D2DARP: Device-to-Device Address Resolution Protocol

A Secure and Dynamic IP Address Resolution for Modern Decentralized Networked Environments

Researchers: Steve Yoo
Publisher: Data Foundation Lab

June 2024

Abstract

The Device-to-Device Address Resolution Protocol (D2DARP) offers an innovative solution for dynamic address resolution within decentralized networked environments, prioritizing security, data privacy, and decentralization. At the core of D2DARP is a decentralized DNS resolving server that manages data and processes client IP address requests using synthetic subdomain identifiers. The protocol ensures that only authorized clients can access IP addresses by employing robust encryption and authentication mechanisms. It authorizes clients at the subdomain DNS query level, effectively protecting IP addresses from unauthorized access by returning masked invalid IP addresses to unauthorized queries. Additionally, a Virtual Private Server (VPS) is introduced to act as a relay component, serving as a public endpoint that forwards requests to the concealed DNS server, further enhancing privacy and security. This paper examines the design, implementation, and benefits of D2DARP, demonstrating its effectiveness for applications that demand high levels of security and dynamic IP management.

1 Introduction

1.1 Background

Dynamic DNS (DDNS) has been a critical technology in networking, enabling devices to maintain a consistent domain name despite frequently changing IP addresses. Traditionally, DNS records are static, mapping domain names to fixed IP addresses. However, with the proliferation of broadband internet connections and the use of DHCP (Dynamic Host Configuration Protocol) by ISPs, IP addresses assigned to devices often change. This created a need for DDNS, which dynamically updates DNS records to reflect new IP addresses, ensuring that domain names always point to the correct location.

1.2 Problem Statement

Current Dynamic DNS (DDNS) solutions, while effective in maintaining domain-to-IP mappings, present several significant challenges:

1. **Third-Party Control:** Most DDNS services are managed by third-party providers, requiring users to trust these providers with their IP address data. This centralized control represents a single point of failure and a potential data privacy risk.

2. **Lack of Security:** Standard DDNS services typically do not offer robust security measures to protect IP address data. The absence of encryption and secure access control mechanisms can expose devices to unauthorized access and cyber threats. Standard DDNS services generally "point" to a raw specified IP address via a domain query, lacking advanced security protocols.

3. **Inflexibility:** Traditional DDNS solutions often fail to adapt to specific security requirements and diverse use cases, rendering them unsuitable for applications requiring high levels of security and data privacy.

Given these challenges, there is a clear necessity for a secure, private, and dynamic address resolution protocol.

1.3 Objectives

The primary goal of the Device-to-Device Address Resolution Protocol (D2DARP) is to provide a secure, private, and dynamic address resolution protocol that addresses the limitations of current DDNS solutions. Specifically, D2DARP aims to:

1. **Enhance Security and Data Privacy:** Implement robust encryption and authentication mechanisms to protect IP address data, ensuring that only authorized clients can access this information.

2. **Maintain Decentralized Control:** Empower users to control their own DNS infrastructure, thereby reducing dependence on third-party services and enhancing data sovereignty.

3. **Support Dynamic IP Management:** Facilitate real-time updates and management of IP addresses to ensure continuous and coherent device connectivity.

1.4 Related Works

In conceptualizing the Device-to-Device Address Resolution Protocol (D2DARP), it is essential to consider the existing body of research and solutions that address similar challenges in dynamic DNS, device-to-device communication, security, and data privacy. This section reviews relevant works that provide context and background for D2DARP, highlighting their contributions and limitations.

- ***Security and Privacy in Device-to-Device (D2D) Communication:*** Haus et al. (2016) provide a comprehensive review of security and data privacy issues in D2D communication. Their work identifies key threats, such as unauthorized access, man-in-the-middle (MiTM) attacks, and data breaches, and discusses various mitigation strategies. The authors emphasize the importance of robust encryption and authentication mechanisms, which align with D2DARP's focus on ensuring secure and private communication between devices. By addressing these security and data privacy challenges, D2DARP aims to create a more resilient and trustworthy network environment.

- ***Dynamic DNS in IoT Networks:*** Benomar et al. (2021) discuss a cloud-based dynamic DNS approach to enable the Web of Things, focusing on the dynamic management of IP addresses in IoT networks. Their approach leverages cloud infrastructure to handle DNS queries, ensuring scalability and reliability. However, this reliance on centralized cloud services introduces potential data privacy and control issues. D2DARP, in contrast, offers a decentralized solution that enhances data sovereignty and reduces dependence on third-party services, making it more suitable for environments requiring high levels of security and data privacy.

- ***IPv6 Addressing in IoT:*** Zarif et al. (2018) present a hybrid method of IPv6 addressing for IoT devices, aimed at improving address management and network efficiency. While their approach addresses some of the challenges of IP addressing in IoT, it does not focus specifically on the security and data privacy aspects of dynamic address resolution. D2DARP builds on these concepts by incorporating robust encryption and authentication mechanisms to protect IP address data and ensure that only authorized clients can access this information.

- ***Remote Access Using Dynamic DNS:*** Belimpasakis (2006) explores the use of dynamic DNS for remote access to home services, demonstrating how dynamic DNS can facilitate secure remote management of devices. This work highlights the practical applications of dynamic DNS in providing continuous connectivity despite changing IP addresses. D2DARP extends this concept by implementing a decentralized DNS resolving server (DDNSRS) that securely manages IP address changes and ensures that only authorized users can access remote devices, thereby enhancing security and data privacy.

- ***Approaches for Resolving Dynamic IP Addressing:*** Foo et al. (1970) provide foundational insights into methods for resolving dynamic IP addressing, laying the groundwork for modern dynamic DNS solutions. Their research addresses the challenges of maintaining consistent domain names despite frequently changing IP addresses, a core problem that D2DARP aims to solve. By building on these foundational techniques, D2DARP introduces advanced security measures and a decentralized architecture to offer a more secure and private solution for dynamic IP management.

- ***High-Availability Architecture for Dynamic DNS:*** Filippi (2008) discusses the importance of high-availability architectures in dynamic DNS systems, ensuring that DNS services remain operational and responsive under various conditions. This work is relevant to D2DARP's goal of providing a reliable and robust DNS infrastructure. By implementing decentralized control and load-balancing mechanisms, D2DARP aims to achieve high availability and resilience, essential for supporting dynamic and distributed network environments.

The existing body of research highlights the importance of security, data privacy, and reliability in dynamic DNS and device-to-device communication. D2DARP builds on these concepts by introducing a decentralized approach that enhances data sovereignty and provides robust security measures. By addressing the limitations of traditional DDNS solutions and incorporating advanced encryption and authentication mechanisms, D2DARP offers a comprehensive solution for secure, dynamic, and private address resolution in modern networked environments.

2 D2DARP Framework

D2DARP is designed to facilitate secure, private, and dynamic communication between devices. It leverages a decentralized DNS resolving server, which itself is a decentralized device, communicated through a VPS with a static IP address. The VPS allows only ports 53 (DNS) and 22 (SSH) to be open, ensuring secure communication. This setup ensures reliable and secure resolution of IP addresses without exposing data or storing sensitive information.

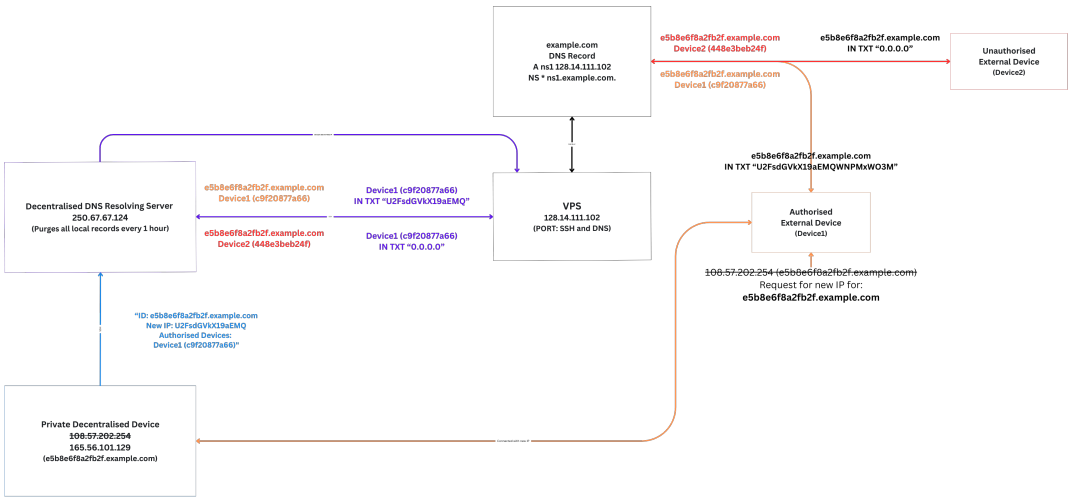

Figure 1: Architecture of D2DARP

2.1 Components of D2DARP

There are four key components within D2DARP, all of which communicate in a decentralized manner.

Decentralized DNS Resolving Server (DDNSRS). The Decentralized DNS Resolving Server (DDNSRS) is a core component of D2DARP, responsible for managing DNS queries and securely storing encrypted IP addresses. This server operates as a decentralized device and is accessed through a VPS with a static IP address. The DDNSRS authorizes client requests at the subdomain DNS query level, ensuring that only authenticated clients can access the actual IP addresses. Unauthorized clients are returned a masked invalid IP address (0.0.0.0), thereby protecting the IP information at the forefront. Regular purging of stored DNS records ensures data privacy and security.

VPS with Static IP. The VPS serves as the public-facing endpoint for D2DARP. It has a static IP address and is configured to only allow traffic on ports 53 (DNS) and 22 (SSH). Acting as a relay, the VPS forwards DNS queries to the hidden Decentralized DNS Resolving Server (DDNSRS). By serving as an intermediary, the VPS enhances the security and data privacy of the DDNSRS, preventing direct exposure to the public internet and ensuring that no sensitive data is stored on the VPS itself.

Decentralized Devices. Decentralized devices are integral to the D2DARP architecture. Each device allocates itself a unique synthetic subdomain identifier which does not exist in any public DNS cache and is responsible for monitoring its own IP address. Upon detecting any changes in its IP address, the device encrypts the new IP information using its own secure keys and the secure keys provided by authorized clients during the initial connection. This ensures that the information is securely tied to both the decentralized device and the clients. Additionally, the information relayed to the Decentralized DNS Resolving Server (DDNSRS) includes the encrypted hashed identifiers of authorized clients. This mechanism ensures that only authorized clients can decrypt and access the new IP address. Even if an unauthorized client or a man-in-the-middle (MiTM) attacker gains access to the encrypted IP address, it will be unusable because it is bound to the authorized client device's hardware hashed identifier. This dynamic update mechanism allows decentralized devices to maintain seamless connectivity and secure communication within the network.

Clients. Clients within D2DARP are those that need to resolve the IP addresses of decentralized devices. These clients query the Decentralized DNS Resolving Server (DDNSRS) using the unique synthetic subdomain identifiers allocated by the decentralized devices. For security, the DDNSRS implements robust authentication mechanisms to ensure that only authorized client devices can retrieve the encrypted IP addresses. Unauthorized queries result in the client receiving a masked invalid IP address, protecting the integrity and data privacy of the decentralized network.

2.2 Workflow of D2DARP

2.2.1 Setting Up

The initial setup of the Device-to-Device Address Resolution Protocol (D2DARP) involves several crucial steps to ensure secure and reliable operation.

1. Deploy a Virtual Private Server (VPS) with a static IP address. This VPS acts as the public-facing endpoint of the D2DARP system.

2. Configure the VPS to relay DNS queries to the decentralized DNS resolving server

(DDNSRS) over SSH. This involves setting up the necessary SSH keys and ensuring that the VPS can securely communicate with the DDNSRS.

3. Register and configure a domain (e.g., example.com) to point to the VPS's static IP address. This ensures that all DNS queries directed to the domain are routed through the VPS.

4. Set up the VPS to allow traffic only on ports 53 (DNS) and 22 (SSH), closing all other ports to enhance security. This configuration ensures that the VPS can handle DNS queries and secure communication with the DDNSRS without exposing other services.

2.2.2 Handling DNS Query

Once the initial setup is complete, the system can handle DNS queries securely and efficiently.

1. When a client needs to resolve the IP address of a decentralized device, it sends a DNS query to the main root domain (e.g., example.com) using the synthetic unique subdomain identifier (e.g., abcd.example.com).

2. The VPS receives the DNS query and forwards it to the decentralized DNS resolving server (DDNSRS) using SSH. This secure communication ensures that the query is transmitted without interception.

3. Upon receiving the query, the DDNSRS processes it using the synthetic subdomain identifier and verifying the client's authorization. The server uses the client's hashed identifier to check if the client is authorized to access the IP address information.

4. If the client is authorized, the DDNSRS responds with the encrypted IP address of the decentralized device. If the client is unauthorized, the server returns a masked invalid IP address (e.g., 0.0.0.0). This ensures that only authorized clients receive valid IP address information.

2.2.3 Dynamically Managing IP Addresses

The dynamic IP management within D2DARP ensures that the system remains updated and secure.

1. Decentralized devices continuously monitor their own IP addresses. When a device detects a change in its IP address, it triggers the update process.

2. Upon detecting an IP address change, the decentralized device encrypts the new IP address using its secure keys and the secure keys of authorized client devices exchanged earlier when setting up. It also includes the hashed identifiers of the authorized clients in the broadcast.

3. The encrypted IP address, along with the client identifiers, is broadcasted to the DDNSRS. This ensures that the DDNSRS always has the most current IP address information.

4. The DDNSRS updates its local records with the new IP address information if an old IP address exists within the 1-hour purge window. Otherwise, it creates a new entry in the record. This update process includes verifying the broadcasted information.

5. To maintain data privacy and security, the DDNSRS regularly purges all DNS records every 1-hour. This purging process ensures that only current and necessary information is retained, reducing the risk of data breaches if they unfortunately occur and maintaining the integrity of the system.

3 Implementation Factors

3.1 Security

Encryption of IP Addresses. In D2DARP, IP addresses are encrypted using advanced encryption algorithms such as AES-256. This approach ensures that even if data is intercepted during transmission, it cannot be read or altered by unauthorized parties. Each decentralized device uses its secure keys along with the secure keys provided by authorized clients to encrypt the IP address information. This dual encryption strategy ensures that only authorized clients can decrypt and access the IP address.

Authorizing Clients. The decentralized DNS server (DDNSRS) implements robust authentication mechanisms to verify client authorization before granting access to IP address information. Each client is assigned a unique hashed identifier during the initial connection setup. When a DNS query is received, the DDNSRS checks the hashed identifier against its list of authorized clients. Only clients with valid identifiers are granted access to the encrypted IP addresses, ensuring that unauthorized clients cannot access sensitive information.

Restricting Access of Ports. The VPS, acting as the relay point, is configured to minimize potential vulnerabilities by shutting off all ports except for ports 53 (DNS) and 22 (SSH). This configuration ensures that the VPS only handles DNS queries and secure SSH communication with the DDNSRS. By restricting port access, the system reduces the attack surface and prevents unauthorized access to other services or data on the VPS.

3.2 Data Handling

Minimal Data Storage. The VPS operates with minimal data storage requirements. It only stores the dynamic IP address of the decentralized DNS server (DDNSRS) through an SSH tunnel for communication purposes only. This means that the VPS acts as a temporary relay, forwarding DNS queries to the DDNSRS without retaining sensitive data. This approach minimizes the risk of data exposure and ensures that the VPS does not become a target for data breaches.

Regular Data Purging. The decentralized DNS server (DDNSRS) regularly (every 1-hour) purges stored DNS records to maintain data privacy and security. This purging process involves deleting all DNS records from the server's local cache.

End-to-End Encryption. All communication between the VPS and the DDNSRS, as well as between decentralized devices and the DDNSRS, is encrypted. This end-to-end encryption ensures that data remains secure throughout the entire transmission process, from the client to the decentralized server and back. The use of SSH for secure communication further enhances this encryption, protecting data from interception and tampering.

Data Integrity Checks. The DDNSRS performs regular integrity checks on the data it stores. These checks involve verifying the authenticity and completeness of synthetic DNS records and IP addresses. By conducting regular integrity checks, the system ensures

that the data has not been altered or corrupted, maintaining the accuracy and reliability of the DNS resolution process.

4 Conceptual Threat Model Analysis

4.1 Threat: Man-in-the-Middle (MiTM) Attacks

In a Man-in-the-Middle (MiTM) attack, an attacker intercepts communication between two parties to eavesdrop or alter the data being transmitted, compromising the integrity and confidentiality of DNS queries and responses. To mitigate such risks, D2DARP employs robust end-to-end encryption mechanisms, such as AES-256, to ensure that all data transmitted between client devices, the VPS, and the decentralized DNS resolving server (DDNSRS) is encrypted, making it extremely difficult for attackers to intercept and read the data. Additionally, communication between the VPS and the DDNSRS is conducted over SSH, providing an extra layer of security. SSH ensures that even if an attacker intercepts the communication channel, they cannot decrypt or alter the data without the appropriate keys. Keeping the SSH keys secure is a must.

4.2 Threat: Unauthorized Access

Unauthorized access occurs when an attacker gains access to sensitive information or services without permission. In the context of D2DARP, this could involve unauthorized clients attempting to resolve IP addresses or access the DDNSRS. To mitigate this risk, D2DARP uses robust authentication mechanisms, assigning unique hashed identifiers to each authorized client during the initial setup. When a DNS query is received, the DDNSRS checks the hashed identifier against its list of authorized clients, ensuring that only authenticated devices can access the IP address information. Additionally, unauthorized queries are responded to with masked invalid IP addresses (e.g., 0.0.0.0).

4.3 Threat: Data Breaches

Data breaches involve unauthorized access to sensitive data, which can lead to data theft, loss, or exposure. In D2DARP, a data breach could compromise the encrypted IP address information stored on the DDNSRS. To mitigate this risk, D2DARP employs regular data purging (every 1-hour), ensuring that only current and necessary information is retained, thereby reducing the amount of sensitive data stored on the server and minimizing the impact of any potential data breach. Additionally, all IP address data is encrypted using robust encryption algorithms, ensuring that even if a data breach occurs, the encrypted data remains unreadable without the decryption keys, thus protecting the confidentiality of the IP addresses.

4.4 Threat: Distributed Denial of Service (DDoS) Attacks

A DDoS attack aims to overwhelm a service with a flood of traffic, rendering it unavailable to legitimate users. Such attacks could target the VPS or the DDNSRS in the D2DARP framework. To mitigate this risk, the VPS is configured to only allow traffic on ports 53 (DNS) and 22 (SSH), significantly reducing the attack surface by minimizing potential entry points for DDoS attacks. Additionally, future enhancements to D2DARP include

implementing load-balancing mechanisms to distribute DNS query handling across multiple DDNSRS instances. This approach helps to mitigate the impact of DDoS attacks by spreading the load and preventing any single server from becoming overwhelmed.

4.5 Threat: IP Spoofing

IP spoofing involves an attacker sending packets with a forged IP address to impersonate another device, potentially disrupting communication and DNS query handling in D2DARP. To mitigate this risk, each client is assigned a unique hashed identifier, which the DDNSRS verifies before responding to any DNS query. This ensures that only legitimate, authenticated devices can participate in the network, rendering IP spoofing attempts ineffective. Additionally, when decentralized devices broadcast their new IP addresses to the DDNSRS, the information is encrypted and includes the hashed identifiers of authorized clients. This encryption ties the IP address data to specific client devices, preventing attackers from spoofing IP addresses.

5 Applications

The Device-to-Device Address Resolution Protocol (D2DARP) is designed to address dynamic address resolution challenges in various networked environments. Its robust security, data privacy features, and decentralized nature make it suitable for a wide range of applications. This section explores the practical applications of D2DARP, highlighting its benefits in Internet of Things (IoT) networks, decentralized applications, and remote access and management scenarios.

5.1 Internet of Things (IoT) Networks

D2DARP provides a robust solution for managing the dynamic address resolution needs of IoT networks. IoT devices often operate in environments where their IP addresses can change frequently due to DHCP or network reconfigurations. D2DARP ensures that these changes are securely managed and propagated throughout the network, allowing devices to maintain consistent and reliable communication. Security and data privacy are crucial in IoT ecosystems, where devices may collect and transmit sensitive data. D2DARP's encryption and authentication mechanisms ensure that only authorized devices can access the network and communicate with each other. This protection is crucial for preventing unauthorized access, data breaches, and cyber-attacks, thereby maintaining the integrity and confidentiality of the IoT network. The protocol's ability to dynamically update and resolve IP addresses allows for the seamless integration of new devices into the IoT ecosystem. As new devices are added or existing devices change their IP addresses, D2DARP automatically updates the necessary DNS records, ensuring uninterrupted communication and functionality across the network.

5.2 Decentralized Applications

Decentralized applications (dApps) often rely on peer-to-peer (P2P) communication to function effectively. D2DARP supports these communication models by providing a secure and efficient way to resolve IP addresses dynamically. This ensures that peers can always locate and connect to each other, even as their network addresses change. Security and data privacy are critical in decentralized networks, where the absence of a

central authority requires robust mechanisms to prevent unauthorized access and data leaks. D2DARP's promise in strong encryption and authentication protocols ensures that only authorized nodes can participate in the network, enhancing the overall security and data privacy of decentralized applications. Decentralized networks can grow rapidly, with nodes frequently joining and leaving the network.

5.3 Remote Access and Management

One of the key challenges in remote access and management is ensuring that connections are secure and that only authorized users can access the devices. D2DARP addresses this challenge by utilizing encrypted communication channels and robust authentication mechanisms to verify user credentials before granting access. This ensures that remote connections are secure and protected from unauthorized access. For organizations managing a large number of remote devices, keeping track of dynamic IP addresses can be challenging. D2DARP simplifies this process by automatically updating the DNS records as devices change their IP addresses. This automated management reduces administrative overhead and ensures that remote devices can always be reached. Authorized users can securely connect to remote devices to monitor their status, perform maintenance tasks, or update configurations. The protocol's ability to handle dynamic IP changes ensures that these remote management tasks can be performed coherently, without interruption.

6 Advantages of D2DARP

D2DARP offers numerous advantages that enhance security, data privacy, and control over DNS infrastructure. By encrypting IP address data and implementing robust authentication mechanisms, the protocol ensures that only authorized clients can access sensitive information. Users maintain control over their DNS infrastructure, reducing reliance on third-party services and enhancing data sovereignty. The protocol's support for real-time updates and continuous IP management ensures coherent connectivity and communication between devices. Additionally, D2DARP's adaptability to various network environments and security requirements makes it suitable for a wide range of applications, providing a flexible and scalable solution for modern networked environments.

6.1 Enhanced Security and Privacy

D2DARP encrypts IP address data using advanced encryption techniques such as AES-256. This ensures that sensitive information is protected during transmission and storage, preventing unauthorized access and data breaches. Even if data is intercepted, it remains unreadable without the appropriate decryption keys, which are limited by device hardware keys and other necessary keys used. The protocol implements stringent authentication mechanisms to verify the identity of clients before granting access to IP address information. Each client is assigned a unique hashed identifier, which is checked against the decentralized DNS resolving server's (DDNSRS) list of authorized clients. This process ensures that only authenticated devices can access sensitive data, further enhancing security and data privacy.

6.2 Data Sovereignty

By maintaining control over its own DNS infrastructure, users can avoid relying on third-party Dynamic DNS services. This autonomy reduces potential vulnerabilities associated with third-party management, such as single points of failure, data exposure, and service outages. Users also retain full ownership and control over their synthetic DNS data, ensuring that it is managed and stored according to their policies and requirements. This approach enhances data sovereignty, allowing organizations to comply with regulatory standards and protect their data from external threats.

6.3 Real-Time Updates

D2DARP supports real-time updates and continuous management of IP addresses, ensuring that devices remain connected even when their IP addresses change. The decentralized devices automatically detect IP address changes, encrypt the new information, and broadcast it to the DDNSRS. This dynamic update mechanism maintains coherent communication between devices, minimizing downtime and disruptions. The protocol automates the process of updating synthetic DNS records, reducing the administrative burden on network administrators. This automation ensures that DNS records are always current, allowing devices to locate and communicate with each other without manual intervention.

6.4 Versatility

D2DARP is designed to be adaptable to a wide range of network environments, from small-scale home networks to large enterprise systems. Its flexibility allows it to be implemented in diverse scenarios, including IoT ecosystems, decentralized applications, and remote access management. The protocol can be tailored to meet specific security requirements of different applications. Organizations can implement custom encryption algorithms, authentication methods, and access control policies to align with their security standards. This adaptability makes D2DARP suitable for applications with varying levels of security and data privacy needs. As networks expand, D2DARP can scale to accommodate an increasing number of devices and IP address changes. The protocol's efficient handling of synthetic DNS queries and dynamic IP updates ensures that it remains effective even in large, complex network environments.

7 Conclusion

D2DARP is a novel solution that addresses the limitations of traditional DDNS services by providing a secure, private, and dynamic address resolution protocol. By leveraging a decentralized DNS resolving server with robust encryption and authentication mechanisms, D2DARP ensures that only authorized clients can access the dynamic IP addresses of devices, maintaining high levels of security and data privacy. This protocol is ideal for applications requiring secure, dynamic, and private communication in modern decentralized networked environments.

8 Future Works

In the future, we plan to implement D2DARP into real-world applications to thoroughly explore and evaluate its benefits, scalability, performance, and optimization factors. This comprehensive evaluation will entail real-world implementation and testing, scalability assessment, performance optimization, security enhancements, and the development of user experience and management tools.

9 References

1. Haus, M., Waqas, M., Ding, A. Y., Li, Y., Tarkoma, S., Ott, J. (2016). *Security and Privacy in Device-to-Device (D2D) Communication: A Review. IEEE Communications Surveys Tutorials.* https://doi.org/10.1109/COMST.2016.2632422

2. Benomar, Z., Longo, F., Merlino, G., Puliafito, A. (2021). *A Cloud-Based and Dynamic DNS Approach to Enable the Web of Things. Proceedings of the IEEE Global Communications Conference (GLOBECOM).* https://doi.org/10.1109/GLOBECOM.2021.9652318

3. Zarif, N. S., Najafi, H., Imani, M., Qiyasi Moghadam, A. (2018). *A New Hybrid Method of IPv6 Addressing in the Internet of Things.* Technical and Vocational University (TVU), Tehran, Iran. Retrieved from https://www.researchgate.net/publication/324556782

4. Belimpasakis, P. (2006). *Remote Access to Home Services Utilizing Dynamic DNS and Web Technologies.* Tampere University of Technology, Department of Information Technology. Retrieved from https://trepo.tuni.fi/handle/10024/93982

5. Foo, S., Hui, S. C., Yip, S. W., He, Y. (1970). *Approaches for Resolving Dynamic IP Addressing. Journal of Network and Computer Applications*, 7(1), 1-12. https://doi.org/10.1016/1970.002

6. Filippi, G. G. (2008). *A High-Availability Architecture for the Dynamic Domain Name System.* Virginia Tech. Retrieved from https://vtechworks.lib.vt.edu/handle/10919/28961

10 Appendix

- **Dynamic DNS (DDNS):** A method that automatically updates the domain name system (DNS) to reflect the changes in the IP addresses of devices. This allows domain names to remain consistent despite the frequently changing IP addresses assigned by ISPs.
- **Device-to-Device Address Resolution Protocol (D2DARP):** A secure and dynamic protocol designed for resolving the IP addresses of devices in a decentralized manner, emphasizing security, data privacy, and user control over DNS infrastructure.
- **Decentralized DNS Resolving Server (DDNSRS):** A core component of D2DARP that manages DNS queries and stores encrypted IP addresses. It operates as a decentralized device, ensuring secure handling of data and client requests.
- **Virtual Private Server (VPS):** A virtualized server that acts as a public-facing endpoint for D2DARP. It relays DNS queries to the decentralized DNS resolving server while only allowing traffic on ports 53 (DNS) and 22 (SSH).
- **Secure Shell (SSH):** A cryptographic network protocol used for secure communication over an unsecured network. In D2DARP, SSH is used to securely relay DNS queries from the VPS to the decentralized DNS resolving server.

- **Internet of Things (IoT):** A network of interconnected devices that communicate and exchange data with each other. IoT networks often require dynamic address resolution due to frequent IP address changes.
- **Synthetic Subdomain Identifier:** A synthetic unique identifier allocated by decentralized devices in D2DARP, used to manage and resolve their IP addresses through the decentralized DNS resolving server.
- **Authentication Mechanism:** Security processes used in D2DARP to verify the identity of clients before granting access to IP address information. This ensures that only authorized devices can access sensitive data.
- **Encryption:** The process of converting data into a coded format to prevent unauthorized access. In D2DARP, encryption is used to protect IP address data during transmission and storage.
- **Man-in-the-Middle (MiTM) Attack:** A security breach where a malicious actor intercepts and possibly alters the communication between two parties. D2DARP mitigates this risk by using encryption and secure client authentication.
- **Data Purging:** The process of regularly deleting outdated or unnecessary data to maintain privacy and security. In D2DARP, this involves purging old DNS records from the decentralized DNS resolving server.
- **Scalability:** The ability of a system to handle increased load or expand in capacity. D2DARP is designed to scale efficiently to accommodate more devices and higher traffic volumes.
- **Data Sovereignty:** The concept that data is subject to the laws and governance structures within the nation it is collected. D2DARP enhances data sovereignty by allowing users to control their own DNS infrastructure without reliance on third-party services.
- **Load Balancing:** A technique used to distribute workloads across multiple computing resources. Future work on D2DARP includes exploring load balancing to manage high traffic volumes efficiently.
- **End-to-End Encryption:** A method of data transmission where only the communicating users can read the messages. In D2DARP, this ensures that data remains encrypted throughout its entire transmission journey.