Data and service deployment strategy anticipating network disruption

2410132 NAKAMURA Kazuki

Information communication via the Internet has evolved into critical social infrastructure underpinning daily life and economic activities. Under such an environment, physical network partitioning caused by large-scale natural disasters signifies a complete separation from information sources. This results in significant disadvantages for users, such as delays in ensuring safety during emergencies and the inability to access vital evacuation instructions. The "Guidebook for Introducing Disaster-Resilient Information and Communication Networks 2024," published by the Ministry of Internal Affairs and Communications, explicitly points out that the loss of communication infrastructure hinders the initial transmission of crisis information, safety confirmation, and the collection of evacuation center data. A critical issue often overlooked in disaster countermeasures is the logical dependency of services. Even if data physically exists within a partitioned local network, acquiring such content becomes difficult due to "Hidden Dependency Services." These are protocols and their interrelations required for information communication that users are typically unaware of, such as the Domain Name System (DNS). When these underlying services become unreachable due to backbone fragmentation, the entire service layer fails, rendering local connectivity useless. This study defines this phenomenon as the "Hidden Dependency" problem and positions it as a core challenge for realizing true disaster resilience.

Various studies have proposed methods to secure communication during disasters. Mobile Ad-Hoc Networks (MANET) and Delay Tolerant Networks (DTN) have been widely discussed to secure communication paths without fixed infrastructure. Additionally, practical initiatives by three major mobile carriers in Japan (KDDI, Softbank, and NTT Docomo) include the rapid deployment of vehicle-mounted base stations and satellite communication services like Starlink. These efforts primarily focus on securing physical communication paths to improve accessibility. However, they do not sufficiently consider the impact of Hidden Dependency Services, often assuming that once connectivity is restored, services will function normally. Regarding Edge Computing, commercial services such as Cloudflare Workers and AWS Wavelength leverage edge locations to reduce network latency and improve efficiency under normal operating conditions. However, these architectures generally assume a healthy backbone network. Their behavior and autonomous operation during disasters, particularly when the connection to the core cloud is severed, have not been sufficiently examined. Consequently,

there is a lack of established strategies for maintaining service continuity in a completely isolated local environment.

This study proposes a disaster-resilient network architecture by utilizing Edge Computing and applying a novel data and service placement strategy. The primary objective is to construct a system immune to the influence of hidden dependency services, ensuring that essential services and data remain accessible within a local network even when physically isolated from the global Internet.

Hidden dependency services and associated challenges were analyzed by examining past large-scale communication failures and protocol stack behavior. Furthermore, dependencies were analyzed from the perspective of network topology. Consequently, three major challenges were defined: (1) Complexity of Communication Establishment via Protocol Stack: If protocols used for communication establishment, centering on DNS, stop functioning, content acquisition becomes impossible even if the server holding the content exists. (2) Congestion of Communication Bandwidth: Even if a communication path is established, traffic surges during disasters can cause severe congestion, compressing bandwidth and causing timeouts that make data acquisition impossible. (3) Centralized Topology: The current Internet arranges servers hierarchically. If upper-tier servers cannot be reached due to network partitioning, resolving domain names becomes impossible. To validate these analyses, a confirmation experiment simulated a network partition. Results confirmed that when separated from the backbone, communication to the global network fails, but local network communication is maintained. Therefore, service availability is significantly enhanced by placing content locally, provided logical dependencies are resolved locally.

In the proposed placement strategy, data required during disasters was classified into three types: Type A (Data necessary for immediate evacuation, sent from Municipality to General Public), Type B (Information shared between municipalities), and Type C (Safety confirmation among citizens). Priorities were defined for these data types across three disaster phases: Initial, Emergency, and Recovery. Services were classified into "Push-type" and "Pull-type." While Pull-type services are prioritized in normal times, Push-type services should take precedence immediately after a disaster to forcibly deliver critical alerts. Based on these classifications, four system requirements were defined: (R1) Autonomous Operation, the ability to function independently without external upstream systems; (R2) Physical Proximity, placing resources within the physical reach of users; (R3) Dynamic Resource Optimization, dynamically prioritizing essential traffic (Type A) and blocking non-essential traffic to conserve bandwidth; and (R4) Information Reliability, ensuring disseminated information is trustworthy.

To satisfy these requirements, this study proposes an autonomous decentralized architecture using an Edge Gateway. The core mechanism automatically switches between "Normal Mode" and "Disaster Mode." The Edge Gateway constantly monitors external network liveness. Upon detecting a disconnection from the backbone, the system autonomously transitions to Disaster Mode. In this mode, the gateway executes DNS Hijacking via Destination NAT. It intercepts all DNS lookup queries from client devices and forcibly forwards them to the local Edge Server. This mechanism allows the user's device to resolve domain names to the local server's IP address without manual configuration changes, such as setting static IP addresses or proxies. Consequently, users can acquire disaster information replicated in advance on the local server, transparently and immediately.

The effectiveness of the proposed method was evaluated through a Proof of Concept (PoC) implementation. The experimental environment used VyOS as the gateway router and Ubuntu as the edge server and client within a virtual environment. The experiment simulated a backbone network failure using Blackhole Routing. The monitoring script successfully detected the communication loss and triggered the transition to Disaster Mode. Client terminals, which lost access to external websites, were automatically redirected to the local edge server and successfully downloaded map data. This demonstrated that the architecture satisfies the requirement for autonomous operation and transparent user guidance.

Based on the findings, several future challenges have been identified. First, the evaluation revealed security challenges related to HTTPS and HSTS (HTTP Strict Transport Security). Since the proposed redirection mechanism behaves similarly to a Man-in-the-Middle approach, browsers with HSTS enabled block connections due to certificate mismatches. Addressing this requires utilizing Captive Portal functions to legitimately display disaster information pages or establishing a local trust model. Second, since the current evaluation was conducted in a virtual environment, implementing the system on power-saving hardware such as Raspberry Pi is necessary to ensure operation during power outages. Finally, performance verification in actual wireless LAN environments is required, considering potential radio interference and bandwidth saturation when a large number of evacuees connect simultaneously.

In conclusion, this research demonstrates that by strategically placing data and services at the edge and employing an autonomous switching mechanism, it is possible to build a disaster-resilient network that overcomes the vulnerabilities of hidden dependency services. This approach offers a practical solution for maintaining essential information flow during the critical initial phase of a disaster.