RESEARCH ARTICLE OPEN ACCESS

Security Mechanism in RIPv2, EIGRP and OSPF for Campus Network - A Review

Devansh Diwan, V.K.Narang, Anuj Kumar Singh
Amity School of Engineering & Technology
Amity University
Haryana - India

ABSTRACT

In the developing world, campus network is generally concerned with the government, corporate and educational organization. Basically one have LAN connections in campus network which is connected to some internet service provider which provides internet connectivity and connects with the outside world. For any campus network, network architecture and it's confidential information is crucial. So, in this research work will be providing the overview of the routing protocols that can be used in campus network and security mechanisms that can be implemented in a campus networks.

Keywords :— Campus Network, Security, RIPv2, EIGRP, OSPF

I. INTRODUCTION

LAN is a logical explanation for how big your area is called local when two or more communicating devices communicate in a room, building or in a campus, they are said to be communicating in a LAN[1]. Few characteristics of LAN and campus network are devices should used be compact and cheap, bandwidth should be high, the owner of promises is owner of LAN, LAN may have distributed or centralized team to handle it. Campus network can be used for government, university and other organization [27]. Campus network typically extend from few 100 of meters to few 10 of kilometre. Campus network can have different type of LAN and it has some service provider with LAN handling team [28]. Over the years different topology, design, architecture have been used for campus network with traffic filtering and security schemes [1].

Routing in campus network is needed for it's internal and external communication. Routing protocol are divided in two category interior gateway dynamic routing protocol and exterior gateway dynamic routing protocol. Interior gateway dynamic routing protocol such as RIP, EIGRP and OSPF are used for internal communication within the organization and external gateway dynamic routing protocol such as BGP is used for external communication.

In nowadays, scenario mostly one dynamic routing protocol such as OSPF or EIGRP is used in campus network. By using more than one routing protocol we can improve campus network. OSPF can be configured in the part of campus network where we have large number of nodes and we require detailed information [10]. EIGRP can be used where we want convergence to be fast. RIP can be used where we have limited number of nodes [9]. Access list are used to provide prioritization to the user. VLAN are used to separate different group of users. Security in campus network is one major issue, security threats may be internal or external. Internal threads occur when someone from inside leaks the information to the outside world whereas external threads occurs when some hacker attacks the network and gets in to the network by crossing all the security mechanism [13]. Thus, to secure confidential information and to prevent network architecture from being exposed we require better security mechanism. Campus network can have better security by using mechanism like DHCP snooping, Time based ACLS, authentication, etc[26]. Security can be enforced at each layer in campus networks. Network monitoring tools can be used to monitor the network and to have better and graphical display of performance and other network parameters[18].

II. LITERATURE REVIEW

An easy way to comply with the conference paper formatting requirements is to use this document as a template and simply type your text into it. The role of campus network has proven to be positive and significant in teaching, scientific research, and campus administration. It is important to have a secure and good campus network to provide important features to the organizations or institute having such campus network. In the next sub heading we will be discussing about the related work done by different authors in past.

A. Related Work

Mohammed Nadir Bin Ali et al [1] purposed secure network architecture for Campus Networks. The author mainly targeted towards campus networks which deliver required security. The research work provide network architecture which is not so flexible and some security mechanism considered are obselete.

Yaxun Lan et al [2] purposed OSPF security optimization mechanism for Campus Network, which aimed at the OSPF security problems existing in the large campus network, the paper research work shows how overhead can be reduced and optimization can be done. There is lack of OSPF key chain authentication mechanism and the concept of totally not so stubby area can be used for full reachability.

Song ji et al [3] performed campus network analysis and design a security system for campus network. The research work reflects the internal and external threads to campus network. There is need for better secure mechanism like ACLs and monitoring tool.

Qiang Li et al [4] worked on Comparison and analysis of IPv4-IPv6 Traffic on the Campus Network. In this research work the traffic management is shown and detection of abnormal behavior is done. However the ways to deal with abnormal behavior must be provided.

Golap Kanti Dey et al [5] performanced Analysis and Redistribution among RIPv2, EIGRP & OSPF Routing Protocol. The ultimate concentration of this research work is to depict the behavior of dynamic routing protocol and to analyze their performance in different scenario. Better graphical performance analysis can be provided and the condition to use particular dynamic routing protocol can be better explained.

Abhishek Verma et al [6] performed survey of RIP and OSPF dynamic Routing Protocols. This research work provides comparison of RIP and OSPF by comparing certain network parameter and metrics..

Eiji Oki et al [7] implemented Traffic Distribution Function of Smart OSPF in Software-Defined Networking. The system shows that a conflict occurs on the common forwarding table, which is accessed by OSPF and SDN, in the edge router when we try to utilize existing software modules in SDN. To solve such problem, author proposed a hybrid router with virtualization technique which provides traffic distributed function with congestion control mechanism.

Manoj Barnela et al [8] worked on the analysis of OSPF, RIP, IGRP and EIGRP Routing Protocols using OPNET 14.5 Simulator. In this research work comparison done among dynamic routing protocol does not considered all the network parameter and also it does not mention when to prefer which particular dynamic routing protocol as per different conditions.

Chandra Wijaya [9] performed a Analysis of Dynamic Routing Protocol EIGRP and OSPF in IPv4 and IPv6 Network. This research reflect behaviour of OSPF and EIGRP routing protocols in IPv4 and IPv6 network. The research work provides comparison of EIGRP an OSPF in different network condition. The author does not provides full graphical representation of performance and other network parameter.

Megha Jayakumar et al [10] studied the comparative behaviour of RIP and OSPF protocols. This paper presents a simple comparative study of RIP and OSPF dynamic routing protocols. The work do not compare them in all possible circumstances as per network parameter.

S. A. Maskari et al [12] provides security and vulnerability Issues in University Networks using CVAT. The scope is limited to use of VPN and VLAN.

Song Ji et al [13] purposed strategy for campus network security by implementing security mechanism at network, system and application layer. The system uses only firewall for security and secure at critical point only.

Q. Zhao et al [14] design a security authentication system based on campus network. There is lack of security at lower layer and device level.

X. Wang et al [15] research about optimization of campus network security system. It only provided detail about few security mechanism which can be used in campus network. Some which are obsolete.

G. Nakibl [16] performed a analysis of OSPF Vulnerability to Persistent Poisoning Attacks. Self defence mechanism can be improved and OSPF key chain authentication can be used. Also stubby area and not so stubby area can be used. Virtual link can be created.

M. Nadir et al [17] design a Secure Campus Network using VLAN and firewall. Traffic filtering is limited to VLAN and security is limited to use of firewall.

X. Li et al [18] design a campus network monitoring system which uses packet capturing technique. Lack of lower level security mechanism and scope is limited to use of network monitoring tool.

W. Zongjiang et al [19] provides a proposal of new type of intelligent network security model for campus study. The system is bounded to use of security model and use of intrusion prevention system can be replaced by better mechanisms like firewalls.

E. Kaffashi et al [20] identified new attack on link-state database in OSPF. Lack of OSPF authentication mechanism and to avoid routing table alteration OSPF should share full database with its neighbor.

S. Publisher et al [21] improved the EIGRP protocol routing algorithm by using security risk parameters. Overheads are increased to keep detail of risk parameters.

K. A. Al-Saud et al [22] provides a performance comparison of MD5 authenticated routing traffic with EIGRP, RIPv2, and OSPF.

M. Yang et al [23] designed a WinPcap based ARP spoofing defence system. The author make use of Intrusion detection system which has been obsolete.

O. Verma [24] effective remote management technique for inter-VLAN routing networks. Use of revision number and pruning mechanism can be done which will provide better stability.

D. Srinath et al [25] provides mechanism for detection and prevention of ARP spoofing. The system make use of centralized server and thus providing single point of failure.

The summary of the work done in the area of security of RIPv2, EIGRP and OSPF in campus network as discussed above is mentioned in Table I.

B. Observations

It can be seen from the literature review that generally in campus network we don't use more than one routing protocol and there is lack of security mechanisms. If there is a lack of security mechanism then it may lead to some security issues in the network. No secure entry point for network such as firewall, there should be one entry point of the network from which whole traffic should pass. There is a scope for implementing secure mechanism like Time based Access-list which allows access to certain feature during certain interval of time only. Further desired level of security can be achieved by using mechanisms like port security, ARP inspection and DHCP snooping. Authentication of different routing protocols allows them to be recognized in the network. Comparative analysis of RIPv2, EIGRP and OSPF in the previous research shows the behaviour of RIPv2, EIGRP and OSPF behave in the network. There comparative behaviour is also known in terms of their convergence and performance. The study of redistribution among RIPv2, EIGRP and OSPF shows that how we can use more than one network protocol in the same network and how these protocol react when redistributed. Previous research shows authentication mechanism of RIPv2, EIGRP and OSPF which help to identify the protocol in the network. The research shows that we can make routing protocol like OSPF more useful by not allowing big routing table to be formed.

TABLE I : SUMMARY OF RELATED WORK

Author(s)	Focus of Study	Findings	Limitations/Gaps
Mohd. N.B.Ali et al [1]	Architecture and security issues in campus network.	Topology and security mechanism used in campus network.	Poor traffic filtering mechanism and slow http response.
Yaxun Lan et al [2]	Use of OSPF in campus network.	Campus network brief and OSPF security mechanism.	Poor mechanism used for best path selection and lack of OSPF authentication.
Song ji et al [3]	Security system of campus network.	Security design and attacks.	Limited to few secure mechanism and no device level security is provided.
Qiang Li et al [4]	Configuration of campus network by IPv4 and IPv6 .	Traffic pattern analysis in campus network and between IPV4 and IPV6 traffic features.	Comparison is done only in terms of packet size and flow size.
Golap Kanti Dey et al [5]	Routing protocols and there redistribution .	Difference among RIPv2, EIGRP and OSPF on the basis of various parameter .	The Scope is limited to few metrics and network parameter.
Abhishek Verma et al [6]	OSPF and RIP and their performance.	Describe behaviour of rip and OSPF considering various network parameter.	It does not consider redistribution among the two routing protocols.
Eiji Oki et al [7]	Functioning of smart OSPF and its distribution.	Implementation of smart OSPF.	Only one routing protocol is considered and there is no optimization in the network.
Manoj Barnela et al [8]	Performance evaluation of OSPF,RIP ,IGRP and EIGRP.	Use of opnet 14.5 simulator and IGRP routing protocol.	There is no redistribution and optimization.
Chandra Wijaya[9]	Analysis of EIGRP and OSPF using both ipv4 and ipv6.	Performance of EIGRP and OSPF using ipv6.	There is no redistribution among routing protocols.
Megha Jayakumar et al [10]	Behaviour and comparison of RIP and OSPF .	Different parameters for RIP and OSPF.	There is no redistribution and optimization among routing protocol.
Lalita Kumari et al [11]	Security status, analysis and strategies for campus network.	Network information and, security problems.	It scope is limited to use of VLAN, VPN and traffic filtering mechanism.
Sanad Al Maskari et al	Campus network	Important of network architecture	Scope is limited to use of CVAT and

[12]	architecture and security issues.	and vulnerabilities due to critical points.	firewalls. Security is provided only at critical points.
Dawei Song et al [13]	Campus network security and security strategies.	Safety Management at Network ,System and Application layer.	System only provide review and comparison with two tier architecture.
Qing Zhao et al [14]	Secure authentication mechanism by providing tickets in campus network	Authentication provided at lower layers for campus network.	System only uses authentication mechanism for security.
Xuanpeng Wanga, et al [15]	Internal network security.	Network security monitoring by using global security.	Scope is limited to use of same security model which may cause problem if requirement changes.
Gabi Nakibly et al [16]	OSPF spoofing and other vulnerability.	OSPF self defence and security mechanisms.	Only network layer security is provided and self defence mechanism is not accurate.
Mohammed Nadir Bin Ali et al [17]	Detection of different network attacks.	Security mechanisms like VLAN and VPN.	Only VLAN.VPN and firewalls are used no device level or upper layer security mechanism is used.
LI Xingyu et al [18]	Campus Network monitoring system and its operations.	Network and security management by monitoring information flow and network stability.	Visualization at scale problem, baselines and packet capturing.
Wang Zongjiang[19]	Set of security model, firewalls, IDS and IPS.	Defence of external invasion and internal data theft	Mechanism are bounded to security model.
Esmail Kaffashi et al [20]	OSPF attack that affect network security by changing routing domain.	Attack that can change the routing table and harmfully threats for network.	Lack of authentication and network layer security.
Snihurov Arkadii1 et al [21]	EIGRP risk parameter traffic filtering and network security.	EIGRP risk calculation data confidentiality and integrity with traffic filtering.	Prioritization and evaluation of traffic credibility can be improved.
Khalid Abu Al-Saud et al [22]	Authentication and traffic analysis in EIGRP, RIPv2 and OSPF.	Authentication mechanism and security issues.	EIGRP does not provide good performance with MD5.
Mingji Yang et al [23]	Network monitoring software and security mechanism for ARP spoofing.	Security against ARP spoofing and man in the middle attack.	System uses IDS mechanism which is obselete, there is a scope for better mechanism like firewall
Rajiv O. Verma[24]	Inter-VLAN routing and VLAN management,	Providing security in VLAN by using access list. VTP issues and native VLAN.	Pruning mechanism can be used and revision number for providing stability.
D. Srinath et al [25]	ARP spoofing and centralized server approach.	Server authentication, use of ARP cache and intrusion detection at lower level.	System do not have port trusted which can lead to security vulnerability and single point of failure.

III. CONCLUSION

There is a lack of security mechanism which makes the campus network vulnerable to different kinds of threats and attacks. For providing better security to campus network we can use security mechanism like ARP inspection, DHCP snooping, Port Security, Private VLAN, Time based ACLs and firewalls.

Most of these security mechanism where missing in the previous schemes and some of them were used but were not effectively used. Some the security mechanism used in past work are obsolete. Every security mechanism has its own functionality and feature. The study shows that how routing protocols like OSPF authenticates itself and how other routing protocol authenticate themselves and can be distinguished in a network. The performance of network can be analysed when we use interior gateway dynamic routing protocols such as RIPv2, EIGRP and OSPF. One can decide when to use particular routing protocol as per functionality. We should use OSPF routing protocol at core layer where we want full detailed description of all network and protocol like EIGRP should be used at the distributed layer, where we want fast convergence only. The significant of this research work is that it helps one to select the routing protocol to be used for campus network along with the effective security mechanism.

REFERENCES

[1] M. N. B. Ali, Prof. Dr. M. L. Rahman and Prof. Dr. S. A. Hossain, "Network Architecture and Security Issues in Campus Networks", IEEE International Conference on Computing Communications and Networking (ICCCNT 2013), pp. 2-5, 2013.

[2] Y. Lan, Z. Chen, " The research on the OSPF security optimizing of Campus Network.", IEEE International Conference on Network and Information Systems for Computers (ICNISC 2015), pp. 592-594, 2015.

[3] S. ji, L. Pang and W. Ying, "Campus network security analysis and design of security system.", IEEE International Conference on Computational Intelligence and Communication Networks (CICN 2015), pp. 1064-1066, 2015.

[4] Q. Li, T. Qin, X. Guan and Q. Zheng, "Empirical Analysis and Comparison of IPv4-IPv6 Traffic: A Case Study on the Campus Network", IEEE International Conference on Networks (ICON 2012), pp. 395-398, 2012.

[5] G. K. Dey, Md. M. Ahmed and K. T. Ahmeed, "Performance Analysis and Redistribution among RIPv2, EIGRP & OSPF Routing Protocol", IEEE International Conference on Computer & Information Engineering (ICCIE 2015), pp. 21-24, 2015.

[6] A. Verma and N. Bhardwaj, "A Review on Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) Routing Protocol", International Journal of Future Generation Communication and Networking, Vol. 9, No. 4, pp. 162-168, 2016.

[7] E. Oki, Y. Nakahodo, T. Naito and S. Okamoto, "Implementing Traffic Distribution Function of Smart OSPF in Software-Defined Networking", IEICE In proceedings of APCC, pp. 239-242, 2015.

[8] M. Barnela, A. Kaushik, Satvika, "Performance Analysis of OSPF, RIP, IGRP and EIGRP Routing Protocols", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 5, pp. 1335-1339, 2015.

[9] C. Wijaya, "Performance Analysis of Dynamic Routing Protocol EIGRP and OSPF in IPv4 and IPv6 Network", IEEE First International Conference on Informatics and Computational Intelligence (ICI 2011), pp. 356-360, 2011.

[10] M. Jayakumar N Ramya Shanthi Rekha, and Dr.B.Bharathi, "A Comparative study on RIP and OSPF protocols", IEEE International Conference on Innovations in Information Embedded and Communication Systems (ICIIECS 2015),p. 978, 2015.

[11] S. A. Maskari, D. K. Saini, S. Y. Raut and L. A. Hadimani, "Security and Vulnerability Issues in University Networks", In Proceedings of the World Congress on Engineering (WCE 2011), Vol 1, pp. 978-988, 2011.

[12] D. Song and F. Ma, "Strategy and implementation of campus network security,"2012 IEEE International Conference on Systems and Informatics (ICSAI 2012), pp. 1017–1019, 2012.

[13] Q. Zhao, Y. Mou, and S. H. Qin, "The design of security authentication system based on campus network," Proc. - Int. Conf. Electr. Control Eng. ICECE 2010, pp. 3070–3073, 2010.

[14] X. Wang and S. Zhang, "Research about optimization of campus network security system," Procedia Eng., vol. 15, pp. 1802–1806, 2011.

[15] G. Nakibl, "OSPF Vulnerability to Persistent Poisoning Attacks : A Systematic Analysis", ACMM Annual Computer Security Applications Conference (ACSAC2014), pp. 336-345, 2014.

[16] M. Nadir, B. Ali, M. E. Hossain, and M. Parvez, "Design and Implementation of a Secure Campus Network," Int. J. Emerg. Technol. Adv. Eng., vol. 5, no. 7, pp. 370–374, 2015.

[17] X. Li and T. Jiang, "Design and implementation of the campus network monitoring system," Proc. - 2014 IEEE Work. Electron. Comput. Appl. IWECA 2014, pp. 117–119, 2014.

[18] W. Zongjiang, "A New Type of Intelligent Network Security Model of the Campus Study", IEEE, pp. 325-329, 2011.

[19] E. Kaffashi, A. M. Mousavi, H. R. Rahvard, S. H. Bojnordi, F. Khademsadegh, and S. Amirian, "A new attack on link-state database in open shortest path first routing protocol," vol. 3, pp.39–45, 2015.

[20] S. Publisher, S. Arkadii, C. Vadym, and C. Vadym, "Improvement of EIGRP Protocol Routing Algorithm with the Consideration of Information Security Risk Parameters," vol. 3, no. 8, pp.707–714, 2015.

[21] K. A. Al-Saud, H. Tahir, M. Saleh, and M. Saleh, "A performance comparison of MD5 authenticated routing traffic with EIGRP, RIPv2, and OSPF," Int. Arab J. Inf. Technol., vol. 7, no. 4, pp. 380–387, 2010.

[22] M. Yang, Y. Wang, and H. Ding, "Design of Win Pcap Based ARP Spoofing Defense System," 2014 Fourth Int. Conf. Instrum. Meas. Comput. Commun. Control, pp. 221–225, 2014.

[23] R. O. Verma, "Effective Remote Management for Inter-VLAN Routing Networks," vol. 2013, no. Ratmig, 2013.

[24] D. Srinath, S. Panimalar, A. Jerrin Simla, and J. Deepa, "Detection and Prevention of ARP Spoofing using Centralized Server," vol. 113, no. 19, pp. 26–30, 2015.

[25] Abhishek Verma and Neha Bhardwaj, "A Review on Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) Routing Protocol ", 2013.

[26] Boger, Paul. CCNA Security. 1st ed. Indianapolis, IN: Cisco Press, 2015.

[27] "Free CCNA Tutorials. Study CCNA For Free!". Study-ccna.com. N.p., 2017. Web. 21 Mar. 2017.

[28] Networkstraining.com. N.p., 2017. Web. 21 Mar. 2017.