010 Fifth International Conference on*, Aug 2010, pp. 381–386.

[82] L. Zabala, A. Ferro, and A. Pineda, “Modelling packet capturing in a traffic monitoring system based on linux,” in *Performance Evaluation of Computer and Telecommunication Systems (SPECTS), 2012 International Symposium on*, July 2012, pp. 1–6.

[83] B. Lee, S. Moon, and Y. Lee, “Application-specific packet capturing using kernel probes,” in *Integrated Network Management, 2009. IM ’09. IFIP/IEEE International Symposium on*, June 2009, pp. 303–306.

[84] J. Therdphapiyanak and K. Piromsopa, “An analysis of suitable parameters for efficiently applying k-means clustering to large tcpdump data set using hadoop framework,” in *Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), 2013 10th International Conference on*, May 2013, pp. 1–6.

[85] S. Binti Alias, S. Manickam, and M. Kadhum, “A study on packet capture mechanisms in real time network traffic,” in *Advanced Computer Science Applications and Technologies (ACSAT), 2013 International Conference on*, Dec 2013, pp. 456–460.

[86] I. Cerrato, M. Leogrande, and F. Risso, “Filtering network traffic based on protocol encapsulation rules,” in *Computing, Networking and Communications (ICNC), 2013 International Conference on*, Jan 2013, pp. 1058–1063.

[87] W. Wu and P. DeMar, “Wirecap: A novel packet capture engine for commodity nics in high-speed networks,” in *Proceedings of the 2014 Conference on Internet Measurement Conference*, ser. IMC ’14. New York, NY, USA: ACM, 2014, pp. 395–406. [Online]. Available: http://doi.acm.org/10.1145/2663716.2663736

[88] DARPA, “Rfc 793: Transmission control protocol,” 2012. [Online]. Available: http://datatracker.ietf.org/doc/rfc793/

[89] A. Khadimi, M. Lmater, M. Eddabbah, and M. El Kayyali, “Packet classification using the hidden markov model,” in *Multimedia Computing and Systems (ICMCS), 2011 International Conference on*, April 2011, pp. 1–5.

[90] J. Wang, L. Weiwei, Z. Yan, L. Tao, and W. Zilong, “P2p traffic identification based on netflow tcp flag,” in *Future Computer and Communication, 2009. ICFCC 2009. International Conference on*, April 2009, pp. 700–703.

[91] S. Haris, R. Ahmad, and M. Ghani, “Detecting tcp syn flood attack based on anomaly detection,” in *Network Applications Protocols and Services (NETAPPS), 2010 Second International Conference on*, Sept 2010, pp. 240–244.

[92] S. Yan and L. Shuai, “Robust $\mathscr{H}\infty$ filtering in sensor networks with uncertain rates of packet losses,” in *Control Conference (CCC), 2014 33rd Chinese*, 2014, pp. 5282–5287. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6895840

[93] S. McCanne and V. Jacobson, “The bsd packet filter: A new architecture for user-level packet capture,” in *Proceedings of the USENIX Winter 1993 Conference Proceedings on USENIX Winter 1993 Conference Proceedings*, ser. USENIX’93. Berkeley, CA, USA: USENIX Association, 1993, pp. 2–2. [Online]. Available: http://dl.acm.org/citation.cfm?id=1267303.1267305

[94] L. Abeni, N. Bonelli, and G. Procissi, “Randomized packet filtering through specialized partitioning of rulesets,” vol. 17, no. 12, pp. 2380–2383, 2013. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6656077

[95] L. Ning, S. Sen, J. Maohua, and H. Jian, “A router based packet filtering scheme for defending against dos attacks,” *China Communications*, vol. 11, no. 10, pp. 136–146, 2014. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6969802

[96] G. Wang, M. Xu, and X. Huan, “Design and implementation of an embedded router with packet filtering,” in *Electrical & Electronics Engineering (EEESYM), 2012 IEEE Symposium on*, 2012, pp. 285–288. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6258645

[97] L. Cuizhi, Z. Hui, and W. L. Ping, “The design and research based on the intrusion detection model of packet filtering technology,” in *Computer Science & Education (ICCSE), 2011 6th International Conference on*, 2011, pp. 22–23. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6028575

[98] Z. Wu, M. Xie, and H. Wang, “Design and implementation of a fast dynamic packet filter,” vol. 19, no. 5, pp. 1405–1419, 2011. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5719540

[99] R. Fantacci, L. Maccari, P. Neira Ayuso, and R. Gasca, “Efficient packet filtering in wireless ad hoc networks,” vol. 46, no. 2, pp. 104–110, 2008. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4473091

[100] Q. Chen, W. Lin, W. Dou, and S. Yu, “Cbf: A packet filtering method for DDoS attack defense in cloud environment,” in *Dependable, Autonomic and Secure Computing (DASC), 2011 IEEE Ninth International Conference on*, 2011, pp. 427–434. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6118752

[101] Y. Kim, W. Ren, J.-Y. Jo, Y. Jiang, and J. Zheng, “Sfric: A secure fast roaming scheme in wireless lan using id-based cryptography,” in *Communications, 2007. ICC ’07. IEEE International Conference on*, 24-28 June 2007, pp. 1570–1575.

[102] E. Linda Dacey, *Operations and Algebraic Thinking Leveled Problems: Division and Equal Groups*, ser. 50 Leveled Math Problems, 2014. [Online]. Available: https://books.google.com.my/books?id=3X5TBAAAQBAJ

[103] Y. Xin, *Conceptual Model-Based Problem Solving: Teach Students with Learning Difficulties to Solve Math Problems*, ser. SpringerLink : Bücher. SensePublishers, 2013. [Online]. Available: https://books.google.com.my/books?id=7c5JAAAAQBAJ

[104] Types of multiplication and division problems. Www.math.ccsu.edu/mitchell/multiplicationanddivision.pptx, Jan 14 2015.

[105] R. Antonius, *Interpreting Quantitative Data with SPSS*. SAGE Publications, 2003. [Online]. Available: https://books.google.com.my/books?id=H1_mH0glk0IC

[106] C.-M. Bao, "Intrusion detection based on one-class svm and snmp mib data," in *Proc. Fifth International Conference on Information Assurance and Security IAS '09*, vol. 2, Aug. 18–20, 2009, pp. 346–349.

[107] M. Amezziane, E. Al-Shaer, and M. Ali, "On stochastic risk ordering of network services for proactive security management," in *Network Operations and Management Symposium (NOMS), 2012 IEEE*, April 2012, pp. 994–1000.

[108] Z.-Y. Li, C.-H. Xie, R. Tao, H. Zhang, and N. Shi, "A network security analysis method using vulnerability correlation," in *Natural Computation, 2009. ICNC '09. Fifth International Conference on*, vol. 1, Aug 2009, pp. 17–21.

[109] L. Bhebhe, "Mobility management issues in heterogeneous mobile wireless networks," in *Globecom Workshops (GC Wkshps), 2012 IEEE*, Dec 2012, pp. 787–791.

[110] E. Wonghirunsombat, T. Asawaniwed, V. Hanchana, N. Wattanapongsakorn, S. Srakaew, and C. Charnsripinyo, "A centralized management framework of network-based intrusion detection and prevention system," in *Computer Science and Software Engineering (JCSSE), 2013 10th International Joint Conference on*, May 2013, pp. 183–188.

[111] P. Goyal, R. Mikkilineni, and M. Ganti, "Fcaps in the business services fabric model," in *Enabling Technologies: Infrastructures for Collaborative Enterprises, 2009. WETICE '09. 18th IEEE International Workshops on*, 2009, pp. 45–51. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5159212

[112] S. Jacobs, "Introduction," in *Security Management of Next Generation Telecommunications Networks and Services*. Wiley-IEEE Press, 2014.

[113] D. C. Lee, B. Park, K. E. Kim, and J. J. Lee, "Fast traffic anomalies detection using snmp mib correlation analysis," in *Proc. 11th International Conference on Advanced Communication Technology ICACT 2009*, vol. 01, Feb. 15–18, 2009, pp. 166–170.

[114] E. Harahap, J. Wijekoon, R. Tennekoon, F. Yamaguchi, S. Ishida, and H. Nishi, "A router-based management system for prediction of network congestion," in *Advanced Motion Control (AMC),2014 IEEE 13th International Workshop on*, 2014, pp. 398–403. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6823315

[115] G. Xilouris, G. Gardikis, K. Sarsembagieva, and A. Kourtis, "Snmp-driven active measurements in diffserv networks," in *Communications (ICC), 2013 IEEE International Conference on*, 2013, pp. 2545–2549. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6654917

[116] G. Gardikis, K. Sarsembagieva, G. Xilouris, and A. Kourtis, "An snmp agent for active in-network measurements," in *Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2012 4th International Congress on*, 2012, pp. 302–307. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6459684

[117] T. Kazaz, M. Kulin, E. Kaljic, and T. Carsimanovic, "One approach to the development of custom snmp agents and integration with management systems," in *MIPRO, 2012 Proceedings of the 35th International Convention*, 2012, pp. 557–561. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6240708

[118] E. Barka, F. Sallabi, and A. Hosani, "Managing access and usage controls in snmp," in *Computing, Communications and Applications Conference (ComComAp), 2012*, 2012, pp. 41–47. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6154000

[119] A. Adya, P. Bahl, R. Chandra, and L. Qiu, "Architecture and techniques for diagnosing faults in ieee 802.11 infrastructure networks," in *MobiCom '04: Proceedings of the 10th annual international conference on Mobile computing and networking*. New York, NY, USA: ACM, 2004, pp. 30–44.

[120] J. Yeo, M. Youssef, and A. Agrawala, "A framework for wireless lan monitoring and its applications," in *WiSe '04: Proceedings of the 3rd ACM workshop on Wireless security*. New York, NY, USA: ACM, 2004, pp. 70–79.

[121] P. Bahl, R. Chandra, J. Padhye, L. Ravindranath, M. Singh, A. Wolman, and B. Zill, "Enhancing the security of corporate wi-fi networks using dair," in *MobiSys '06: Proceedings of the 4th international conference on Mobile systems, applications and services*. New York, NY, USA: ACM, 2006, pp. 1–14.

[122] W. Wei, S. Jaiswal, J. Kurose, and D. Towsley, "Identifying 802.11 traffic from passive measurements using iterative bayesian inference," in *INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings*, April 2006, pp. 1–12.

[123] U. Deshpande, T. Henderson, and D. Kotz, "Channel sampling strategies for monitoring wireless networks," in *Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks, 2006 4th International Symposium on*, April 2006, pp. 1–7.

[124] S. Shetty, M. Song, and L. Ma, “Rogue access point detection by analyzing network traffic characteristics,” in *Military Communications Conference, 2007. MILCOM 2007. IEEE*, 29-31 Oct. 2007, pp. 1–7.

[125] L. Watkins, R. Beyah, and C. Corbett, “A passive approach to rogue access point detection,” in *Proc. IEEE Global Telecommunications Conference GLOBECOM ’07*, Nov. 26–30, 2007, pp. 355–360.

[126] P. Asadoorian, “Using nessus to discover rogue access points,” 2014. [Online]. Available: http://www.tenable.com/blog/using-nessus-to-discover-rogue-access-points

[127] R. Pacchiano, “How to track down rogue wireless access points,” 2006. [Online]. Available: http://www.smallbusinesscomputing.com/webmaster/article.php/3590656/How-to-Track-Down-Rogue-Wireless-Access-Points.htm

[128] G. Shivaraj, M. Song, and S. Shetty, “A hidden markov model based approach to detect rogue access points,” in *Proc. IEEE Military Communications Conference MILCOM 2008*, 16–19 Nov. 2008, pp. 1–7.

[129] E. Chen and M. Ito, “Using end-to-middle security to protect against evil twin access points,” in *World of Wireless, Mobile and Multimedia Networks Workshops, 2009. WoWMoM 2009. IEEE International Symposium on a*, 2009, pp. 1 –6.

[130] K. Gao, C. Corbett, and R. Beyah, “A passive approach to wireless device fingerprinting,” in *Dependable Systems and Networks (DSN), 2010 IEEE/IFIP International Conference on*, 282010-july1 2010, pp. 383 –392.

[131] M. Rodrig, C. Reis, R. Mahajan, D. Wetherall, and J. Zahorjan, “Measurement-based characterization of 802.11 in a hotspot setting,” in *E-WIND ’05: Proceedings of the 2005 ACM SIGCOMM workshop on Experimental approaches to wireless network design and analysis*. New York, NY, USA: ACM, 2005, pp. 5–10.

[132] S. Jana and S. K. Kasera, “On fast and accurate detection of unauthorized wireless access points using clock skews,” in *MobiCom ’08: Proceedings of the 14th ACM international conference on Mobile computing and networking*. New York, NY, USA: ACM, 2008, pp. 104–115.

[133] H. Han, B. Sheng, C. C. Tan, Q. Li, and S. Lu, “A timing-based scheme for rogue ap detection,” vol. 22, no. 11, pp. 1912–1925, 2011.

[134] H. Han, F. Xu, C. C. Tan, Y. Zhang, and Q. Li, “Defending against vehicular rogue aps,” in *Proc. IEEE INFOCOM*, 2011, pp. 1665–1673.

[135] C. Yang, Y. Song, and G. Gu, “Active user-side evil twin access point detection using statistical techniques,” vol. 7, no. 5, pp. 1638–1651, 2012. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6236067

[136] S. Vanjale and P. Mane, “A novel approach for elimination of rogue access point in wireless network,” in *India Conference (INDICON), 2014 Annual IEEE*, 2014, pp. 1–4. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7030418

[137] G. Qu and M. Nefcy, “Rapid: An indirect rogue access points detection system,” in *Performance Computing and Communications Conference (IPCCC), 2010 IEEE 29th International*, 2010, pp. 9 –16.

[138] A. Ahmad, S. Hassan, and M. H. Omar, “Inbound time stamping for detecting rogue access point,” in *Proc. International Conference on Computing and Informatic (ICOCI13)*, 2013. [Online]. Available: http://www.icoci.cms.net.my/proceedings/2013/PDF/PID113.pdf

[139] T. CarstensZola and G. Harris, “Programming with pcap,” 2014. [Online]. Available: http://www.tcpdump.org/pcap.html

[140] Z. Xiaohui, C. Shuqiao, and L. Ping, “On traffic characteristics and low-cost router design,” in *Multimedia Information Networking and Security, 2009. MINES ’09. International Conference on*, vol. 1, Nov 2009, pp. 268–272.