International Journal of Scientific Research and Engineering Development-– Volume 4 Issue 3, May-June 2021

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Overview of Multicast Domain Name System

Anshul Agrawal, Yash T Jain, Shravan Y R, Hemavathy R
(Computer Science and Engineering, RV College of Engineering, Bangalore
Email: anshulagrawal.cs17@rvce.edu.in)
(Computer Science and Engineering, RV College of Engineering, Bangalore
Email: yashtjain.cs17@rvce.edu.in)
(Computer Science and Engineering, RV College of Engineering, and Bangalore
Email: shravanyr.cs17@rvce.edu.in)
(Computer Science and Engineering, RV College of Engineering, and Bangalore
Email: hemavathyr@rvce.edu.in)

----------**********----------

Abstract:

Multicast DNS, a popular technique for configuration-less service delivery and discovery, is responsible for a large amount of traffic in today's local networks. If a user wants to enter a local area network without any manual setup, it allows them to use services like computer synchronization, file sharing, and chat. Another issue is the massive volume of multicast traffic that is generated, which is particularly problematic for big Wi-Fi networks. In the case of the mDNS protocol, it is necessary to investigate the element of decentralization of name services and identify security issues arising from the relocation of name servers and Resource Record providers as a result of a shift in the communication paradigm from unicast to multicast. Despite the fact that the resolver and name server communicate in distinct ways,the nature of the communication and security issues has remained essentially the same. This paper highlights the importance of mDNS along with its working process and performance evaluation.

Keywords **— mDNS , DNS , Bonjour , Avahi , Zeroconf.**

----------**********----------

I. INTRODUCTION

The Multicast Domain Name System protocol is a DNS service that allows small networks without a local name server to resolve hostnames to IP addresses. Multicast Domain Name System uses UDP packet instead of the traditional unicast DNS. Therefore, the request to rectify a hostname is received by any node on the network that subscribes to that multicast address. The host that owns that domain name responds with its IP address, often using multicast. As a result, the DNS cache of every node that is connected is updated . The standard DNS infrastructure is not convenient for local services configuration with the invention of IPv6 and the repeated use of multiple embedded devices[1].

A. Scope

I mDNS was designed to find printer devices on a network at first, but it was later extended to resolve local hostnames. The main advantages of mDNS are that it needs no setup and has no infrastructure. It can be accessed without using the traditional DNS settings and without the use of a local name server. Users can also attach to and use network devices more easily because system access is intuitive.

B. Motivation

There is currently no effective method for supporting IP- level Internet-wide multi-source multicast sessions that can be used by almost any ISP.But, mDNS has a number of flaws. For starters, if exposed to the Internet, an intruder can easily get the information about the network's devices and services the user is accessed to. Multicasting is an

inherently effective method of launching DoS attacks[2].Since mDNS is an UDP- based protocol, amplification attacks using mDNS queries are possible, and spoofing attacks are easy.

II. WORKFLOW

Multicast DNS is a name resolution protocol designed specifically for smaller networks. It is done in such a way that differs from the well-known Domain Name System. Rather than questioning a name server, all network members are answered directly. The appropriate client broadcasts a multicast message to the network, inquiring which network member matches the hostname[3]. A multicast is a special type of communication in which a single message is sent to a number of people.

As a result, the request is sent to the community member who owns the hostname that is being looked for. The hindmost responds to all of the network's requests that are generated. Each one is conscious of the connection between the IP address and the name, and they may append a corresponding entry to their cache of mDNS. No one on the network needs to ask for the host name as long as this notation is accurate. While multicast DNS generates a significant amount of traffic, it tries to conserve active network resources. To accomplish it, the client generating the request sends the answer that, in their opinion, is right which is based on the current cache entry[4]. The recipient is required to respond only when this is no more correct. Generally, multicast DNS can only resolve hostnames that end with .local .

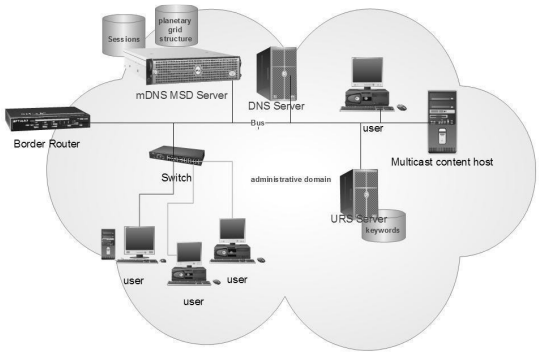

Fig. 1. Typical mDNS System[5]

So on local networks it restricts the use of this kind of name resolution. mDNS does not process hostnames with other top-level domains (TLDs), such as .de or .com. Hence, this technology cannot be used to resolve the web address .

C. Zero Configuration Network

MDNS was created as part of the zeroconf project (Zero Configuration Networking). Zero Configuration Networking is based on the premise that computers can communicate with humans without requiring extensive pre-configuration. Multicast DNS complies with these limitations. The multicast mechanism is part of TCP/IP and can work even if the required parameters aren't in place[6].

III. BENEFITS

D. Compatibility

Multicast DNS is a type of DNS that is meant to make tiny networks more user-friendly. The aim is that users will have no problems connecting devices in covert LANs. No server or directory is required because all devices communicate with one another using their IP addresses[7]. Additional devices can be added quickly and dynamically in this way.

E. Additional Connection

Apple's Bonjour is one of the prominent mDNS implemen- tations. The service is primarily designed to establish connect- ing network printers

to a PC or Mac more conveniently. The devices send and receive information via their IP addresses , hence the user does not need to set up the connection explicitly. You can now utilise the open source programmed Avahi as a mDNS provider in addition to Apple's service([8][9]).

F. Extendibility

This allows you to connect several devices without having to do any setups before. mDNS has been a feature of the Microsoft operating system since Windows 10.

IV. DRAWBACKS

G. Processing Power

There are certain disadvantages to the simple operation. One issue stems from the multicasting technique itself. Although the protocol aims to reduce network traffic, the computers involved must constantly watch the network and process in-coming communications[10]. This puts a strain on the computer's processing power.

H. Assignment of Hostname

Furthermore, the assignment of host names is a difficulty. In theory, as long as it ends in '.local.' you can give each device any name you want. This can result in two network participants having the same host name. The developers of mDNS purposefully did not include a solution for this case.

I. Hazard Source

A hazard source is another issue. The mDNS is open in many circumstances. This means it responds to external queries as well via the Internet. These kinds of open services can be found by cyber thieves and used for DDoS assaults. The devices on the network are then leveraged to flood a target server with inquiries. An open multicast DNS can also be used to find sensitive info[11]. This information is utilized by attackers to read the Mac addresses of connected devices and use it in future assaults.

V. PERFORMANCE

Users do not want to pay for performance degradation,but they also do not want to pay for privacy as well.One of the key aims of our privacy extension is to be at least as fast as conventional mDNS-SD on both the network and the host. Our privacy addition does not add to network burden; in fact, we minimise it by primarily using unicast rather than multicast[12].

J. Responsive and Battery Life

Processing burden on the host devices is undetectable to the user. Our extension restricts access to private services to friends who have been granted permission to connect, as well as the ability to send queries to those who provide the corresponding service, preventing other hosts in the network from being bothered by announcements of services they are not permitted to use and queries for private services that they cannot possibly answer[13]. Remember that private service requests are only sent to friends who offer such services, and private service announcements are only made to friends who have been given permission to connect.

K. Network Load

Instead of delivering a single multicast, the privacy exten- sion sends a unicast to each of those friends whenever a service instance or a service type must be supplied to several friends. This may appear to be a performance issue, however on small networks, the impact of mDNS- SD packets on network load is minor, and on large networks, sending many upstream packets has a lesser effect than receiving a large number of downstream packets, as is the case with multicast[14].

L. Evalutaiom

If each user wishes to send one service discovery packet every time unit, he must send one packet but receive as many packets as there are users in the network using multicast. He must transmit and receive at least as many packets as there are online friends' devices while using unicast. Because many services are only available to a small number of friends, such as device synchronisation, assuming that each packet is sent to 20 devices is

already a lot for networks with up to 1000 members.The number of online friends devices grows as the network grows, but multicasts become even less efficient, making the unicast approach preferable in terms of network load. Because multicasts are delivered at a relatively low transmission rate, older devices that do not support higher transmission rates can receive them as well, multiple multi- casts have a particularly negative influence on network load in large WiFi networks[15-18].

VI. CONCLUSIONS

In this paper, we provide a privacy tweak that allows Zeroconf service discovery while remaining efficient and transparent without multicasting private data. It's highly user- friendly in terms of overhead and control, and it cuts down on the amount of multicast messages transmitted, making mDNS- SD more efficient. One of the most significant advantages of our addition to existing systems is that no existing OSI layer protocols or client software must be modified.Only the Zeroconf daemon on the users' devices needs to be changed, and it can still share service information with unmodified daemons after that. While our privacy modification lets us publish services in a manner that protects users' privacy, it also enables us to multicast nonsensitive services to every user on the network, trying to make it backwards compatible.

ACKNOWLEDGMENT

Our sincere thanks to Dr. Ramakanth Kumar P., Professor and Head, Department of Computer Science and Engineering, RVCE for his support and encouragement. We express sincere gratitude to our beloved Principal, Dr. K. N. Subramanya for his appreciation towards this work.

REFERENCES

[1] J. He, Y. Zhang and X. Yuan, "MDNS based automatic discovery method in optical NMS," 2017 16th International Conference on Optical C.

[2] I. Doln a´k, A. Jantos˘ova´ and J. Litvik, "An overview of DNS security in V2X networks," 2019 17th International Conference on Emerging eLearning Technologies and Applications (ICETA), 2019, pp. 156-159, doi: 10.1109/ICETA48886.2019.9040111.

[3] Communications and Networks (ICOCN), 2017, pp. 1-3, doi: 10.1109/ICOCN.2017.8121329.

[4] S. Cheshire and M. Krochmal, DNS-Based Service Discovery, ser.Request for Comments. Internet Engineering Task Force (IETF), 2013,no. 6763.

[5] https://securityaffairs.co/wordpress/35607/hacking/mdns-amplify-ddos-attack.html

[6] S. Hong, S. Srinivasan, and H. Schulzrinne, "Measurements of multicast service discovery in a campus wireless network," in Global Telecommu- nications Conference, 2009. GLOBECOM 2009.IEEE, 2009, pp. 1–6.

[7] A. Ismail and W. Kastner, "Discovery in SOA-governed industrial middleware with mDNS and DNS-SD," 2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA), 2016, pp. 1-8, doi: 10.1109/ETFA.2016.7733529.

[8] Wireless LAN Medium Access Control (MAC) and Physical Layer(PHY) Specifications, IEEE Computer Society LAN MAN Stan-dardsCommittee IEEE Std 802.11 TM - 2012, 03 2012.

[9] M. Stolikj, P. J. L. Cuijpers, J. J. Lukkien and N. Buchina, "Context based service discovery in unmanaged networks using mDNS/DNS-SD," 2016 IEEE International Conference on Consumer Electronics (ICCE), 2016, pp. 163-165, doi: 10.1109/ICCE.2016.7430565.

[10] B. Konings, C. Bachmaier, F. Schaub, and M. Weber, "Device names in the wild: Investigating privacy risks of zero configuration networking,"in Mobile Data Management (MDM), 2013 IEEE 14th InternationalCon- ference on, vol. 2. IEEE, 2013, pp. 51–56.

[11] A. Siljanovski, A. Sehgal and J. Schönwälder, "Service discovery in resource constrained networks using multicast DNS," 2014 European Conference on Networks and Communications (EuCNC), 2014, pp. 1-5, doi: 10.1109/EuCNC.2014.6882683.

[12] Krebs M., Krempels KH., Kucay M. (2008) A Unified Service Discovery Architecture for Wireless Mesh Networks. In: Das A., Pung H.K., Lee F.B.S., Wong L.W.C. (eds) NETWORKING 2008 Ad Hoc and Sensor Networks, Wireless Networks, Next Generation Internet. NETWORKING 2008. Lecture Notes in Computer Science, vol 4982. Springer, Berlin, Heidelberg.

[13] Kaiser, Daniel & Waldvogel, Marcel. (2014). Efficient Privacy-Preserving Multicast DNS Service Discovery. 10.13140/2.1.1759.9367.

[14] D. Kaiser and M. Waldvogel, "Adding Privacy to Multicast DNS Service Discovery," 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications, 2014, pp. 809- 816,doi:10.1109/TrustCom.2014.107.

[15] J. Macker and I. Taylor, "INDI: Adapting the multicast DNS service discovery infrastructure in mobile wireless networks," 2011 - MILCOM 2011 Military Communications Conference, 2011, pp. 1616-1621, doi: 10.1109/MILCOM.2011.6127540.

[16] Ashmita Raju, Ramya Ramanathan and Dr. Hemavathy R, " A Comparative Study of Spark Schedulers' Performance ", 4th IEEE International conference on Computational Systems and Information Technology for Sustainable Solution (CSITSS-19) , at RV College of Engineering , 20-21st dec 2019.

[17] Sindhu B Dinesh, Hemavathy R -" A review of stream processing platforms and techniques", International Journal of Emerging Technologies and Innovative Research, May 2019, *UGC approved Journal* ,Volume 6, Issue 5, ISSN : 2349-5162.

[18] Ramya Ramanathan, Ashmita Raju , Hemavathy R- "A Comparative Study of Spark Schedulers' Performance", International Journal of Emerging Technologies and Innovative Research(JETIR), UGC approved Journal, May 2019, JETIR209833, ISSN:2349-5162.

