Proceedings of CONF-SEML 2026 Symposium: Computational Analysis and Modeling in Complex Intelligent Systems
DOI: 10.54254/2755-2721/2026.GU32420

A Review of Technologies for Preventing DNS Hijacking in Smart Home Systems

Ruize Xu

School of Mechanical Engineering, Hefei University of Technology, Hefei, China
2024211603@mail.hfut.edu.cn

Abstract. With the widespread adoption of smart homes, Domain Name System (DNS), as a core infrastructure, is facing severe hijacking threats. This paper adopts a systematic literature review method, focusing on the prevention technologies of DNS hijacking in smart home scenarios. It is organized from four dimensions: attack mechanism, vulnerability, defense technology, and architecture design. The research clarifies the amplification effect of DNS hijacking, which is formed by the router as the pivot, resulting in "one point breakthrough and total network collapse". It summarizes the threefold hazards of privacy leakage, network fraud, and botnets. It analyzes the vulnerabilities at the terminal, network, routing, and upstream service levels. Through in-depth analysis of representative studies such as DNSwitch, LDoS detection, LKTADN, ID/Loc separation, ZT-BlocIoT, and DBDNS, it reveals the trend of defense technology evolving from single-point encryption to system architecture and from passive response to active trust assessment. Currently, the research still faces challenges such as lightweight deployment and cross-layer collaboration. In the future, it should integrate zero trust, blockchain, and edge intelligence to build a collaborative protection system with active perception and trusted verification.

Keywords: Smart home system, DNS hijacking, Zero trust architecture

1. Introduction

DNS is a basic infrastructure of the Internet that resolves domain names into IP addresses and serves as the indispensable link for interconnecting smart home devices and the invocation of cloud services. However, DNS hijacking attacks which redirects user to malicious websites by tampering with resolution results are increasingly threatening smart home system security. Attackers can utilize router vulnerabilities or employ DNS pollution to hijack and steal privacy, illegally control key devices such as smart locks and even form botnets [1].

The rise of DNS privacy protection has become an irreversible technological trend. However, while the community embraces this trend, it should also expand its research focus to the solutions themselves and their profound impact on the existing network architecture and associated services. This is a necessary prerequisite for ensuring a smooth and orderly implementation process of the technology and a safe and reliable system evolution.

In recent years, encryption-based DNS protocols such as DNS over HTTPS/ DNS over TLS (DoH/DoT) verification mechanisms and zero-trust architectures have made significant progress in

© 2026 The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

DOI: 10.54254/2755-2721/2026.GU32420

defense technologies, but there are still key gaps: the current solutions are mostly designed for the general Internet environment and lack in-depth adaptation to the characteristics of limited resources and heterogeneous devices in smart home scenarios. Moreover, most focus on achieving breakthroughs in individual points and have not yet established an architecture protection system.

This paper adopts the systematic literature review method, focusing on the architecture of smart home systems for preventing DNS hijacking. It systematically reviews the attack surface and defense technologies, summarizes architectural design principles and explores future research directions. This research aims to provide a theoretical framework for subsequent researchers, and also offers reference and guidance for the industry in building a secure and trustworthy smart home environment.

2. Risk mechanism

2.1. The principle and types of DNS hijacking

DNS hijacking is an attack method that disrupts the integrity of the domain name resolution process and redirects user traffic to malicious servers. The core principle is to tamper with the DNS query-response chain. When the user's device sends a domain name resolution request to the DNS server, the attacker interferes with the response data and returns a forged IP address, enabling the user to access a phishing website or malicious servers without their awareness.

According to the location where the attack is carried out, DNS hijacking can be mainly classified into the following types: Local DNS hijacking refers to the act where an attacker modifies the local DNS configuration through malicious software or router vulnerabilities; Man-in-the-middle DNS hijacking occurs during the query transmission process. The attacker modifies the response data in real time through means such as Address Resolution Protocol (ARP) spoofing; DNS cache poisoning is a method that causes DNS servers to store incorrect domain-name-to-IP mapping relationships in their cache. Router DNS hijacking is particularly common in smart home systems. Attackers exploit vulnerabilities in routers to modify the DNS forwarding settings, thereby achieving the batch hijacking of all devices in the home. Malicious DNS server hijacking involves controlling authoritative DNS servers or forging malicious resolution services to undermine the credibility of the resolution process at its source.

2.2. The vulnerability of the smart home system

The DNS vulnerability of the smart home system stems from the structural contradiction between its complex architecture and limited protection.

At the terminal level, a large number of intelligent devices are constrained by computing resources and cost control, and generally lack an in-built DNS query verification mechanism. Attackers can carry out local DNS hijacking by using malicious software or weak passwords. By modifying the device configuration files, they can direct the device to a fake site to steal cloud service credentials.

At the network transmission level, the Wi-Fi environment commonly used in smart homes provides the technical conditions for man-in-the-middle attacks. The attacker uses ARP spoofing or forging of the access point to tamper with the DNS response data in real time on the wireless link. Such attacks are transparent to the terminals and it is difficult for users to establish effective awareness.

DOI: 10.54254/2755-2721/2026.GU32420

The more critical vulnerabilities are concentrated at the router level. As the network hub, vulnerabilities in the router firmware or default credential settings can be exploited to carry out DNS hijacking of the router. Once the attacker modifies the DNS forwarding configuration, they can achieve batch control over all the devices in the house. However, the terminal devices are unable to detect such anomalies.

Furthermore, attacks targeting the upstream part of the chain also pose a serious threat. DNS cache poisoning can redirect the firmware upgrade domain name to malicious servers. It may cause the device to lose control on a large scale. Also, malicious DNS server hijacking may undermine the credibility of domain name resolution by controlling authoritative servers or forging resolution services at the source.

In conclusion, the DNS vulnerability of the smart home system is a systemic risk caused by the heterogeneity of devices, the openness of the network, and the loose configuration. Attackers can find opportunities at any node in the resolution chain.

2.3. The harm caused by DNS hijacking to smart homes

In the smart home environment, the reason why DNS hijacking constitutes a serious threat lies in the fact that it uses the router as the attack point, creating an amplification effect of "a single point of failure leading to the collapse of the entire network". Once the DNS configuration of the router is tampered with, the entire smart home ecosystem will face three significant and substantial hazards: First, the leakage of sensitive data. The attacker can use a malicious DNS server to intercept the communication metadata of devices such as smart door locks, video streams from security cameras, and voice assistant commands. This enables them to conduct long-term surveillance and eavesdropping on the user's home activities.

Second, precise online fraud. For instance, in the large-scale router hijacking incident in Brazil in 2019, the attackers tampered with the DNS settings of over 180,000 devices. They redirect users' legitimate requests to access bank websites to phishing pages, resulting in the theft of a large number of financial credentials.

Thirdly, they become zombies for cyber-attacks. Devices affected by DNS hijacking may be infected with malicious software. For instance, the "Kimwolf" botnet that was exposed in 2025 infected over 180,000 smart TVs and set-top boxes. It exploited these devices to launch a distributed denial-of-service attack with a peak traffic volume of nearly 30 Tbps, causing users to unknowingly become involved in cybercrime activities.

Therefore, DNS hijacking has formed a complete attack chain that extends from privacy theft, property loss to resource blackmail. This fully highlights the urgency and necessity of strengthening the security protection of the basic network infrastructure of smart homes.

3. Preventive technology

3.1. DNSwitch

Maksutov et al. conducted a systematic study on the detection and defense mechanisms for DNS spoofing attacks [2]. This study first analyzed the principle of the man-in-the-middle attack based on SSLstrip+, pointing out that it can forge DNS responses through the dns2proxy tool, effectively circumventing the protection of the HTTP Strict Transport Security (HSTS) policy, and thereby posing a substantial threat to HTTPS communication. Based on the review of the existing defense solutions including IPSec tunnels and DNSCrypt, the author pointed out that these methods all

DOI: 10.54254/2755-2721/2026.GU32420

ensure communication security at the cost of continuous encryption, and it is difficult to balance the efficiency of resolution and the reliability of transmission. To address this contradiction, this research proposed and implemented a lightweight detection tool named DNSwitch. Its core mechanism lies in concurrently initiating DNS resolution requests through both the local plaintext channel and the remote encrypted channel, and identifying potential attacks by comparing the response results. DNSwitch supports two operation modes: single detection and continuous monitoring. It can automatically switch to an encrypted communication channel upon detecting deceptive behavior, thereby enhancing the proactive defense capability of the local area network environment without significantly increasing system overhead. Experimental results show that this tool can effectively identify IP tampering attacks targeting domain name resolution and is feasible for collaborative deployment with existing security solutions.

3.2. A detection method combining two-step cluster analysis and UTR analysis

Tang et al. proposed a detection method for low-rate denial of service (LDoS) attacks in 2020, which integrates two-step clustering analysis with User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) traffic ratio (UTR) analysis [3]. This study first points out that LDoS attacks trigger the TCP congestion control mechanism by intermittently sending bursty traffic, causing the TCP throughput to periodically decline. Their low-rate characteristic makes traditional detection methods based on statistical anomalies difficult to effectively identify. Based on this, the author of this article introduces variance and information entropy as the characteristic metrics of TCP traffic to describe the discreteness and instability of TCP traffic under attack conditions; meanwhile, considering that LDoS attacks usually use the UDP protocol to construct attack flows, UTR will show significant changes during the attack period. The detection process is divided into two stages: Firstly, a two-step clustering analysis based on the BIRCH algorithm and agglomerative hierarchical clustering is used to group traffic data with similar characteristics into the same cluster; subsequently, through UTR analysis and comparison with the preset threshold, it is determined whether each cluster has been subjected to LDoS attack. A series of experiments was conducted on the NS2 simulation platform, physical test bed, and WIDE public dataset. The results show that this method performs well in terms of detection accuracy, recall rate, and F1 score, and has a competitive advantage over existing methods such as multifractal, Kernel Principal Components Analysis(KPCA), and wavelet feature extraction in terms of false alarm rate and missed detection rate. The paper also points out that the current method is only applicable to the detection of UDP-based LDoS attacks. The detection mechanism for TCP-type LDoS attacks still needs further research.

3.3. LKTADN

Yao and Lin, in 2025, addressed the issues of difficulty in extracting multi-scale spatiotemporal features, imbalance of category samples, and low efficiency of model deployment in the detection of abnormal network traffic, and proposed an anomaly detection network LKTADN, based on lightweight knowledge transfer [4]. This study first constructed a multi-scale spatiotemporal feature extraction network (MSTFN) by introducing multi-scale residual modules and long short-term memory networks, to jointly model the local spatial features and temporal dependencies of network traffic. Based on this, the research further introduces the knowledge distillation technique, transferring the deep spatiotemporal knowledge extracted by the complex teacher model MSTFN to the lightweight student model LSTFEN. It also combines the focal loss function to enhance the

DOI: 10.54254/2755-2721/2026.GU32420

recognition ability for minority class abnormal samples, thereby reducing the model parameters and computational cost while maintaining the detection accuracy. The experimental part was conducted based on public datasets such as CICIDS 2017 and UNSW-NB15. The results show that LKTADN outperforms traditional methods like support vector machines, decision trees, and random forests in multiple indicators including accuracy, F1 score, and specificity. Moreover, it demonstrates excellent robustness and network adaptability in simulation tests for different attack types (such as DDoS attacks, port scanning, and malware propagation). When the sample size is 5000, the training time of this model is 22.8 seconds, the inference time is 0.06 seconds, and the parameter quantity is only 1.9×10^4. This verifies its lightweight advantage and application potential in resource-constrained scenarios.

4. System architecture

4.1. Experimental Cyber Physical System (CPS) architecture projects

Pivoto et al. systematically reviewed the mainstream architecture models and technical characteristics of information-physical systems in the context of Industry 4.0 in 2021 [5]. The aforementioned study first elaborates on the core concepts of Industry 4.0 and Industrial Internet of Things, pointing out that CPS, as a key technology connecting the physical space and the virtual space, is the fundamental support for achieving intelligent manufacturing. The research conducts in-depth analysis around three representative CPS reference architectures: The 5C architecture focuses on data collection and processing, covering five levels including intelligent connection, data information conversion, networking, cognition, and configuration, and is applicable to embedded systems and small-scale industrial environments; Reference Architectural Model Industrie 4.0 (RAMI 4.0), as a three-dimensional architecture model oriented towards the entire manufacturing value chain, realizes asset virtualization and full-process integration through three dimensions: hierarchy, life cycle, and architecture layer, emphasizing standardized representation of management and assets; IIRA focuses on cross-industry interoperability, constructing the industrial Internet of Things system from four perspectives: business, usage, function, and implementation, highlighting the design of functional domains and cross-cutting functions. The paper further explores the functional mapping relationships and the implementation paths for interoperability among the aforementioned architectures, and systematically reviews the application mechanisms of core communication protocols and standards such as Open Platform Communications United Architecture (OPC UA), AutomationML, and Data Distribution Service (DDS) within the CPS architecture. It is worth noting that in the literature review, this summary incorporated the identity resolution architecture for IoT devices based on DNS proposed by Karakostas et al. This solution achieves the decoupling of identity and location by mapping the unique identifier of physical objects to a network address, providing name resolution support for modern mobile-friendly networks. The aforementioned study result has an inherent connection with the prevention of DNS hijacking in smart home scenarios: The essence of smart home DNS hijacking is the alteration of the mapping relationship between device identities and network locations by attackers. The ID/Locator separation mechanism advocated by Karakostas provides methodological inspiration for building an anti-hijacking smart home DNS resolution system - by deploying independent identity resolution services at the edge of the network, and decoupling the device identifier from its network location, it can effectively prevent attackers from hijacking and controlling the communication traffic of devices by modifying the router's DNS configuration. Therefore, the CPS architecture concepts and

DOI: 10.54254/2755-2721/2026.GU32420

the DNS identity resolution research covered in this review provide an important theoretical reference for the construction of the DNS hijacking defense system in the smart home environment.

4.2. ZT-BlocIoT

Salim et al. in 2023 proposed a ZT-BlocIoT framework based on the zero-trust principle, blockchain technology and deep reinforcement learning to address the scalability and security challenges faced by the Internet of Things environment [6]. This framework achieves continuous device authentication through a dynamic trust gateway and introduces a DRL-driven sharding mechanism to optimize the scalability of the blockchain. It can achieve a throughput of 2500 TPS and a low latency of 42 ms under 700 nodes conditions, and still maintain 85% throughput even when 20% of the nodes are malicious. The technical architecture of this study in aspects such as trust assessment, access control, and attack detection is intrinsically related to the research topic on DNS hijacking prevention in smart home systems. As an important application scenario of the Internet of Things, the core feature of DNS hijacking attacks in smart homes lies in the fact that the attacker achieves full network control by tampering with the DNS configuration of the router. Essentially, it is an abuse of trust in device identity and communication paths. The zero-trust architecture concept advocated by ZT-BlocIoT - namely, "never trust, always verify" - provides a methodological inspiration for DNS security protection in the smart home environment: By deploying a dynamic trust assessment mechanism at the network edge layer to conduct real-time behavior analysis and trust scoring for each DNS resolution request of every smart device, it can effectively identify domain name resolution anomalies caused by DNS hijacking; at the same time, the self-adaptive resource allocation idea embodied by the DRL-driven sharding optimization mechanism can also be applied to the dynamic scheduling of smart home DNS query traffic, preventing the paralysis of the resolution service caused by large-scale DNS flooding attacks. Therefore, the zero-trust and AI collaborative protection framework proposed by this research institute provides a technical reference for building an active DNS hijacking defense system in the context of smart home scenarios.

4.3. DBDNS system

Zheng Xu proposed and implemented a decentralized DNS system called DBDNS in 2019, aiming to address issues such as security, fairness in privacy, and delay in update and effectiveness caused by the centralized architecture of the current domain name system [7]. This research first designed a dedicated DNS blockchain called NameChain. Through customized block structure and transaction types, it achieved native support for domain name registration, update, cancellation, transfer, etc. At the consensus mechanism level, a two-stage connection strategy of Proof of Stake (POA) and Proof of Work (POW) was adopted to accumulate computing power in the early stage of system development and ultimately achieve true decentralization. At the same time, to enhance system stability, a block size algorithm based on dynamic adjustment of the transaction memory pool and a difficulty adjustment algorithm suitable for the POW consensus were proposed to resist blockchain DOS attacks and computing power fluctuations. At the system architecture level, DBDNS adopts a layered model. From bottom to top, it consists of the blockchain layer, the cache layer, the control layer, and the application interface layer. The cache layer, considering the divergent characteristics of node access in a decentralized environment, has designed the DLFU and DFIFO dual-queue cache update algorithms to enhance the efficiency of domain name resolution. In the deployment level, a scheme of light nodes and full nodes collaborating is proposed, enabling user nodes to participate in the system only by storing the block headers, significantly reducing resource

DOI: 10.54254/2755-2721/2026.GU32420

occupation. Experimental results show that this system occupies less than 100MB of disk space when storing millions of block headers. The DNS update takes effect within 60 seconds, the cache hit rate is 83%, and it can still maintain service availability even when half of the nodes are down. Zheng's research holds significant implications for the prevention of DNS hijacking in smart home scenarios: The essence of smart home DNS hijacking is the alteration of the mapping relationship between device identities and network locations by attackers. The decentralized domain name resolution system constructed by DBDNS stores domain name mapping data on an immutable blockchain and ensures data authenticity and integrity through cryptographic mechanisms. This approach fundamentally blocks the path through which attackers can hijack by modifying the DNS configuration of routers. Furthermore, the identity and location decoupling mechanism designed in the domain name transfer exchange of Name Chain, as well as the terminal resource adaptation concept embodied in the lightweight node deployment scheme, provide a technical path that can be referred to for building a DNS protection system in the smart home environment that is resistant to hijacking, lightweight, and allows users to independently verify.

5. Conclusion

This research focuses on the core issue of DNS hijacking prevention in smart home systems, and conducts a systematic review from the perspectives of attack mechanism, vulnerability analysis, defense technology evolution, and architecture design. This article first clarifies the principle of DNS spoofing attacks and their amplification effect in smart homes: The attacker uses the router as the hub to tamper with the DNS configuration, achieving batch control of all home devices, resulting in three major hazards: privacy leakage, network fraud, and botnets. Then, it analyzes the DNS security vulnerabilities in smart homes from four levels: terminals, network transmission, routing facilities, and upstream services, and points out that device heterogeneity, network openness, and loose configuration are the root causes of the risks. In the defense technology section, six representative studies are deeply analyzed: DNSwitch lightweight detection, LDoS traffic anomaly identification, LKTADN resource constrained detection, ID/Loc separation architecture enlightenment, ZT-BlocIoT zero-trust framework, and DBDNS blockchain evidence storage. The research shows that defense technologies are evolving from single-point encryption to system architecture, and from passive response to active trust assessment. In conclusion, the current defense technologies are showing a general trend of evolving from single-point encryption verification to systematic architecture protection, and from passive response to active trust assessment. However, current research still faces key challenges such as lightweight deployment, compatibility with heterogeneous devices, and cross-layer collaborative defense. Future research should focus on building a collaborative protection system that integrates zero-trust architecture, blockchain evidence storage, and edge intelligence in order to achieve active perception, real-time blocking, and trusted verification of DNS hijacking in the smart home environment.

References

[1] Zhiwei Yan & Jong-Hyouk Lee.(2020).The road to DNS privacy.Future Generation Computer Systems, 112(prepublish), 604-611. https: //doi.org/10.1016/j.future.2020.06.012.

[2] A.A. Maksutov, I. A. Cherepanov and M. S. Alekseev, "Detection and prevention of DNS spoofing attacks, " 2017 Siberian Symposium on Data Science and Engineering (SSDSE), Novosibirsk, Russia, 2017, pp. 84-87, doi: 10.1109/SSDSE.2017.8071970.

[3] Tang, D., Dai, R., Tang, L. et al. Low-rate DoS attack detection based on two-step cluster analysis and UTR analysis. Hum. Cent. Comput. Inf. Sci. 10, 6 (2020). https: //doi.org/10.1186/s13673-020-0210-9

DOI: 10.54254/2755-2721/2026.GU32420

[4] Yao, W., Lin, W. A lightweight anomaly detection model for network traffic using multi scale spatio temporal residual learning. Sci Rep 15, 20472 (2025). https: //doi.org/10.1038/s41598-025-05190-y

[5] Pivoto Diego G.S., de Almeida Luiz F.F., da Rosa Righi Rodrigo, Rodrigues Joel J.P.C., Lugli Alexandre Baratella & Alberti Antonio M.. (2021). Cyber-physical systems architectures for industrial internet of things applications in Industry 4.0: A literature review. Journal of Manufacturing Systems, 58(PA), 176-192. https: //doi.org/10.1016/J.JMSY.2020.11.017.

[6] Mikail Mohammed Salim, Minji Kim, Sushil Kumar Singh & Jong Hyuk Park. (2026). Zero-trust blockchain-enabled framework for scalable and secure IoT networks. Future Generation Computer Systems, 175, 108093-108093. https: //doi.org/10.1016/J.FUTURE.2025.108093.

[7] Xu Zheng. (2019). Research and Implementation of the Decentralized Blockchain-Based Domain Name System(A Dissertation Submitted for the Degree of Master, South China University of Technology). Master https: //doi.org/10.27151/d.cnki.ghnlu.2019.003663.