Position Paper on Thing Name Service (TNS) for the Internet of Things (IoT)

Ning Kong, Shuo Shen
China Internet Network Information Center
nkong@cnnic.cn, shenshuo@cnnic.cn

Introduction

The name service of Internet such as DNS (Domain Name System) [RFC1034] has already been one of the most important infrastructures of the Internet nowadays. For example, DNS is an indispensable system of the Internet used for translating the "human-friendly" host names of computers on a TCP/IP network into their corresponding "machine-friendly" IP addresses. In general, DNS also stores other types of information, such as the list of mail servers that accept email for a given Internet domain. By providing a worldwide, distributed name service, DNS is an essential component of the functionality of the Internet.

Similarly, the name service of the IoT will also be one of essential and key elements in the IoT, which can be used for translating the "thing-friendly" names of things which maybe belong to heterogeneous namespaces (e.g. EPC, uCode, and any other self-defined code) on different networks (e.g. TCP/IP network, constrained network) into their corresponding "machine-friendly" addresses or other related information of another TCP/IP or constrained network. We name this kind of name service as Thing Name Service (TNS). By TNS, the thing of the IoT based on a TCP/IP or constrained network can easily communicate with other thing on the same or any other network by its name, without considering whether the address of the targeted thing has been changed or not.

To fulfill the aforementioned objective, TNS based on the IoT needs to be researched. The efficiency for the constrained network, the compatibility of heterogeneous name spaces and the privacy protection of this kind of service are supposed to be the most important issues to be studied in future.

Efficiency Issues

The IoT would encode trillions of things, and be able to follow the movement of those things. Because most of things maybe frequently move around the world, the relationship between names with addresses of these things should be accordingly changed. The information stored by TNS has to be frequently updated, and the QPS (Queries Per Second) of TNS will far exceed that of DNS. It is a big challenge for TNS to provide efficient name service for trillions of things of the IoT, especially within constrained networks.

One good choice of TNS based on the IoT is suspended on existing long-tested system or techniques. We have already analyzed and developed some steady resolution system, such as DNS. Any other mechanisms for improve the efficiency of TNS, such as DDNS (Dynamic DNS) [RFC 2136], need to be further studied. Especially, we need to pay more attention to study related mechanisms concerning constrained network. If

necessary, we should develop some new mechanism to improve the performance of TNS within constrained networks.

Compatibility Issues

There are multiple code standards for things related with the IoT such as EPC (Electronic Product Code) and uCode (ubiquitous Code). In the future, there may be more code standards for things, for example some self-designed code standards by different industries or countries. So these heterogeneous code standards can cause the conflict problem of the name service for the IoT. TNS should support all different code standards for things in the IoT, although DNS only needs to support one code standard named as domain name.

Our idea about compatibility of TNS is to design multiple ID resolution service architecture and resolution protocol. Currently, we have already partially developed a test system of TNS based on Dynamic Delegation Discovery System (DDDS) [RFC 3401, RFC 3402, RFC 3403, RFC 3404, and RFC 3405] which can provide name service for EPC, uCode and any other self-defined codes. For more information, please refer to the Appendix "A Model Supporting Any Product Code Standard for the Resource Addressing in the Internet of Things".

Privacy Issues

The privacy protection of the IoT has caused wide public concern. This kind of problem also exists in the name service for the IoT, since the information of relationship between names with addresses of things in TNS may leak the privacy of clients. It is important to protect the privacy of information provided by TNS that it is not divulged to malicious parties. By now, DNS doesn't contain any mechanism of privacy protection, so it's necessary to design TNS by any other mechanism except DNS.

Firstly we need to make sure the problem statement of privacy protection of TNS. Then we should analyze exist privacy protection approaches for TNS of the IoT. Fox example, Handle system [RFC 3650, RFC 3651, and RFC 3652] is better than DNS in regard to privacy protection. But the scalability of Handle system is not as good as DNS. It is possible that we need to modify some existing protocols of Internet or design some new protocols to realize the function of privacy protection for TNS. This kind of issues needs to be further studied.

Conclusion

In our opinion, TNS will be one of essential and key elements in the IoT, just like DNS in the Internet. Because of trillions of connected things or constrained devices, IoT has different characteristics against Internet. So there are more challenges of TNS than those of DNS. We divided new challenges of TNS into three categories: efficiency, compatibility and privacy. It is not feasible that reusing DNS protocols to realize TNS because of these new challenges, especially privacy issues.

Efficiency, compatibility and privacy issues of TNS need to be further researched. Some problems related to efficiency and compatibility of TNS should be considered by IETF CoRE working group in future. We suggest other problems in terms of privacy of TNS should be considered by IRTF as long term research items.