JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 30 No. 3, pp. 95-102, March 2025
https://doi.org/10.9708/jksci.2025.30.03.095

The Study of On-Device Recursive DNS Techniques for Improving Recursive DNS Performance and Strengthen Security

Inhoe An*, Dongwook Sim*, Byeongsoo Lee*, Yongwan Ju**, Jundong Lee***

*Student, Dept. of Multimedia Engineering, GangNeung-Wonju National University, Wonju, Korea
**Professor, Industry Cooperation Foundation, GangNeung-Wonju National University, Wonju, Korea
***Professor, Dept. of Multimedia Engineering, GangNeung-Wonju National University, Wonju, Korea

[Abstract]

This paper proposes an on-device recursive DNS strategy to address the issues of the traditional centralized hierarchical DNS. The key idea of this on-device recursive DNS approach is to embed part of the DNS service directly into the device itself, rather than relying on external servers that provide DNS services. This aims to enhance the performance & security of DNS services. The strategy is based on the fact that the performance of most computing devices has advanced to a level where they can internally handle part of the DNS service without any issues. The paper compares traditional centralized recursive DNS with on-device recursive DNS, providing a detailed explanation of its structure and principles, and demonstrates the advantages of on-device recursive DNS while presenting a new paradigm for DNS services.

▸ **Key words**: DNS, Authoritative DNS, Recursive DNS, On-Device Recursive DNS, DNS Performance, DNS Security, Resolver

[요 약]

이 논문에서는 기존의 중앙 집중적인 계층형 DNS의 문제점을 해결하기 위한 온디바이스 Recursive DNS 기법 전략을 제안한다. 이 온디바이스 Recursive DNS 기법의 핵심 아이디어는 기존 Recursive DNS 서비스를 DNS 서비스를 제공하는 서버에 의존하는 것이 아닌, 디바이스 그 자체에 DNS 서비스의 일부를 구현하는 것으로 DNS 서비스의 성능과 보안 강화를 의도하는 것이다. 본 설계는 대부분의 컴퓨팅 기기의 성능이 DNS 서비스 일부를 자체 내장하여도 문제 없을 수준으로 발전한 것에 기인한다. 기존 중앙 집중형 Recursive DNS와 온디바이스 Recursive DNS를 비교하여 소개하며 보다 상세한 구조와 원리를 설명하며, 온디바이스 Recursive DNS의 이점을 실증하면서 DNS 서비스의 새로운 패러다임을 제시하고자 한다.

▸ **주제어**: DNS, 권위있는 DNS, 리커시브 DNS, 온디바이스 리커시브 DNS, DNS 성능, DNS 보안, 리졸버

• First Author: Inhoe An, Corresponding Author: Jundong Lee
*Inhoe An (inhoe.an@gmail.com), Dept. of Multimedia Engineering, GangNeung-Wonju National University
*Dongwook Sim (a1wook@naver.com), Dept. of Multimedia Engineering, GangNeung-Wonju National University
*Byeongsoo Lee (bslee@dnacloud.co.kr), Dept. of Multimedia Engineering, GangNeung-Wonju National University
**Yongwan Ju (ywju@gwnu.ac.kr), Industry Cooperation Foundation, GangNeung-Wonju National University
***Jundong Lee (jlee@gwnu.ac.kr), Dept. of Multimedia Engineering, GangNeung-Wonju National University
• Received: 2025. 02. 25, Revised: 2025. 03. 18, Accepted: 2025. 03. 24.

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

I. Introduction

DNS는 인터넷의 발전에 따라 웹, 이메일 등 가장 기본적인 인터넷 서비스 접속을 위하여 전세계 인터넷 이용자들의 질의를 수용하는 기반 응용 서비스로 자리매김해 왔다. 특히 우리나라의 경우 K-컬처(관광, 공연, 음식, 의료 등)의 붐으로 인해 전세계적으로 유입되는 DNS 질의량이 지속적으로 증가하고 있다.

그러나 이러한 DNS는 중앙 집중적인 계층형 서비스 메카니즘을 가지고 운영되고 있어 성능의 한계 및 해킹 등 인터넷 역기능으로 인한 보안상의 취약점 문제를 안고 있고, 이를 해결하기 위하여 글로벌 전문가들은 성능 향상 기법, 보안성 향상을 위한 다양한 기법들을 추가적으로 연구 및 적용하고 있지만 여전히 한계를 보여주고 있다.

1987년에 발간된 RFC1030 등 표준 문헌을 시작으로 기존에 PC 단에서 수행하던 Recursive DNS 기능이 이용자의 증가에 따라 별도의 독립된 Recursive DNS가 설치되어 운영하는 형태로 현재까지 문헌 연구 및 응용 서비스가 적용되어 왔다. 그러나 이러한 집합적인 대행처리는 개방성을 전제로한 DNS 서비스의 특성상 성능의 제약 및 해킹 등의 위협에 노출되어 있다.

이제 H/W, S/W의 기술이 혁신적으로 발전됨에 따라서 온디바이스 AI가 출현하는 시대에 Recursive DNS 기능을 개인용 디바이스에서 수행할 수 있는 상황으로 본 논문에서는 기존의 문헌연구에서 진행해온 서버형 Recurvise DNS에서 벗어나 온디바이스 Recursive DNS 기법 제안을 통해서 DNS 서비스의 성능 향상과 보안상의 위협을 개인단으로 분산함으로 주요 기반시설인 DNS의 안정적인 운영 및 통합적 관리 용이성 등을 달성해 보고자 한다.

II. Preliminaries

2. Related works

2.1 DNS definition and working method

DNS는 인터넷상의 통신기기간의 상호인식을 위한 식별체계인 IP(Internet Protocol) 주소와 사람이 인식하기 쉬운 도메인 네임을 연결하는 매핑기능을 제공하는 계층적인 구조의 글로벌 데이터베이스로서 웹, 메일 등 주요 인터넷 응용 서비스들의 접속을 지원하는 주요 인터넷 기반 서비스이다.

이러한 DNS는 계층적인 도메인 네임 정보를 보유하고 있는 Authoritative DNS와 이의 정보를 찾아주는 서비스적 차원의 Recursive DNS로 크게 나누어지는데 먼저, Authoritative DNS는 전세계 루트로부터 .com, .net, .kr 등와 같은 최상위 도메인, co.kr, ac.kr 등과 같은 차상위 도메인 등 계층적으로 구성되어 도메인 네임 체계에서 그 하위 영역에 대한 위치 정보를 지정하는 권한을 가지는 DNS를 말한다.

대표적인 Authoritative DNS의 시작점인 최상위 루트 DNS의 경우 [fig 1]와 같이 현재 총 13개(A부터 M까지)가 운영 중이다.

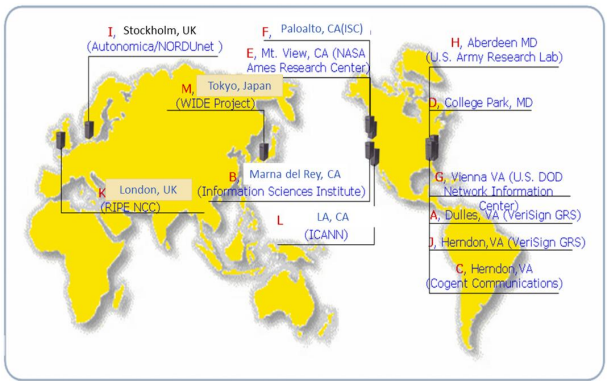


Fig. 1. Top Level Root DNS

2.2 Authoritative DNS

DNS는 주 네임서버(Primary Nameserver), 보조 네임서버(Secondary Nameserver), 존 파일(Zone File), DNS 레코드 등 주요하게 이 4가지 기능으로 구성된다.

① 주 네임서버(Primary Nameserver) : 도메인의 DNS 레코드를 직접 관리하고 업데이트하는 서버로 모든 변경사항은 이 서버에서 시작되며, 보조 네임서버로 전파하는 기능을 담당한다.

② 보조 네임서버(Secondary Nameserver) : 주 네임서버의 데이터를 복제하여 저장하는 서버로 주 네임서버의 부하를 분산시키고 중복성을 제공하여 시스템의 안정성을 향상시킨다.

③ 존 파일(Zone File) : 도메인의 모든 DNS 레코드를 포함하는 텍스트 파일로 이파일은 주 네임서버에서 관리하며 보조 네임서버로 전송된다.

④ DNS 레코드 : A, AAAA, MX, CNAME, TXT 등 다양한 유형의 DNS 레코드가 존재하며, 각기 DNS 활용을 위한 특정 목적을 위해서 사용된다.

Authoritative DNS의 기본적인 작동 방식은 다음과 같다.

① DNS 쿼리 수신

- Recursive DNS로부터 특정 도메인에 대한 DNS 쿼리를 받는다.

② 존(Zone) 데이터 검색

- Authoritative DNS는 자신의 존(Zone) 파일에서 요청된 도메인에 대한 정보를 검색한다.

③ 응답 생성

- 검색한 정보를 바탕으로 DNS 응답을 생성한다. 이 응답에는 요청된 레코드 타입에 따른 정보를 포함한다.

④ 응답 전송

- 생성된 DNS 응답을 쿼리를 보낸 Recursive DNS로 전송한다.

⑤ 캐싱 및 전파

응답을 받은 Recursive DNS는 이 정보를 일정 시간 동안 캐시에 저장하여 향후 같은 쿼리에 대해 빠르게 응답할 수 있도록 한다.

이러한 Authoritative DNS는 [fig 2]와 같이 Authoritative DNS내에 이에 대한 접속 로그 정보를 유지한다. 따라서 이를 분석해 보면 Authoritative DNS에 질의하는 전 세계에 분포하는 Recursive DNS의 위치 정보를 IP 주소를 기반으로 확인할 수 있다.

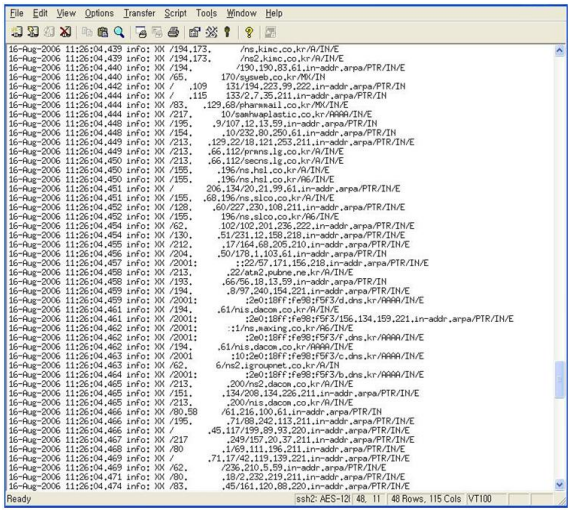


Fig. 2. Log Information of Authoritative DNS

2020년을 기준으로 대한민국에 국가 DNS로 유입되는 DNS 질의는 총 9,237억 건으로, 일 평균 25.2억건, 초당 평균 29,210건 유입되었고, 국가 DNS 질의량은 2021년 이후 연속 증가하고 있으며, 2020년 증가율은 2010년 이후 가장 높은 수치를 보이고 있다.

Table 1. Average daily query volume by year for the past three years

	Year 18	Year 19	Year 20
Daily Average Query	1,956,465,879	2,162,491,589	2,523,707,302
Average Query Per Second	22,644	25,029	29,210
Variation (%)	2.0	10.5	16.7

특히, 최근 5년간 국가 DNS 질의량은 2018년을 제외하고 매년 5%이상 증가하였으며, 2년 연속 10%이상 높은 증가율을 보이고 있다.

Table 2. National DNS average daily query volume by year

	2016	2017	2018	2019	2020
Daily Average Query (Million)	1,797	1,917	1,956	2,162	2,523
Variation (%)	6.36	6.64	2.05	10.53	16.70

2.3 Recursive DNS

이에 반해 Recursive DNS는 클라이언트의 요청을 받아 위의 Authoritative DNS에 계층적인 질의를 통하여 최종 결과 정보를 받아서 클라이언트에게 제공해 주는 역할을 수행하는 DNS를 의미한다.

클라이언트로부터 요청된 재귀적 질의에 대해서 DNS와 함께 포함되어 구현된 리졸버 루틴이 이 요청을 넘겨받는다. 리졸버 루틴은 캐쉬나 DNS의 공유 데이터베이스 등의 로컬 정보를 조회하여 해당 요청 도메인 네임에 대한 정보가 있는 경우 이를 바로 응답으로 반환한다. 만일 그 해당 정보가 없는 경우 리졸버는 루트 DNS로부터 시작하는 도메인 트리 구조를 순차적으로 조회하기 시작하는데 이를 위해서 Recursive DNS의 환경 설정 데이터로 존재하는 전세계 루트 DNS의 IP 주소 정보를 참고하게 된다.

리졸버는 이용자 프로그램을 DNS로 접속해 주는 프로그램으로, 가장 간단한 경우는 리졸버가 서브루틴 호출이나 시스템 호출 등의 형식으로 이용자 프로그램으로부터 요청을 수신하고, 요구되는 정보를 로컬 호스트의 데이터 양식과 호환되는 형식으로 결과를 반환한다.

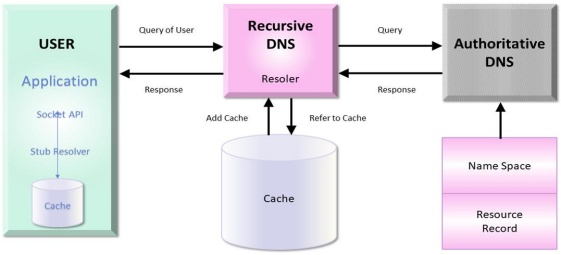


Fig. 3. Service mechanism of Recursive DNS, Authoritative DNS

즉, 리졸버는 [그림 4]에서와 같이 도메인 트리 구조를 순차적으로 탐색하면서 해당 DNS의 IP 주소를 파악한다. 그리고 해당 DNS로 질의를 수행하는데 UDP에 기반을 둔 패킷 구조를 사용하여 단말 클라이언트에 리졸빙한 정보를 응답 후, 리졸버 루틴은 응답 결과를 로컬 캐쉬에 저장한다.

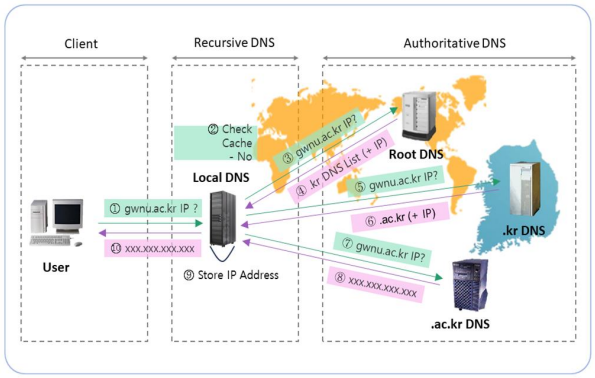


Fig. 4. Example of DNS service based on school domain

.kr과 같은 국가최상위도메인의 경우 gwnu.ac.kr과 같은 3단계 공식 도메인 모두를 .kr에 대한 권위있는 DNS가 관장하여 운영하는 체계로 구성되어 있다. 따라서 이러한 .kr 이하 DNS 정보를 조회하기 위해서는 전세계 모든 Recursive DNS가 .kr 에 대한 Authoritative DNS 에 대한 IP 주소 정보 등 기본적인 정보들을 확인 할 수 있다.

일반적으로 클라이언트에 설정하는 DNS 주소는 Recursive DNS의 IP 주소이며 이는 ISP(Internet Service Provider)에서 초고속 인터넷 접속 서비스를 제공하기 위한 ISP형 Recursive DNS와 회사와 같은 제한된 영역에서 사용하는 가입자형 Recursive DNS로 구분된다. 사용 방법은 동일하게 각각의 이용자에게 그 IP 주소를 공개함으로서 클라이언트가 인터넷 서비스 접속이 가능한 체계로 이루어진다.

2.4 Threats to Recursive DNS

Recursive DNS는 앞에서 설명한 바와 같이 DNS에서 특정 웹사이트나 웹 도메인의 IP 주소를 찾는 첫 번째 단계이다. 이용자가 브라우저에 웹 도메인을 입력하면 DNS 요청 또는 DNS 룩업이 일반적으로 이용자의 ISP(Internet Service Provider)에서 관리하는 Recursive DNS의 서버나 DNS 리졸버로 전송된다. Recursive DNS 리졸버는 로컬 캐시에 저장된 데이터의 IP 정보로 응답하거나 검색을 시작해 다른 DNS를 쿼리하고 최종적으로 Authoritative DNS 서버로부터 정보를 검색한다.

이러한 과정에서 Recursive DNS는 다양한 방식으로 역기능의 표적이 되거나 악용될 수 있는데 현재까지 확인된 주요한 위협은 다음과 같다.

① Dos 공격 : 이러한 캠페인은 압도적인 양의 트래픽과 DNS 요청을 보내 DNS 서버가 느려지거나 충돌을 일으키게 만든다.

② 증폭 공격 : 증폭 공격은 해커가 봇넷으로 알려진 멀웨어에 감염된 머신 네트워크를 사용해 대량의 DNS 쿼리로 DNS 서버를 폭주시키는 일종의 플러드 공격으로 그 결과 DNS 서버에 과부하가 걸려 속도가 느려지거나 충돌을 일으킬 수 있다. 증폭 공격에서 해커는 공격 대상 머신에 매우 긴 응답을 요청하는 방식으로 DNS 요청을 발행해 공격의 영향을 악화시킨다.

③ 캐시 포이즈닝 : 공격자는 DNS 캐시 포이즈닝 공격을 통해 리졸버 서버의 캐시 내에 있는 정상적인 DNS 정보를 악성 웹사이트의 주소로 바꿀 수 있다. 이 경우 정상적인 웹사이트를 찾는 이용자에게 원래 사이트와 동일하게 보이는 완전히 다른 사이트의 IP 주소가 제공되어, 해커는 이 방법을 사용해 이용자를 속이고 로그인 인증정보나 계정 정보와 같은 민감한 정보를 공개하도록 유도한다.

④ 터널링 : DNS 터널링 공격은 DNS를 은밀한 통신 채널로 이용함으로써 방화벽과 네트워크 보안 장치의 탐지를 피해 민감한 데이터를 유출하거나 IT 네트워크 내의 감염된 디바이스를 제어하는 위협이다.

2.5 Status of response to threats

DNS 위협에 대하여 일반적으로 대응장비를 통해서 대응을 하는 Dos 공격이나 증폭 공격 등을 제외하고는 DNSSEC의 도입을 통해서 위협에 대응하고 있다. DNSSEC는 Authoritative DNS 내의 도메인 정보에 대한 암호화를 통해서 인증된 도메인 정보만이 이용자에게 전달되는 것을 확인하는 체계로 이는 크게 서명 부분과 검증 부분으로 나누어진다.

DNSSEC의 서명 부분은 도메인 관리자가 자신의 도메인 존을 서명하기 위한 과정으로, 이는 권한 있는 DNS에 해당된다. 서명 하는 해당 도메인에 대해 키를 생성하고, 공개 키 부분을 존에 삽입한 뒤 비밀키로 존을 서명하는 방식으로 이루어진다. 서명 시 생성되는 보안 위임 정보를 상위 존으로 전송하는 방식으로 작동한다.

그리고 검증 부분은 Recursive DNS가 수행하는 부분으로 도메인 및 IP 정보와 같은 원본 데이터와 더불어 수신되는 서명값에 대한 검증 작업을 수행한다.

III. The Proposed Scheme

3.1 Suggested Method

기존 문헌연구에서 확인된 것과 같이 Recursive DNS의 기능은 처음 일반 PC에서 수행하던 것을 처리해야 하는 정보가 많아짐으로써 더 높은 성능을 요구하게 됨에 따라서 이의 효율적인 처리를 위해서 별도의 Recursive DNS를 설치해 운영하는 방식으로 기존 연구가 진행되어 왔다.

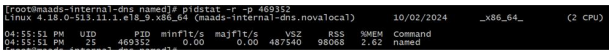
그러나, 디지털 기술의 급격한 발전에 따라 현재 일반 디바이스가 고성능화되고 있고 최근 SLM 기반의 생성형 AI까지 온디바이스화가 가능해짐에 따라서 일반 디바이스 내에서 충분히 Recursive DNS 기능을 수행할 수 있는 시대가 되었다.

일반적으로 디바이스에서 가장 많이 사용하는 OS인 윈도우를 기준으로 권장 메모리 시대적 변화에서 윈도우 7이 출시된 2009년 이후로는 이용자단 디바이스에 Recursive DNS 설치에 필요한 환경을 충족하고 있고, 최근 일반적인 PC 사양을 기준으로 보면 2Core, 3.40GHz, 8GB를 충족하고 있다.

Window Ver.	Recommend Mem.	Window Ver.	Recommend Mem.	Window Ver.	Recommend Mem.
1.0 (1985)	512KB	2.0 (1987)	1MB	3.0 (1990)	2MB
3.1 (1992)	4MB	95 (1995)	8MB	98 (1998)	16MB
2000 (2000)	128MB	ME (2000)	128MB	XP (2001)	256MB
Vista (2007)	1GB	7 (2009)	4GB	8 (2012)	4GB
10 (2015)	4GB	11 (2021)	8GB		

Recursive DNS를 PC단에서 수행하기 위해 필요한 사양을 현재 Recursive DNS 기준으로 볼 때 CPU 2Core 기준 0.02% 정도가 사용 중이고 메모리는 4GB 중 2.62% 정도를 사용 중인 것으로 확인되었다.

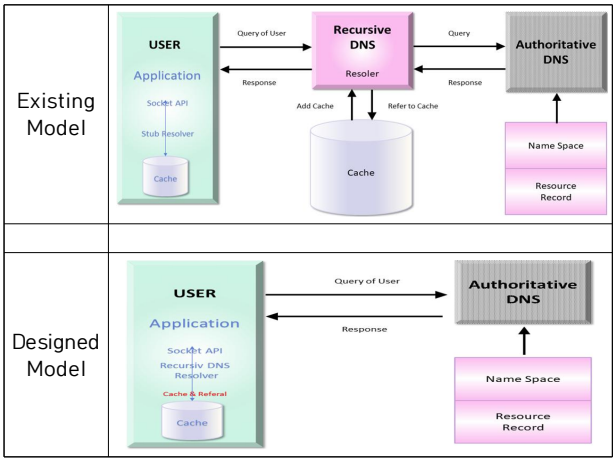
- CPU 0.02% (2Core 기준)



- 메모리 4GB 2.62% (98MB 사용)

이에 따라 현재 PC단의 윈도우를 기준으로 윈도우 8 이상의 버전에서 권장 메모리가 4GB 이상으로 충분히 윈도우 버전의 Recursive DNS 탑재가 가능한 수준이다.

이에 따라서 온디바이스에 캐쉬의 변동을 최소화하고 온디바이스의 부담을 줄인 경량형 Recursive DNS를 온디바이스에 적용시 아래와 같이 현재의 DNS 서비스 체계 및 구성을 단순화하여 이용자단에서 Recursive DNS 서비스 기능을 수행할 수 있다.



이를 위해서는 이용자단 디바이스에서 Resolving 기능을 강화하여 Recursive DNS가 수행하는 Resolving 기능과 캐쉬 관리 기능 등을 추가하도록 구성하여야 하고 이를 위해서 일반 디바이스의 OS 또는 API를 환경에 맞게 설정이 요구된다.

본 온디바이스 Recursive DNS는 ①Recursive Query를 수신하는 수신부 ② Authoritative DNS 정보를 주고받는데 사용하는 Iterative Query 송신부 ③ 송수신 정보를 보관하고 처리하는 다단계 캐쉬 처리부 ④ 그리고 마지막으로 DNS 정보를 암호화하는 DNSSEC 처리부 4개 주요 기능으로 설계되어서 위의 Designed Model과 같이 구축 운영되어야 한다.

이러한 기법의 적용은 DNS 서비스가 로컬상에서 이루어져 응답 시간이 빨라지고, 데이터의 외부 처리로 인한 보안 위협을 해소하면서 보안성을 강화할 수 있고, 하드웨어 요구사항이 낮아지고 업데이트가 편리해 지는 등 다양한 장점을 주면서 전 DNS 서비스에 있어서 성능 향상과 위험영향성을 이용자단으로 분산할 수 있다.

구분	온디바이스 DNS	일반 DNS
데이터 저장 및 쿼리 위치	기기 자체	외부 서버 또는 클라우드 컴퓨팅 리소스
데이터 양 및 용량	로컬 하드웨어 용량에 따라 제한	대규모 데이터 처리 및 무제한 스토리지
응답시간	로컬 처리로 인한 빠른 응답 시간	네트워크 연결에 의한 지연으로 온디바이스 DNS 보다 느린 응답 시간
정보 보호	로컬 처리로 인한 정보 보호 강화	데이터의 외부 처리로 인한 보안 위협 존재
업데이트 및 유지 관리	업데이트 용이	중앙 서버를 통해서 업데이트 및 유지 관리 필요
하드웨어 요구사항	낮음	중간 이상

구분	Benefit	Cost
일반 PC	빠른 DNS 질의.응답	Recursive DNS 기능 수행에 따른 시스템 활용
기존 Recursive DNS	설치.운영 비용 제로	없음
	보안위험에 관한 위험성 분산 효과	없음
전 DNS 서비스	IPv6, DNSSEC 등 차세대 기술 적용 용이	없음
	Recursive DNS 위험영향성 분산 효과	없음

IV. Method-Effect Evaluation

4.1 Improved query and response speed of DNS service

일반적인 DNS 서비스 체계에서 이용자에게 서비스를 제공하는데 소요되는 시간 TDNS는 아래의 식에 의해 계산될 수 있다.

$$TDNS = TRDT + TRDP + n \times (TADT + TADP) \times CAuth$$

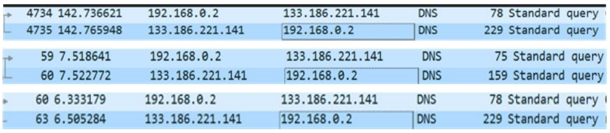
여기서 TRDT는 이용자 클라이언트와 Recursive DNS 간의 데이터 전송 시간을 의미하며, TRDP는 DNS 정보를 얻기 위하여 Recursive DNS내에서 처리되는 시간을 의미한다. TADT와 TADP도 각각 Recursive DNS와 Authoritative DNS간의 데이터 전송시간과 Authoritative DNS에서의 데이터 처리 시간을 의미한다. 이러한 Authoritative DNS 질의는 여러 단계를 거치게 되므로 n은 Authoritative DNS를 거치는 단계를 의미하며 CAuth는 각 단계의 Authoritative DNS에서의 지연시간을 의미한다.

그러나 제안된 기법을 적용할 경우 TRDT와 TRDP가 제거되어서 이용자 단말단에서 바로 처리되는 부분으로 이 부분만큼의 질의.응답 속도가 개선될 수 있다.

$$TDNS = n \times (TADT + TADP) \times CAuth$$

DNS 캐쉬가 PC 및 로컬 recursive DNS 에 없는 경우 TDNS = 0.17ms

- DNS 캐쉬가 로컬 Recursive DNS에 있는 경우 TDNS = 0.03ms
- DNS 캐쉬가 로컬 PC에 있는 경우 TDNS = 0.004ms



4.2 Dispersing the impact of security threats caused by hacking

기존에 Recursive DNS 자체에 집중되어 있는 캐쉬가 오염될 경우 이러한 오염된 캐쉬는 본 Recursive DNS를 사용하는 전체 이용자에게 영향을 미치고, 또한 해당 DNS에 DDoS 공격시 이를 이용하는 전체 이용자에게 서비스가 단절되는 등 문제의 영향이 클 수 있다.

본 기법의 적용이 이러한 DDoS 공격 범위, 캐쉬 오염의 영역이 이용자단 디바이스에만 영향을 미치므로 보안 위협의 영향성을 Recursive DNS 전체 이용자에서 해당 디바이스 이용자 수준으로 낮출 수 있다.

특히 ISP단의 Recursive DNS를 활용하여 인터넷에 접속하는 경우 이러한 보안상의 위협이 해당 ISP를 사용하는 전체 이용자에게 영향을 미칠 수 있으나 본 기법의 적용시 앞에 상술한 대로 ISP의 사용 여부와 관계없이 의존성을 혁신적으로 낮추어서 이용자 본인의 디바이스 영역에서만으로 문제 발생을 최소화 할 수 있다.

V. Conclusions

온디바이스라는 개념은 AI 시대가 다가오면서 다시금 주목받는 개념이다. 온디바이스 Recursive DNS는 온프레미스, 클라우드 등에서가 아닌 디바이스 자체에서 DNS 서비스를 실행하며 이용자가 기존 방식보다 더 빠르고, 안정적으로 DNS 서비스를 받을 수 있는 기법이다.

이는 DNS 쿼리 처리가 DNS 서버로 전송되는 과정 중 일부를 이용자 디바이스 자체에서 처리하여 DNS 쿼리 과정상에 처리 속도를 개선할 수 있고, 네트워크의 의존성을 현존하는 방식보다 낮출 수 있으며, DNS 레코드 데이터에 대한 보안성을 향상시키면서 속도와 반응성 측면에서 향상을 가져올 수 있다.

특히, 정부, 공공에서 물리적 망분리 의무화 규제가 완화되는 시점에서 이러한 서비스 적용시 고도의 보안성이 요구되는 국가 및 공공기관, 산업기밀을 취급하는 기관 등에서 실재 적용시 외부의 서버 사용 없이 온디바이스에서 인터넷의 접속점 확인 서비스를 사용할 경우 현존하는 방식보다 접속 속도가 빨라질 뿐만 아니라 외부 인터넷 환경의 보안 취약점에 의존하지 않고 자신의 PC에서만 처리가 가능하여 전체적인 보안성 향상을 가져올 수 있어 향후 안정적인 인터넷 서비스 도입에 기여할 것으로 기대된다.

본 기법은 향후 DNS 공격 등에 대한 다양한 정보 등을 수집할 수 있는 연구 인프라로도 활용될 수 있어 이에 대한 실험 환경 및 실 환경에서의 성능과 보안성의 실증 및 효과 검증은 향후 연구 과제로 지속적으로 추진되어야 한다.

ACKNOWLEDGEMENT

This work was supported by the Institute of Information & Communications Technology Planning & Evaluation(IITP)-Innovative Human Resource Development for Local Intellectualization program grant funded by the Korea government(MSIT) (IITP-2025-RS-2023-00260267)

REFERENCES

[1] Kim HJ, & Ju Yong Wan (2005-11-19). Analysis of main technique for DNS Cache Poisoning and their counterplans. Proceedings of Symposium of the Korean Institute of communications and Information Sciences, Seoul.

[2] Seunghoon Lee, Yongwan Ju, & Weon Kim (2005-06-30). A Study of Anycast DNS implementation for KR Name Server. Proceedings of Symposium of the Korean Institute of communications and Information Sciences, Pyeongchang.

[3] Geonung Kim, Byung-Kwen Song, Jae-Chang Kwak, Seung-Hoon Lee, Yong-Wan Ju, & Weon Kim (2004-11-20). DNS Extensions and BIND 9.x. Proceedings of Symposium of the Korean Institute of communications and Information Sciences, Seoul.

[4] Seunghoon Lee, Yong-Wan Ju, & Weon Kim (2004-04-28). A Study on the Applicable IPv6 DNS for .KR Name Server.

[5] Geonung Kim, Byung-Kwen Song, Yong-Wan Ju, & Weon Kim Survey on the IETF Activities for IPv6 Multi-homing. Proceedings of Symposium of the Korean Institute of Information Scientists and Engineers.

[6] Patrik Hudák, “Analysis of DNS in cybersecurity”, https://is.muni.cz/th/byrdn/Thesis.pdf

[7] Google Cloud, “General DNS overview”, https://cloud.google.com/dns/docs/dns-overview?hl=en

[8] Microsoft, “DNS standards Documents”, https://learn.microsoft.com/en-us/windows/win32/dns/dns-standards-documents

[9] RedHat, “Chapter1. Introduction to the DNS service”, https://docs.redhat.com/en/documentation/red_hat_openstack_platform/17.1/html/configuring_dns_as_a_service/intro-dns-service_rhosp-dnsaas#intro-dns-service_rhosp-dnsaas

[10] Akhavan Niaki, Seyed Arian, “MEASURING NETWORK INTERFERENCE AND MITIGATING IT WITH DNS ENCRYPTION”, University of Massachusetts Amherst, Vol. 1, No. 1, pp. 1-13, January 2025, DOI:10.7275/28406713

[11] Dongwon Kim “ DNS amplification attack for SDN”, KICS, Vol 43-11, pp. 1959-1969, Nov. 2018, DOI:10.7840/kcis.2018.43.11.1959

[12] Dongwon Kim “DNS Design based on Blockchain Network”, KIISE, Vol 45-1, pp. 123-126, Dec. 2018, DOI:10.3745/PKIPS.y2018m12a.123

[13] Mike Kosek, Luca Schumann, Robin Marx, Trinh Viet Doan, Vaibhav Bajpai, “DNS privacy with Speed? Evaluating DNS over QUIC and its Impact on Web Performance”, arXiv preprint arXiv:2305.00790, May 2023, DOI:10.48550/arXiv.2305.00790

[14] Levent Csikor, Dinil Mon Divakaran, “The Evolution of DNS Security and Privacy”, arXiv preprint arXiv:2312.04577, May 2023, DOI:10.48550/arXiv.2312.04577

Authors

Inhoe An is the Director of the MyData Promotion Center at the Korea Internet & Security Agency (KISA). He received a B.S. in Computational Statistics from Dankook University and an M.S. in Computer Engineering from Yonsei University. His research interests include personal data protection, information security, and platform technologies.

DongWook Sim is a director of the Personal Data Secure Usage Group at Korea Internet & Security Agency. He received as B.S., M.S. degree from Sungkyunkwan University and completed a doctorate at Gangneung-Wonju National University. His research interests include IT, Data Privacy, Cyber Security, and Digital Business.

Byeongsoo Lee is a CEO of DNA Cloud Co., Ctd. and is a master's student in the Department of Multimedia Engineering at GangNeung-Wonju National University. His research areas include networks, DNS, and DNS security.

Yongwan Ju is a professor at GangNeung-Wonju National University. He received as B.S., M.S. respectively in Business Adminstraion in Hankook University Foreign Study and Ph.D. degree in Computer Science from Soongsil Unversity, Seoul Korea in 2007. His research interests include IoT, Platform Business, Big Data and Security etc.

Jundong Lee is a professor with the Department of Multimedia Engineering at GangNeung-Wonju National University. He received as B.S., M.S., and Ph.D. degree in Computer Science from HongIk Unversity, Seoul, Korea in 1990, 1993, and 2001, respectively. His research interests include programming language, IoT, and platform.