White Paper

FUJITSU

Trust-Enhanced Networking

Trust delivered by networks that connect cyberspace and the real world

(Overview) As the activities of companies and society shift to cyberspace along with the emergence of metaverse and Web3, it is necessary to introduce additional information that serves as evidence of the trustworthiness of activities in order to build relationships with various stakeholders in cyberspace. This paper presents the concept of "Trust-Enhanced Networking", which brings trust to cyberspace through the verification of physical attributes of the real-world assets, as a new paradigm in networking.

1. Introduction

Today, IT infrastructure is deeply reliant on networks, and various information has been digitized and distributed through the Internet. Moreover, due to the rapid spread of smartphones and the development of online services such as SNS (Social Network Service) and e-Commerce, people are constantly connected to the Internet. Going forward, along with the evolution of IoT (Internet of Things) and AI (Artificial Intelligence), the authors believe that the services leveraging these technologies will lead to a "cyber society" in which more daily activities and interactions between people would be conducted over the Internet.

In order to realize the safe and stable cyber society, the services and functions of the Internet are steadily evolving. In this context, the authors are focusing on two social changes with a high impact. (i) The first one is the shift from "on-premises" to "cloud", where companies and organizations store their data in remote data centers provided by cloud services. With the widespread of cloud services, much of companies and organizations data is distributed across multiple cloud service providers. Trustworthiness is a key requirement for selecting the right cloud service providers. (ii) The second change is related to the emergence of corporate and social activities in cyberspace also referred to as "metaverse". Within the next few years, more business and social activities is expected to move to the metaverse, along with electronic contracts, online conferences and meetings. This would bring even more businesses opportunities from the real world to cyberspace. Thus, many new businesses in cyberspace would be created by building new relationships with diverse stakeholders across the world regardless of the region or country.

On the other hand, it is also important to consider the changes in the world situation and the corresponding legal systems in relation to these changes. The importance of geo-aware data governance has increasingly grown from the perspective of data protection to economic security and GDPR (General Data Protection Regulation) that come to effect in 2018 in Europe. Corporates and organizations should address the real world-related concerns such as cross-border data transfer and geographical locations of partners in order to safely conduct their activities and business in cyberspace. Along with traditional trust policies, the authors believe that an established trust in cyberspace would be strongly required from the viewpoint of networks connecting cyber (digital) space and the physical (real) world.

As social responsibility, Fujitsu has been actively developing digital trust technologies, such as IDYX [1], CDL [2], and Transparent trust technology [3]. This white paper summarizes the role that future networks should play in order to bring trustworthiness into the cyber realm with the aim of addressing the challenges arisen from the foreseen social changes.

2. Trust in Cyber Society

2.1. Trust based on Physical Attributes

Digital trust mechanisms ensure that the data is authentic, has not been tampered with or placed in an unintended state (from the perspective of data owners and the valid users), and is used as intended. In the cyber society, we believe that the concept of digital trust, based on attributes from the physical world, will be important as an addition to the current security standards and technologies, such as access authentication and encryption. For example, when data is transmitted online across countries and regions, there is a possibility that the data does not fully comply with the regulations of its sender or recipient. Moreover, there is always a possibility that the person on the other side of the line, in an online communication for instance, may not be who or where they claim to be, and a malicious person might gain access to sensitive information that was sent to the person we are talking to.

In this context, "geographical attributes" of data and business partners throughout the cyberspace are considered to be very important for achieving trustworthiness in cyber society. In order to bring trust in

cyber society, it is necessary to consider the physical attributes of the real-world entities and the trustworthiness levels of the data centers that store data and the networks that transmit data. Thus, the question that we attempt to address in our line of research is: What kind of physical attributes from the real world do we need to strengthen trust in cyber society? One answer is "location information", which indicates the geographical position of each device in the network, such as servers, routers, and terminals. If we can reliably figure out the correct location of the device being used by a business partner in cyberspace, we have less chance of sharing sensitive data with a "malicious person" impersonating the business partner. Also, if we know where the device is located, we will be able to specify the network route that the user trusts for sending and receiving data.

The authors believe that it is essential to accurately understand and utilize the geographical location of networks, servers, and storage systems, which are distributed across multiple data centers, as a means of strengthening trust that supports the complex and evolving cyber society.

2.2. Challenges in Networking

As for location in networks, GPS (Global Positioning System) and base stations to which a mobile device is connected are now widely used for applications such as mappings and weather forecasting. Information about the physical location of network devices, such as routers, is also used for network management and control, and for route optimization. Database services called IP Geolocation are widely used for these purposes, where a database links pairs of IP addresses and information about their estimated location.

However, information about the estimated location might not be reliable. For example, there is always a possibility for the location information obtained through IP Geolocation services to be tampered with or changed depending on network providers, or whether remote connection services such as VPN (Virtual Private Network) are used to obfuscate the actual position. Even with the use of GPS for a higher accuracy, there are tools that can spoof the location information of mobile devices. For all these reasons, the authors consider that it is difficult to reliably use existing location information as “evidence of trustworthiness” in cyberspace.

How about the communication route? In the current mainstream networks, it is difficult for users to control or even reliably check the route through which the data they sent is expected to travel. In addition, if the wrong communication route is advertised on the Internet by malicious attackers or misconfigurations, data may not pass through the most appropriate route. With the goal of bringing trust in cyber society, it is of the most importance to solve the above issues by collecting and providing reliable information on the safety and trustworthiness of communication routes to the network users.

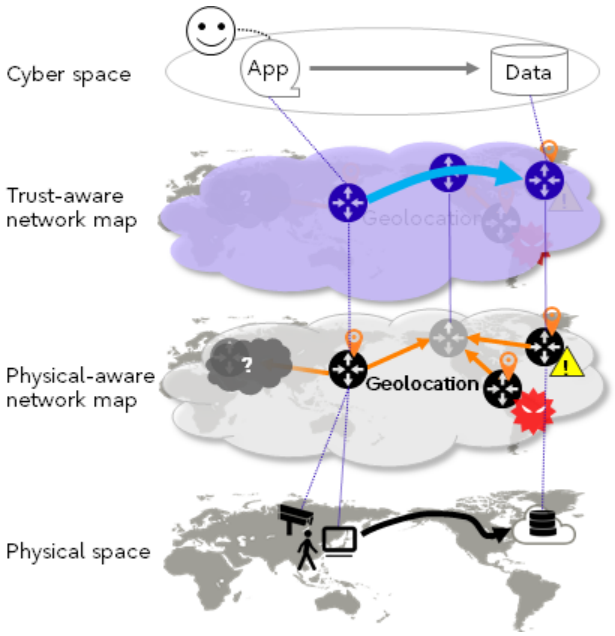

Figure 1 Concept of Trust-Enhanced Networking

3. Trust-Enhanced Networking

The authors propose the concept of “Trust-Enhanced Networking” as a new dimension for networks in order to bring trust to the cyber society of the future. Recent advances in networking technologies made network equipment invisible from cyberspace by introducing network virtualization technologies such as SDN (Software Defined Networking) and NFV (Network Functions Virtualization), which enable flexible and efficient network management and control. On the other hand, our "Trust-Enhanced Networking" concept focuses on using geographical information about network entities for providing reliable information in cyberspace, and making the overall network trustable for users. For example, it is assumed that location information of end devices, such as mobile terminals, and network devices, such as routers, and storage devices, will be incorporated into cyberspace in a way that can be verified. As such a new trustable route control would be eventually conducted using the verified geographical locations.

For this purpose, “Trust-Enhanced Networking” performs step-by-step mapping from physical space to cyberspace, as shown in Figure 1. In the first layer, the "Physical-aware network map" attempts to verify the geographical location of end devices, network devices, and the links. Taking into account the requests form the user in cyberspace, the second layer, representing the “Trust-aware network map”, focuses on providing network control functions based on verifiable inputs originating from the previous "Physical-aware network map". One of the most relevant inputs that can be used is geographical location. The detail of each map is described in the following subsections.

3.1 Network Location Verification

"Physical-aware network map" is created in order to utilize networks for assessing the trustworthiness of objects or data in cyberspace. In this map, geographical location and device authenticity are closely assessed and used in evaluating the trustworthiness of the physical entities in the network. For this purpose, it is required to verify the location information of end devices and network devices such as routers.

Currently, however, it is not possible to verify the location of every device. In some cases, it is possible to verify the geographical location from reliable sources such as network providers, and in other cases, it is only possible to provide an estimation for a narrow down possible location. Furthermore, in other cases we cannot get any clues to infer the location of devices or even reliably verify the location of devices especially if they were exposed to malicious attack. In this way, there is a low degree of confidence in geographical location of network devices. "Trust-Enhanced Networking" includes developing technology that will expand the range of possible location verification targets and increase the accuracy of such location verification.

3.2. Trust Measurement and Networking

In the context of measuring trust, the authors introduce Quality of Trust (QoT) as an important evaluation measurement for the effective implementation of trustworthy networking and services. Envisioned as the next level for network performance measurements, we describe QoT as a logical continuation to Quality-of-Service (QoS) and Quality-of-Experience (QoE), with a strong emphasis on trusted networks and communications. Such measure would provide valuable, reliable, and trustworthy information about the level of trust for a given entity or service in the network. As such, QoT can provide for links, network and the storage devices a quantitative degree to which the user is likely to trust them. A Trust-oriented "Trust-aware network map" can be derived by computing the QoT using information from the "Physical-aware network map" and subjective requirements for trusting networking from users in cyberspace. This metric can vary depending on the subjective view of each user or service. Based on the "Trust-aware network map", services such as route selection can be executed where data only passes through trustable network devices or region for users.

4. Summary

Digital trust will become increasingly important in corporate and social activities in the future cyber society. Current networks carry data in physical space, however in the future, the authors believe that networks will play an important role of providing physical attributes from the real world and strengthening trust in response to the conditions and demands of cyberspace. In order to prepare the network for playing this key role, it is deemed necessary to introduce a new concept for network trust as shown in section 3. In addition, to further strengthening trust in cyberspace, it is also important to align our efforts with trust infrastructures and technologies such as the Trustable Internet [4], which can verify the authenticity of data by managing and providing additional information such as verification of data in cyberspace. In order to carry out these activities, the authors are promoting and actively engaging in the development of digital trust technology, which will be necessary for the future society, in cooperation with partners from different companies, universities and standardization bodies.

References

[1] IDYX: IDentitY eXchange. Fujitsu's technology that securely distributes personal identities (such as IDs and attribute information) among companies and individuals.
https://www.fujitsu.com/global/about/resources/news/press-releases/2019/0704-01.html

[2] CDL: Chain Data Lineage. Fujitsu's technology that can trace the distribution process and processing of data and goods back to their origin. Ensures end-to-end traceability of data and goods across organizations and improve the reliability of data distribution across industries.
https://www.fujitsu.com/global/about/resources/news/press-releases/2018/0920-02.html

[3] Transparent trust technology: Technology to prevent falsification in the creation and approval of business data exchanged between companies and government ministries, and to ensure its authenticity.
https://www.fujitsu.com/global/about/resources/news/press-releases/2020/1006-01.html

[4] Trustable Internet: A technology concept that makes it easy to verify the reliability of data on the Internet in a general-purpose manner.
https://www.fujitsu.com/global/about/resources/news/press-releases/2022/1013-01.html

For further information, please contact:
contact-nwt@cs.jp.fujitsu.com
Data&Security Laboratory
Fujitsu Limited