UNIVERSITI PUTRA MALAYSIA

SECURE ADDRESS RESOLUTION PROTOCOL PROXY IN SOFTWARE DEFINED NETWORK

MUNTHER NUMAN MUNTHER

FK 2018 47

SECURE ADDRESS RESOLUTION PROTOCOL PROXY IN SOFTWARE DEFINED NETWORK

By

MUNTHER NUMAN MUNTHER

Thesis submitted to the School of Graduate Studies, Universiti Putra Malaysia in fulfillment of the Requirements for the degree of Master of Science

March 2018

COPYRIGHT

DEDICATION

This thesis is dedicated to

All those I love

Especially

My dearest parents

My brothers and sister

For their endless encouragement, patience, and support and for being a great source of motivation and inspiration

Abstract of the thesis presented to the Senate of Universiti Putra Malaysia in fulfillment of the requirement for the degree of Master of Science

SECURE ADDRESS RESOLUTION PROTOCOL PROXY IN SOFTWARE DEFINED NETWORK

By

MUNTHER NUMAN MUNTHER

March 2018

Chairman : Fazirulhisyam Hashim, PhD
Faculty : Engineering

Ethernet is one of the most important and dominant protocols residing in the second layer of the seven-layer Open Systems Interconnection (OSI) model. It has many features such as simplicity, ease, and low-cost. All these advantages have enabled it to spread widely in all types of network topology, and therefore Ethernet ports become an essential part of computer and network architecture. Despite its advantages, Ethernet suffers from scalability issue where the increasing number of hosts in a single broadcast domain will significantly increase the number of broadcast traffic in the network. Address Resolution Protocol (ARP) proxy is regarded as one of the best solutions to reduce broadcast traffic in a single broadcast domain, where ARP normally constitutes the bulk size of the broadcast traffic.

With the emergence of Software Defined Network (SDN) based architecture, researchers exploited the SDN features and ARP proxy by enabling SDN controller with ARP proxy feature to suppress the broadcast traffic. In the existing literature, most works have focused on suppressing the broadcast traffic without changing the network architecture or adding new equipment. However, the security aspect has been neglected and attackers can easily exploit the inherent security limitation of ARP working principle to penetrate the network. Note that the SDN controller can be reached by ARP broadcast traffic with a single hop, and since the ARP can be easily manipulated by attackers, this scenario may eventually lead to the increase of attack probability on SDN controller. Two common ARP-based attacks that can be initiated are ARP spoofing and ARP storm.

In this thesis, a secure ARP proxy with SDN controller is proposed in order to provide full protection to SDN controller and network host from ARP-based attacks. Therefore, the proposed approach contains collecting information algorithm, ARP storm attack detection algorithm, and ARP spoofing attack detection algorithm. In

addition, ARP based attack detection technique combines ARP storm and ARP spoofing detection algorithms. In general, the proposed approach will check incoming ARP request packet before replying to ARP request. In case found any wrong information in ARP received packet; the proposed approach will consider the packet sender is the attacker and insert sender information to ARP-based attacks tables. In order to demonstrate the efficiency of the proposed approach, several attack scenarios are developed in a Mininet testbed. The attack scenarios consisted of various potential attack combinations that can be initiated by attackers, malicious or even normal hosts. The analysis of simulation and testbed results indicated that the proposed approach achieved 100% suppresses of ARP broadcast traffic in the broadcast domain. In addition, it was also successful in protecting the network from ARP-based attacks where the true positive ratio of attack detection for the first stage was 57.14% and, for the second stage is 66.66%, while it reached 100% in the final stage. Meanwhile, the CPU consumption for SDN controller of the proposed approach is increased in comparison with the general SDN controller with ARP proxy feature.

Abstrak tesis ini yang dikemukakan kepada Senat Unversiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Master Sains

PROTOKOL PELERAIAN ALAMAT PROKSI YANG SELAMAT DALAM RANGKAIAN PERISIAN TAKRIF

Oleh

MUNTHER NUMAN MUNTHER

Mac 2018

Chairman : Fazirulhisyam Hashim, PhD
Fakulti : Kejuruteraan

Ethernet adalah salah satu protokol yang paling penting dan dominan yang berada di lapisan kedua antara tujuh lapisan model dalam sistem terbuka saling sambung (OSI). Ia mempunyai banyak ciri-ciri seperti keringkasan, kemudahan, dan kos rendah. Semua kelebihan ini membolehkannya tersebar secara meluas dalam semua jenis topologi rangkaian. Oleh itu, port Ethernet menjadi satu bahagian yang penting dalam seni bina rangkaian dan komputer. Walaubagaimanapun, Ethernet mengalami masalah boleh skala apabila pertambahan bilangan hos dalam satu domain siaran tunggal meningkatkan jumlah trafik siaran dalam rangkaian tersebut. Protokol Peleraian Alamat (ARP) proksi dianggap sebagai salah satu penyelesaian terbaik untuk mengurangkan trafik siaran dalam domain siaran tunggal, di mana ARP biasanya menyumbangkan saiz trafik siaran yang besar.

Dengan kemunculan seni bina berasaskan Rangkaian Perisian Takrif (SDN), banyak penyelidik mengeksploitasi ciri-ciri SDN dan ARP proksi dengan membolehkan pengawal SDN mengguna ciri ARP proksi untuk menyekat trafik siaran. Dalam literatur yang sedia ada, sebahagian besar daripadanya telah menumpukan perhatian untuk menumpaskan traffik siaran tanpa mengubahsuai seni bina rangkaian atau menambah peralatan baru. Walau bagaimanapun, aspek keselamatan telah diabaikan dan penyerang boleh mengeksploitasi batasan keselamatan prinsip kerja ARP yang sedia ada dengan mudah untuk menembusi rangkaian. Keupayaan traffik siaran ARP untuk mencapai pengawal SDN dalam satu hop patut diberi perhatian, dan oleh sebab ARP dapat dimanipulasi dengan mudah oleh penyerang, senario ini boleh menyebabkan pertambahan kebarangkalian serangan terhadap pengawal SDN. Dua serangan berasaskan ARP yang biasa ialah perdayaan ARP dan ribut ARP.

Dalam tesis ini, satu ARP proksi yang selamat dengan pengawal SDN dicadangkan untuk membolehkan Ethernet boleh skala dengan penumpasan traffik siaran. Ia mengandungi pakej perlindungan lapisan berbilang yang terbina daripada algoritma pengesanan dan pengurangan untuk melindungi rangkaian daripada serangan berasaskan ARP. Pendekatan yang dicadangkan akan menumpaskan traffik siaran dan mengekalkan kewibawaan pengawal SDN dan peranti rangkaian. Dalam usaha untuk menunjukkan kecekapan algoritma yang dicadangkan, beberapa senario serangan telah dibina dalam tapak uji Mininet. Senario serangan tersebut terdiri daripada pelbagai kombinasi potensi serangan yang boleh dilakukan oleh penyerang, hos jahat atau hos biasa. Analisis terhadap keputusan simulasi dan tapak uji menunjukkan bahawa pendekatan yang dicadangkan mencapai 100% dalam penumpasan traffik siaran siaran ARP pada domain siaran. Di samping itu, ia juga berjaya melindungi rangkaian daripada serangan berasaskan ARP di mana nisbah dedikasi sebenar pengesanan serangan untuk tahap pertama adalah 57.14% dan 66.66% untuk tahap kedua manakala mencapai 100% pada peringkat akhir. Sementara itu, penggunaan CPU bagi pengawal SDN dalam pendekatan yang dicadangkan telah meningkat berbanding dengan pengawal SDN umum dengan ciri ARP proksi.

ACKNOWLEDGEMENTS

First of all, I would like to express my gratitude to my supervisor, Dr. Fazirulhisyam Hashim for his continuous support, invaluable guidance, and patience as well as his encouragement and inspiration along this research journey without which, this thesis could not be done as smoothly as what we have. I am very thankful for all the tasks he has produced for me. God bless his and his family.

Deep gratitude also goes to my co-supervisor Dr. Nurul Adilah Abdul Latiff for her helpful guidance on the thesis draft helped improve the quality of this work. God bless her and her family.

Most importantly, I want to say thanks to my dearest parents and my brothers and sister. They helped me out during the difficulties in life and provided me with warm encouragement.

I certify that a Thesis Examination Committee has met on 2 March 2018 to conduct the final examination of Munther Numan Munther on her thesis entitled "Secure Address Resolution Protocol Proxy in Software Defined Network" in accordance with the Universities and University Colleges Act 1971 and the Constitution of the Universiti Putra Malaysia [P.U.(A) 106] 15 March 1998. The Committee recommends that the student be awarded the Master of Science.

Members of the Thesis Examination Committee were as follows:

Muhammad Hafiz bin Abu Bakar, PhD
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

Rohaya binti Latip, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Internal Examiner)

Khaizuran Abdullah, PhD
Associate Professor
International Islamic University Malaysia
Malaysia
(External Examiner)

NOR AINI AB. SHUKOR, PhD
Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 26 April 2018

This thesis was submitted to the senate of Universiti Putra Malaysia and has been accepted as fulfillment of the requirement for the degree of Master of Science. The members of the supervisory committee were as follows:

Fazirulhisyam Hashim, PhD
Senior Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

Nurul Adilah Abdul Latiff, PhD
Senior Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Member)

ROBIAH BINTI YUNUS, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

Declaration by graduate student

I hereby confirm that:

- this thesis is my original work;
- quotations, illustrations and citations have been duly referenced;
- this thesis has not been submitted previously or concurrently for any other degree at any other institution;
- intellectual property from the thesis and copyright of thesis are fully-owned by Universiti Putra Malaysia, as according to the Universiti Putra Malaysia (Research) Rules 2012;
- written permission must be obtained from supervisor and the office of Deputy Vice-Chancellor (Research and Innovation) before thesis is published (in written, printed or in electronic form) including books, journals, modules, proceedings, popular writings, seminar papers, manuscripts, posters, reports, lecture notes, learning modules or any other materials as stated in the Universiti Putra Malaysia (Research) Rules 2012.
- There is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity is upheld as according to the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) and the Universiti Putra Malaysia (Research) Rules 2012. The thesis has undergone plagiarism detection software.

Signature: _____ Date: _____

Name and Matric No.: Munther Numan Munther (GS46312)

Declaration by Members of Supervisory Committee

This is to confirm that:

- the research conducted and the writing of this thesis was under our supervision;
- supervision responsibilities as stated in the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) are adhered to.

Signature: _____
Name of Chairman of Supervisory Committee: _____

Signature: _____
Name of Member of Supervisory Committee: _____

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ARP	Address Resolution Protocol
CPT	Control Plane Traffic
CPU	Central Process Unit
DAI	Dynamic ARP inspection
DDoS	Distribution Denial of Service
DHCP	Dynamic Host Configuration Protocol
DHT	Distribution Hash Table
DoS	Denial of Service
DPT	Data Plane Traffic
FCS	Frame Check Sequence
FPR	False Positive Ratio
FSDM	Floodless Service Discovery Mechanism
FT	Flow Table
ICMP	Internet Control Message Protocol
IP	Internet Protocol
LAN	Local Area Network
LLDP	Link Layer Discovery Protocol
MAC	Media Access Control
MITM	Man in The Middle Attack
NAT	Network Address Translation
NIC	Network Interface Card
NTP	Network Time Protocol
OF	OpenFlow
OSI	Open Systems Interconnection
ONF	Open Networking Foundation
OUI	Organizationally Unique Identifier
OVS	Open Virtual switch
PID	Process Identifier
RTT	Round Trip Time
SARP	Secured Address Resolution Protocol

SDN	Software Defined Network
TPR	True Positive Ratio
WLAN	Wireless Local Area Network

CHAPTER 1

INTRODUCTION

1.1 Background

Rapid advancement in networking technologies has enabled a wide variety of applications with diverse requirements on network services. Such diverse requirements and dynamic network services bring in new challenges to service provisioning in future networks. This has made networks architecture more complex and difficult to manage [1]. In addition, there has been a significant evolution in the means and methods of penetration as a result of the evolution in information technology. This made it difficult to detect threats because the threats have become smarter [2]. Therefore, penetrating the networks devices or hosts depending on vulnerabilities is becoming easier for attackers. Consequently, the backbone structure of the computer networks has undergone some challenges in order to cope with these rapid developments. One of these challenges is the scalability issue of Ethernet networks.

In principle, an Ethernet network is one of the most common networks that offer many features and services, making it dominant over layer-2 of OSI model networks. Ethernet network derives its name from the Ethernet protocol [3], which is also one of the most popular protocols. This protocol works in the second layer of OSI model; where in this layer header and trailer are added to the frame before sending. The Ethernet protocol was designed in 1982 and it has been updated over periods of time, but in some cases, this protocol cannot keep up with today's developments in information technology and communication.

Besides that, Address Resolution Protocol (ARP) [4] is one of the more important protocols to complete a network connection between two hosts. It works between layer 2 and layer 3 of the OSI model, where it is responsible for the dynamic mapping of IP address and MAC address. ARP is designed without any security mechanism. Thus, it is designed to operate in safe networks. In principle, any ARP packets are considered to carry trusted information regardless of the packet sender. Therefore, attackers or malicious hosts can exploit ARP operation to launch ARP-based attacks such as ARP spoofing and ARP storm attacks. Furthermore, ARP-based attacks consider the first stage of another attack; for instance, DoS, MITM, and DDoS attacks [5], [6].

To keep abreast these developments and challenges, some proposed solutions emerged as the virtualization, Cloud computing, Software-defined networking (SDN). SDN is a new significant innovation in networking that is expected to address network challenges. SDN introduces the concept of programming networks in a wide network architecture, where the main idea is to separate the data plane and

control plane in the presence of a central device. Therefore, SDN network architecture offers more flexibility to manage the networks. In addition, many security advantageous has been provided depending on the concept of separating planes in the SDN network architecture [7].

1.2 Problem Statement

Ethernet protocol is a dynamic protocol that has many characteristics that allow it to dominate layer 2 networks. Ethernet features allow it to work in different network topologies, where it can be found in LAN network, campus network, enterprise network, and datacenter network. The most prominent features of Ethernet networks are simplicity, low-cost and auto-configuration (plug and play). However, Ethernet networks suffer from the scalability problem, which limits their efficiency and their ability to work when increasing the number of hosts in a network. This is due to the adoption of Ethernet networks on broadcast traffic to discover and update the hosts, where increased broadcast traffic in a single broadcast domain leads to a number of problems that affect heavily on ethernet networks.

Therefore, the researchers have utilized Software Defined Networking (SDN); it is a modern network architecture based on separate network plans (Control and Data planes) to suppress broadcast traffic in Ethernet networks after it has been noticed that ARP and DHCP protocols were the main sources of broadcast traffic. As a result, the researchers succeeded in suppressing broadcast traffic after ARP proxy features are added and the DHCP servers are defined to the SDN controller. Moreover, some hash tables are created to store host information. Therefore, the SDN controller was able to reply to ARP request packet and also to DHCP packets instead of flooding these packets inside the networks.

On the other hand, the researchers had overlooked the interest in the security aspects, where the addition of ARP proxy feature inside the SDN controller will open serious security gaps that can be exploited by attackers, especially ARP where it had some weaknesses in terms of information protection because it did not contain any security mechanism. In this case, the SDN controller became an exhibition by ARP-based attacks. Therefore, the approach of this work depended on previous studies to suppress broadcast traffic after combining two algorithms to protect the SDN controller and other hosts from ARP-based attacks. The first algorithm was the ARP storm detection algorithm, while the second algorithm was the ARP spoofing detection algorithm. The detection algorithms were responsible for analyzing the ARP packet information and comparing the packet information with host information in updated information tables. This research aimed to enhance Ethernet networks by suppressing broadcast traffic and offer protection to the SDN controller and all hosts in the network from ARP-based attacks.

1.3 Research Aim and Objectives

In this research, the main aim is to develop a new mechanism for detecting and mitigating ARP-based attacks on scalable Ethernet network by using Software Defined Network (SDN) technology. In order to achieve this aim, the following areas need attention:

1- To design and develop an ARP Storm detection algorithm based on the updated information tables and the rating of ARP request sent from a host.
2- To design and develop an ARP spoofing detection algorithm based on the updated information table and packet analysis.
3- To develop ARP-based attacks hybrid detection technique in order to create a secure ARP proxy SDN controller.

1.4 Thesis Scope

The scope of this research is focused on providing full protection to SDN controller and network hosts from ARP-based attacks. The most prominent of ARP-based attacks are the ARP storm and ARP spoofing attacks. The proposed approach works in layer 2 (Data Link layer) of OSI model. The proposed approach is implemented by the Mininet emulation program. Furthermore, the proposed approach depended on SDN network architecture features to collect and build update database.

The proposed approach is based on the following assumptions:

1. All DHCP servers are defined to the SDN controller.
2. The host will send an ARP gratuitous packet after static IP configuration.
3. The host will send a DHCP released packet when the host is turned off.

This research is characterized by providing ARP-based attacks detection algorithms.

1.5 Motivation

Network Security has become very challenging over the years. Security vulnerabilities and great advances in technology have made attacks more intelligent and difficult to identify. In general, network attacks are divided into two types which are internal and external attacks. The attacker's location determines the type of the attack. To illustrate, if an attacker is within the network that is to be targeted, this type of attack is called internal attacks. In another case, the type of attack is called external attacks. Meanwhile, these attacks have developed and the intensity of their impact has increased. According to research [8], there are 7,000 DDoS attacks (an attack from the external type) that occur daily and this number is increasing. Internal

attacks also have become a serious risk, threatening the work of local networks. These attacks are characterized by the fact that the attackers are present within the network and may be aware of the network's work, making it sometimes difficult to identify them. According to research [9], there are 65% of organizations worldwide that suffer from DoS attacks (an attack from the internal type). In general, common attacks such as DoS, DDoS, and MITM are based on some other attacks such as Spoofing, Storm, and Scanning as the first stage. For instance, in one of the massive DDoS attacks that occurred in 2014, the attacker used IP spoofing and NTP vulnerabilities (Network Time Protocol) to generate 400 gigabits per second[10].

In addition, new technologies have added a number of other security challenges as a result of their vulnerability. In principle, network programming has brought more security challenges to address some attacks such as spoofing, flooding, and scanning attacks [11]. Furthermore, software defined networks have also opened doors to new threats [12]. The separation of planes (i.e. data and control plane) has given rise to more complex security challenges such as flooding the control plane beyond the capacity of the controllers [13]. This is due to the fact that the implementation of the security protection tasks is left to the developers of the SDN controller applications, who may not be aware of all these attacks [14]. However, there is insufficient research to address all these security challenges [13]. Especially, there are some types of attacks that are executed in a very easy way using available tools that rely on the weakness of protocols such as attacks based ARP, i.e. ARP storm and ARP spoofing attacks.

Consequently, the proposed approach aims to enhance a recent work that addresses the Ethernet scalability problem using software defined network architecture. In principle, from the security aspect, these works are easy to penetrate because they do not have any security mechanism. To the best of the authors' knowledge, this is the first work that combined Ethernet scalability problem and ARP-based attacks.

1.6 Thesis Organization

This dissertation presents how to achieve a scalable and secure Ethernet network from ARP-based attacks. This dissertation is organized as follows. The literature review is present in Chapter 2. An overview of the Ethernet network in terms of the components and addresses used within the network, in addition to the problems experienced by the Ethernet networks, are explained first. Then, the types of network transmission and the broadcast traffic are introduced. Next, in detail the Software-defined networking architecture in addition to the SDN controller and OpenFlow protocol are described. After that, Address Resolution Protocol is illustrated from several axes which are APR messages, ARP operation, and ARP proxy. Then how ARP works inside SDN networks is described. The ARP problems are subsequently explained. Last but not least in Chapter 2, the related work in Ethernet scalability and ARP attacks are presented. Chapter 3 introduced the proposed approach methodology to offer scalable and secure Ethernet network. Here, four algorithms

are presented. The first algorithm is a collecting information algorithm, which is responsible for collecting and updating information of all devices within updated tables. Then, the ARP storm detection algorithm is designed based on comparing packet information with the updated information tables. Next, ARP spoofing detection algorithm is designed based on comparing packet information with the updated information tables. After that, both algorithms are combined (i.e. ARP storm detection algorithm and ARP spoofing detection algorithm) in order to enhance the APR based attack detection. In Chapter 4, the results of experiments are presented in addition to the analyses done with the proper diagrams. Chapter 5 presents the conclusion as well as proposed future work.

REFERENCES

[1] F. A. Lopes, M. Santos, R. Fidalgo, and S. Fernandes, "A Software Engineering Perspective on SDN Programmability," in *IEEE Communications Surveys & Tutorials*, 2016, vol. 18, no. 2, pp. 1255–1272.

[2] "A Security Leader's Definitive Guide to the Threat Landscape [White Paper]," *FORTINET*, 2107. [Online]. Available: https://www.fortinet.com/demand/gated/WP-Security-Leader-Guide-Threat-Landscape.html. [Accessed: 18-Sep-2017].

[3] Digital Equipment Corporation, Intel Corporation, and Xerox Corporation, *The Ethernet: A Local Area Network, Data Link Layer and Physical Layer Specifications*, no. Version 2.0. 1982, pp. 1–103.

[4] D. C. Plummer, "RFC 826: An Ethernet Address Resolution Protocol -- or -- Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware," 1982.

[5] H. Ma, H. Ding, Y. Yang, Z. Mi, J. Y. Yang, and Z. Xiong, "Bayes-Based ARP Attack Detection Algorithm for Cloud Centers," in *Tsinghua Science and Technology*, 2016, vol. 21, no. 1, pp. 17–28.

[6] N. Saputro and K. Akkaya, "PARP-S: A secure piggybacking-based ARP for IEEE 802.11s-based Smart Grid AMI networks," in *Computer Communications*, 2015, vol. 58, pp. 16–28.

[7] S. Scott-Hayward, S. Natarajan, and S. Sezer, "Survey of Security in Software Defined Networks," in *IEEE Communications Surveys & Tutorials*, 2016, vol. 18, no. 1, pp. 623–654.

[8] K. Singh, P. Singh, and K. Kumar, "A systematic review of IP traceback schemes for denial of service attacks," in *Computers and Security*, 2016, vol. 56, pp. 111–139.

[9] D. Kshirsagar, A. Rathod, and S. Wathore, "Performance analysis of DoS LAND attack detection," in *Perspectives in Science*, 2016, vol. 8, pp. 736–738.

[10] J. Kwon, D. Seo, M. Kwon, H. Lee, A. Perrig, and H. Kim, "An incrementally deployable anti-spoofing mechanism for software-defined networks," in *Computer Communications*, 2015, vol. 64, pp. 1–20.

[11] W. Li, W. Meng, and L. F. Kwok, "A survey on OpenFlow-based Software Defined Networks: Security challenges and countermeasures," in *Journal of Network and Computer Applications*, 2016, vol. 68, pp. 126–139.

[12] D. Kreutz, F. M. V. Ramos, and P. Verissimo, "Towards secure and dependable software-defined networks," in *Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking - HotSDN '13*, 2013, p. 55.

[13] H. Wang, L. Xu, and G. Gu, "FloodGuard: A DoS Attack Prevention Extension in Software-Defined Networks," in *Proceedings of the International Conference on Dependable Systems and Networks*, 2015, pp. 239–250.

[14] K. Benton, L. J. Camp, and C. Small, "OpenFlow vulnerability assessment," in *Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking - HotSDN '13*, 2013, pp. 151–152.

[15] T. Kiravuo and S. Mikko, "A Survey of Ethernet LAN Security," in *IEEE Communications Surveys &Tutorials*, 2013, vol. 15, no. 3, pp. 1477–1491.

[16] C. Qian and S. S.Lam, "A Scalable and Resilient Layer-2 Network with Ethernet Compatibility," in *IEEE/ACM Transactions on Networking*, 2016, vol. 24, no. 1, pp. 231–244.

[17] K. Elmeleegy and A. L. Cox, "EtherProxy: Scaling ethernet by suppressing broadcast traffic," in *Proceedings of IEEE INFOCOM*, 2009, pp. 1584–1592.

[18] K. R. Fall and W. R. Stevens, "Ethernet and the IEEE 802 LAN/MAN Standards," in *TCP/IP IIIustrated. Volume 1:The Protocols*, 2nd ed., Addison-Wesley, 2012, pp. 80–84.

[19] D. Law, D. Dove, J. D'Ambrosia, M. Laubach, and S. Carlson, "Evolution of ethernet standards in the IEEE 802.3 working group," in *IEEE Communications Magazine*, 2013, vol. 51, no. 8, pp. 88–96.

[20] W. Odom, "Ethernet Addressing," in *CCENT/CCNA ICND1 100-105 Official Cert Guide*, 1 Edition., Cisco Press, 2016, pp. 52–53.

[21] R. Metcalfe and D. Boggs, "Ethernet: Distributed packet switching for local computer networks," in *Communications of the ACM*, 1976, vol. 19, no. 7, pp. 395–404.

[22] A. Gopalan and S. Ramasubramanian, "Fast recovery from link failures in ethernet networks," in *IEEE Transactions on Reliability*, 2014, vol. 63, no. 2, pp. 412–426.

[23] M. Troy, "Defining Broadcast Domains," in *Cisco Networking Essentials*, 2nd Editio., M. Beth, Ed. Indianapolis, Indiana: Sybex, 2015, p. 281.

[24] H. Cho, S. Kang, and Y. Lee, "Centralized ARP proxy server over SDN controller to cut down ARP broadcast in large-scale data center networks," in *International Conference on Information Networking*, 2015, pp. 301–306.

[25] J. Wang, T. Huang, J. Liu, and Y. Liu, "A novel floodless service discovery mechanism designed for Software-Defined Networking," in *China Communications*, 2014, vol. 11, no. 2, pp. 12–25.

[26] K. Burns, "Limitations of Layer 2 Communication Networks," in *TCP/IP Analysis and Troubleshooting Toolkit*, C. A. Long, Ed. Wiley Publishing, Inc, 2003, pp. 76–77.

[27] Y. Orzach, "Discovering Broadcast and Error Storms.," in *Network Analysis*

using Wireshark Cookbook, First Edit., Packt Publishing Ltd, 2013, pp. 154–155.

[28] "Open Networking Foundation." [Online]. Available: https://www.opennetworking.org/. [Accessed: 02-May-2017].

[29] "Software-Defined Networking: The New Norm for Networks," *ONF White Pap.*, pp. 1–12, 2012.

[30] W. Xia, Y. Wen, C. Foh Heng, D. Niyato, and H. Xie, "A Survey on Software-Defined Networking," in *IEEE Communications Surveys & Tutorials*, 2015, vol. 17, no. 1, pp. 27–51.

[31] E. Kohler, R. Morris, B. Chen, J. Jannotti, M. F. Kaashoek, and · E Kohler, "The Click Modular Router," in *ACM Transactions on Computer Systems (TOCS)*, 2000, vol. 18, no. 3, pp. 263--297.

[32] M. Handley, O. Hodson, and E. Kohler, "XORP: An open platform for network research," in *ACM SIGCOMM Computer Communication Review*, 2003, vol. 33, no. 1, pp. 53–57.

[33] "Quagga Software Routing Suite." [Online]. Available: http://www.nongnu.org/quagga/. [Accessed: 09-Aug-2017].

[34] "The BIRD Internet Routing Daemon." [Online]. Available: http://bird.network.cz/. [Accessed: 09-Aug-2017].

[35] N. Feamster, H. Balakrishnan, J. Rexford, A. Shaikh, and J. van der Merwe, "The case for separating routing from routers," in *Proceedings of the ACM SIGCOMM workshop on Future directions in network architecture*, 2004, pp. 5–12.

[36] J. Rexford *et al.*, "NetworkWide Decision Making: Toward A WaferThin Control Plane," in *Proc. HotNets*, 2004, pp. 59–64.

[37] M. Casado, M. J. Freedman, J. Pettit, J. Luo, N. McKeown, and S. Shenker, "Ethane: taking control of the enterprise," in *ACM SIGCOMM Computer Communication Review*, 2007, vol. 37, no. 4, pp. 1–12.

[38] D. Erickson, "The beacon openflow controller," in *Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking*, 2013, pp. 13–18.

[39] Z. Cai, A. L.Cox, and T. S. Eugene Ng, "Maestro: A System for Scalable OpenFlow Control," 2011.

[40] P. Berde *et al.*, "ONOS: towards an open, distributed SDN OS," in *Proceedings of the third workshop on Hot topics in software defined networking - HotSDN '14*, 2014, pp. 1–6.

[41] T. Koponen *et al.*, "Onix: A distributed control platform for large-scale production networks," in *Proceedings of the 9th USENIX conference on Operating systems design and implementation*, 2010, pp. 1--6.

[42] O. Salman, I. H. Elhajj, A. Kayssi, and A. Chehab, "SDN controllers: A comparative study," in *Proceedings of the 18th IEEE Mediterranean Electrotechnical Conference (MELECON)*, 2016.

[43] N. Gude *et al.*, "NOX: towards an operating system for networks," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 38, no. 3, pp. 105–110, 2008.

[44] "Floodlight OpenFlow Controller." [Online]. Available: http://www.projectfloodlight.org/floodlight/. [Accessed: 16-May-2017].

[45] "The OpenDaylight Platform." [Online]. Available: https://www.opendaylight.org/. [Accessed: 16-May-2017].

[46] Ryu Project Team, *RYU SDN Framework*. 2014.

[47] N. McKeown *et al.*, "OpenFlow: Enabling Innovation in Campus Networks," in *ACM SIGCOMM Computer Communication Review*, 2008, vol. 38, no. 2, pp. 69–74.

[48] S. J. Vaughan-Nichols, "OpenFlow: The Next Generation of the Network?," in *Computer*, 2011, vol. 44, no. 8, pp. 13–15.

[49] "OpenFlow Switch Specification Version 1.0.0," *Open Netw. Found.*, 2009.

[50] "OpenFlow Switch Specification Version 1.5.0," *Open Netw. Found.*, 2014.

[51] S. Carl-Mitchell and J. Quarterman, "RFC 1027: Using ARP to Implement Transparent Subnet Gateways Status," 1987.

[52] L. Toutain and A. Minaburo, "Address Resolution and Automatic Configuration Protocols," in *Local Networks and the Internet: From Protocols to Interconnection*, John Wiley & Sons, 2013, pp. 299–365.

[53] Y. Orzach, "Gratuitous ARP," in *Network Analysis using Wireshark Cookbook*, 2013, p. 186.

[54] J. Singh, S. Dhariwal, and R. Kumar, "A Detailed Survey of ARP Poisoning Detection and Mitigation Techniques," in *International Journal of Control Theory and Applications*, 2016, vol. 9, no. 41, pp. 131–137.

[55] D. Moon, J. D. Lee, Y. S. Jeong, and J. H. Park, "RTNSS: a routing trace-based network security system for preventing ARP spoofing attacks," in *The Journal of Supercomputing*, 2016, vol. 72, no. 5, pp. 1740–1756.

[56] "Proxy ARP," *Cisco*, 2008. [Online]. Available: https://www.cisco.com/c/en/us/support/docs/ip/dynamic-address-allocation-resolution/13718-5.html. [Accessed: 08-Aug-2017].

[57] "Understanding Proxy ARP - Technical Documentation," *Juniper Networks*, 2017. [Online]. Available: https://www.juniper.net/documentation/en_US/junos/topics/concept/port-security-qfx-series-proxy-arp-understanding.html. [Accessed: 08-Aug-2017].

[58] S. Hong, M. Oh, and S. Lee, "Design and implementation of an efficient

defense mechanism against ARP spoofing attacks using AES and RSA," in *Mathematical and Computer Modelling*, 2013, vol. 58, no. 1–2, pp. 254–260.

[59] F. Fayyaz and H. Rasheed, "Using JPCAP to prevent man-in-the-middle attacks in a local area network environment," *IEEE Potentials*, vol. 31, no. 4, pp. 35–37, 2012.

[60] M. S. Song, J. D. Lee, Y. S. Jeong, H. Y. Jeong, and J. H. Park, "DS-ARP: A new detection scheme for ARP spoofing attacks based on routing trace for ubiquitous environments," in *The Scientific World Journal*, 2014, vol. 2014, pp. 1–8.

[61] S. Y. Nam, S. Djuraev, and M. Park, "Collaborative approach to mitigating ARP poisoning-based Man-in-the-Middle attacks," in *Computer Networks*, 2013, vol. 57, no. 18, pp. 3866–3884.

[62] S. Kumar, "Impact of Distributed Denial of Service (DDoS) Attack Due to ARP Storm," in *International Conference on Networking*, 2005, pp. 997–1002.

[63] C. E. Spurgeon and J. Zimmerman, "Broadcast and multicast forwarding," in *Ethernet Switches*, First Edit., M. Blanchette, Ed. O'Reilly Media, Inc, 2013, p. 8.

[64] S. Shukla and I. Yadav, "An innovative method for detection and prevention against ARP spoofing in MANET," in *International Journal of Computer Science and Information Technology & Security*, 2015, vol. 5, pp. 207–214.

[65] F. Li, G. Wu, L. Zhang, J. Chen, and W. Liu, "The Research and Implementation of ARP Monitoring and Protection," in *IEEE International Conference on Internet Technology and Applications (iTAP)*, 2011, pp. 1–4.

[66] A. S. M. Asadujjaman, S. S. Moni, and M. S. Alam, "FCSEA: A Floodless carrier-grade scalable ethernet architecture," in *Proceedings of 9th IEEE International Conference on Electrical and Computer Engineering*, 2017, pp. 427–430.

[67] C. Kim, M. Caesar, and J. Rexford, "Floodless in SEATTLE : A Scalable Ethernet Architecture for Large Enterprises," in *ACM Transactions on Computer Systems*, 2008, vol. 38, no. 4, pp. 3–14.

[68] M. Scott, A. Moore, J. Crowcroft, and D. Wagner-Hall, "Addressing the Scalability of Ethernet with MOOSE," in *DC CAVES Workshop.*, 2009.

[69] K. Kataoka, N. Agarwal, and A. V. Kamath, "Scaling a broadcast domain of Ethernet: Extensible transparent filter using SDN," in *23rd International Conference on Computer Communication and Networks (ICCCN)*, 2014, pp. 1–8.

[70] Y. Xu, X. Lu, and T. Zhang, "A Novel Efficient SDN Based Broadcast Scheme," in *International Conference on Computer Science and Intelligent Communication*, 2015, pp. 196–199.

[71] M. Yokohata, T. Maeda, and Y. Okabe, "An Extension of the Link Layer Discovery Protocol for On-Demand Power Supply Network by PoE," in *27th International Conference on Advanced Information Networking and Applications Workshops*, 2013, pp. 1612–1616.

[72] B. Chen, F. Wei, J. Pan, and Y. Xia, "The Minimum Spanning Trees of tRNA Sequences Based on Prim's Algorithm," in *Fifth International Conference on Natural Computation*, 2009, vol. 6, pp. 176–179.

[73] N. Jehan and A. M. Haneef, "Scalable Ethernet Architecture Using SDN by Suppressing Broadcast Traffic," in *Proceedings of 5th International Conference on Advances in Computing and Communications*, 2015, pp. 24–27.

[74] M. Conti, N. Dragoni, and V. Lesyk, "A Survey of Man in the Middle Attacks," in *IEEE Communications Surveys & Tutorials*, 2016, vol. 18, no. 3, pp. 2027–2051.

[75] "ARPDefender | LAN Intrusion Detection Systems." [Online]. Available: http://www.arpdefender.com/. [Accessed: 14-Mar-2017].

[76] "ARP-GUARD." [Online]. Available: https://www.isl.de/en/arp-guard/product.html. [Accessed: 14-Mar-2017].

[77] Y. Bhaiji., "Security Features on Switches," *Cisco Press*. [Online]. Available: http://www.ciscopress.com/articles/article.asp?p=1181682. [Accessed: 17-Aug-2017].

[78] M. Z. Masoud, Y. Jaradat, and I. Jannoud, "On preventing ARP poisoning attack utilizing Software Defined Network (SDN) paradigm," in *IEEE Jordan Conference on Applied Electrical Engineering and Computing Technologies*, 2015, pp. 1–5.

[79] J. H. Cox, R. J. Clark, and H. L. Owen, "Leveraging SDN for ARP security," in *IEEE SOUTHEASTCON*, 2016, pp. 1–8.

[80] A. Nehra and M. Tripathi, "FICUR : Employing SDN Programmability to Secure ARP," in *7th IEEE Annual Computing and Communication Workshop and Conference (CCWC)*, 2017, pp. 1–8.

[81] T. Alharbi, D. Durando, F. Pakzad, and M. Portmann, "Securing ARP in Software Defined Networks," in *41st IEEE Conference on Local Computer Networks (LCN)*, 2016, pp. 523–526.

[82] L. J. Chaves, I. C. Garcia, and E. R. M. Madeira, "OFSwitch13: Enhancing Ns-3 with OpenFlow 1.3 Support," in *ACM Proceedings of the Workshop on Ns-3*, 2016, pp. 33–40.

[83] Y. Orzach, "ARP and IP Analysis," in *Network Analysis using Wireshark Cookbook*, First Edit., Packt Publishing Ltd, 2013, p. 452.

[84] Cisco System, "Configuring Dynamic ARP Inspection," in *Cisco Nexus 1000v Security Configuration Guide*, 2012, p. (13-1)-(13-18).

[85] J. Postel, "RFC 792: Internet control message protocol," 1981.

[86] Microsoft, "Using the ping command," *Microsoft Technet*, 2017. [Online]. Available: http://technet.microsoft.com/en-us/library/cc737478(v=ws.10).aspx.

[87] D. Hucaby, "Switch port configuration," in *CCNP SWITCH 642-813 Official Certification Guide*, 1 Edition., B. Bartow, Ed. Cisco Press, 2010, pp. 53–54.

[88] Y. Orzach, "Ethernet, LAN Switching, and Wireless LAN," in *Network Analysis using Wireshark Cookbook*, First Edit., Packt Publishing Ltd, 2013, p. 425.

[89] "Ettercap." [Online]. Available: http://sectools.org/tool/ettercap/. [Accessed: 03-Sep-2017].

[90] "dsniff." [Online]. Available: http://sectools.org/tool/dsniff/. [Accessed: 03-Sep-2017].

[91] B. Lantz, B. Heller, and N. McKeown, "A network in a laptop: rapid prototyping for software-defined networks," in *Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks*, 2010, p. 19.

[92] "Open vSwitch." [Online]. Available: http://openvswitch.org/. [Accessed: 24-Oct-2017].

[93] B. Pfaff, J. Pettit, T. Koponen, K. Amidon, M. Casado, and S. Shenker, "Extending Networking into the Virtualization Layer," in *8th ACM Workshop on Hot Topics in Networks*, 2009.

[94] "Wireshark." [Online]. Available: https://www.wireshark.org/. [Accessed: 23-Apr-2017].

[95] "Tcpdump/Libpcap public repository." [Online]. Available: http://www.tcpdump.org/. [Accessed: 23-Apr-2017].

[96] "Top - display Linux tasks." [Online]. Available: https://linux.die.net/man/1/top. [Accessed: 14-Sep-2017].

[97] C. Fernandez, *Software Defined Networking (SDN) with OpenFlow 1.3, Open vSwitch and Ryu*. .

[98] "Scapy." [Online]. Available: http://www.secdev.org/projects/scapy/. [Accessed: 24-Aug-2017].

[99] "XTERM – Terminal emulator for the X Window System." [Online]. Available: http://invisible-island.net/xterm/. [Accessed: 24-Oct-2017].