International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Towards an Intelligent Internet: Surveying the Influence of Cognitive Technologies on Network Architecture and Performance

D.Banupriya[1], K. Prathapchandran[2], S. Sweetlin Devamanohari[3]

[1,3]Research Scholar, Department of Computer Applications, Nehru Arts and Science College, Coimbatore, Tamilnadu 641105, India.
[2]Assistant Professor (SG), Department of Computer Applications, Nehru Arts and Science College Coimbatore, Tamilnadu 641105, India

Abstract:
Internet of Things (IoT) is a heterogeneous, mixed and uncertain ubiquitous network, the application prospect of which is extensive in the field of modern intelligent service. Having done a deep investigation on the discrepancies between service offering and application requirement, we believed that current IoT lacks enough intelligence and cannot achieve the expected increasing applications performance. By integrating intelligent thought into IoT, I presented a new concept of **Cognitive Internet of Things** (CIoT) in this paper. CIoT can apperceive current network conditions, analyze the perceived knowledge, make intelligent decisions, and perform adaptive actions, which aim to maximize network performance. We model the topology of the CIoT network, develop technologies related to the cognitive process, and analyze the results of cooperative intelligence based on game theory. This shows that these new designs can bring intelligence to IoT and significantly improve system performance. Finally, application cases based on the CIoT concept were presented.

Keywords: Cognitive Internet of Things, Cognition; Cross layer, Multi-domain; Cooperation, Network.

Introduction

The Internet of Things (IoT) is proverbially applied in the field of modern intelligent service, such as ecological protection, energy conservation & emission reduction, food security, etc. In order to catch up with the pace of application, researches related to IoT were widely concerned by academe, especially in network architecture, service offering and intelligent features. In the field of architecture, Social Network architectures were paid close attention to by researchers. Several distinctive architectures were achieved[1], some of which could satisfy the need of heterogeneous terminals, generous identifications, network interconnection and object position, and obtain the high robustness and stability simultaneously. Oriented to the special application environment, the diverse network architectures and corresponding protocols were proposed to provide ubiquitous services and access modes, as well as to achieve flexibility and scalability [2]. By analyzing the defects of TCP/IP protocols, a hierarchical architecture was obtained to meet specific circumstances [3]. Those achievements established the basic network architecture for IoT, though the corresponding international standard was still not constituted. With the development of other researches, the functional aspects and functions of IoT became clear. After a

thorough examination of the mismatch between service delivery and demand requirements, it was determined that education could not meet demand requirements. Therefore, we proposed the concept of CIoT (Cognitive Internet of Things) combining artificial intelligence and IoT. CIoT is the Internet of Things (IoT) and the methods of integration and collaboration to drive action and achieve knowledge[4]. CIoT can apperceive current network conditions, analyze the perceived knowledge, make intelligent decisions, and perform adaptive actions, which aim to maximize network performance[5]. In the cognitive process, the multi-domain cooperation can increase network capacity and the machine learning can enhance the intelligence for future. In recent years, cognition and cooperation have become popular research focuses. Since Doctor Mitola presented the concept of cognitive radio [6], cognitive radio network [7] and cognitive network. Researchers have paid much attention and many achievements have been made, greatly promoting the development of network intelligence. In those researches, the cooperative thought was often adopted to address intelligence and performance for asynchronous network [10], multi-user network [1], multi agent network [4], autonomous multi-hop networks[5], bio inspired network[6], autonomic computing system[7-8] and other networks[9]. Besides, cross-layer design [2] and game theory[2] were introduced to improve efficiency and optimize performance. Those literatures accelerated the development of network intelligence. However, few researchers oriented to the intelligence of IoT. This paper focuses on the modeling and design of cognitive process for CIoT to find a new research idea. Our work will have far broader application prospect and great scientific significance.

Basic Concepts

Autonomous Domain (AD): it is an access network domain with autonomy and one of the following features.

- A high coupled and relative independent domain;
- A domain with distinct geographical feature;
- A network for organization, company, enterprise, etc;
- Specially, autonomic devices in core network.

If necessary, an AD can be divided into several Sub-ADs.For example, we can think of the campus network as anAD. Thus, the networks of institutes and departments can be thought of as Sub-ADs.

Cognitive Node: It also called **Cognitive Element (CE)**, refers a node which has the ability to autonomously

optimize network performance according to current conditions.

Simple Node (SN): It refers to a node without intelligence, which is relative to the cognitive node.

There are different numbers of CEs in different ADs, maybe only one under the special circumstances. If there

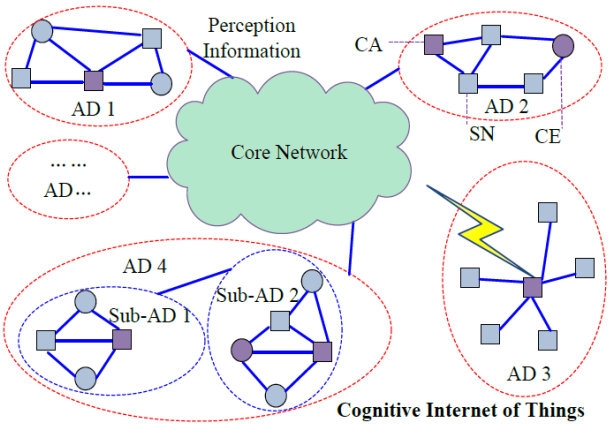
are multi CEs in an AD, two or more CEs can cooperate according to requirements.

Multi-domain Cooperation (MDC): for an application oriented to far broader network environment, the cooperative process of two or more ADs is called MDC.

Cognitive Agent (CA): for a MDC, it refers the specific CEs selected from each domain to carry out cooperative assignments. There is different number of CAs in different domains, maybe only one.

Neighbor: Two ADs with directly cooperative relationship are reciprocally called neighbors, and two ADs with cooperative relationship in virtue of other ADs are reciprocally called extended neighbors. In

CIoT, without artificial interventions, ADs divided, CAs selected and multi-domain cooperated are implemented autonomously.



Topology for CIoT

Design of Cognitive Process

The cognition is the foundation to achieve intelligence of CIoT. Based on this, I proposed a three-dimensional network diagram (TNA), a three-layer cognitive ring (TCR), and a collaborative method. The TNA provides the basic network framework, and TCR and cooperative mechanism addresses the cognitive process.

Three-dimensional Network Architecture

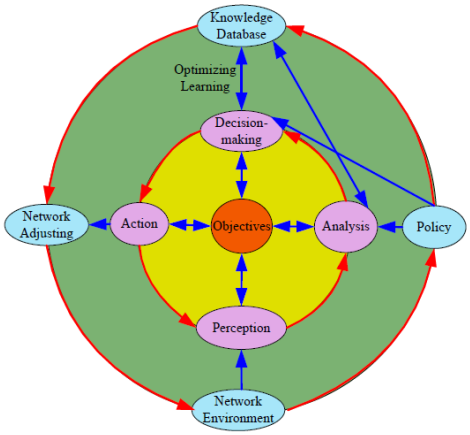
Network architecture is the foundation of a network. Since there is still no global standard, international experts are applying TNA for CIoT by introducing intelligent concepts in the IoT based on the currently known IoT architecture. It is made up of three planes, Protocol Plane (PP), Cognitive Plane (CP) and Adjusting Plane (AP),Referring to the traditional ISO/OSI architecture, PP consists of four layers: information layer (IPL), network link layer (NIL), information integration layer (IFL) and intelligence services layer (ISL). CP understands the current state of the network and performs analysis and decision making to derive strategies to improve CIoT performance. AP implements coordination activities based on the strategy developed by CP. Our research focuses on CP in this paper.

Three-layer Cognitive Rings

The functions of autonomic cognition and intelligent service are newly increased after integrating intelligent thought into IoT. The intelligent cognition is about the internal running level, and the intelligent service is about the external behavior level. Aiming at the internal running level, we propose TCR based on the OODA (Observe-Orient-Decide-Act) cognitive ring in the field of cognitive radio network[10].

Firstly, the TCR perceive a great deal of heterogeneous network conditions information. Secondly, the conditions information is analyzed and fused utilizing data fusion theory. Thirdly, the decision-making is performed based on the results of data fusion to achieve strategies of network behaviors, and machine learning theory is adopted to optimize future decision-making. Finally, network adjusting is executed

according to strategies generated by decision-making. The four process run cooperatively to achieve the network performance objectives referring to policies, laws, and other prescripts etc.



Three – layer cognitive rings for CIoT

IoT Security and Privacy Challenges

IoT has brought great benefits to users. However, it having some challenges. Internet security and risk is a major concern for security researchers and practitioners. Both are very difficult for many business organizations and public institutions. Cyber security attacks have exposed the vulnerabilities of IoT technology. This vulnerability is because the interconnection of networks in the Internet of Things brings access from an anonymous and unreliable Internet that requires new security solutions. For all known reasons, none related to IoT adaptation, Safe and secure. However, it is unfortunate that users often do not realize the security implications until it is breached, causing significant damage, including the loss of sensitive data. Consumer demand for poor security is declining due to security breaches that compromise user privacy. IoT at the consumer level has not fared well in recent privacy and security reviews. Modern automotive systems have many vulnerabilities.

Security:

Because the IoT is different from traditional software and hardware, it is more vulnerable to security issues in several ways. There are many IoT devices designed for mass deployment. A good example of this is sensors. Basically, IoT deployments are a set of similar or nearly identical devices that have similar characteristics. These practices increase the scale of security vulnerabilities that can have a negative impact on security. Similarly, many organizations have established guidelines for conducting risk assessments. This step means an unprecedented number of interconnections between IoT devices. It is also clear that many of these devices can establish connections and communicate with other devices in non-standard ways. Consider the tools, methods and techniques related to IoT security. While security issues are not new to the information and technology industry, IoT implementations have presented unique challenges that must be addressed[7]. Consumers must rely on their IoT devices and services to be fully protected against failure, especially as this technology becomes more and more integrated into our daily lives. The use of insecure IoT devices and services, which is one of the main tools used by cyber attacks, can expose users' data without adequately protecting their data flows.

Privacy

The perspective of the usefulness of the IoT is dependent on how well it can respect the privacy choices of people. Concerns regarding the privacy and the potential harms that come along with IoT might be significant in holding back the full adoption of IoT. It is essential to know that the rights of privacy and user privacy respect are fundamental in ensuring users' confidence and self-assurance in the Internet of Things, the connected device, and related services offered. A lot of work is being undertaken to ensure that IoT is redefining the privacy issues such things as the increase of surveillance and tracking. The reason for the privacy concerns is because of the omnipresent intelligence integrated artifacts where the sampling process and the information distribution in the IoT may be done nearly in any place. The ubiquitous connectivity via the Internet access is also an essential factor that helps in understanding this problem because unless there is a unique mechanism put in place, then it will be decidedly more comfortable to access the personal information from any corner of the world.[9]

Interoperability

The fragmented landscape of IoT technology implementations is known to hinder user value. This is not possible for all products and services, but users may not want to purchase products and services without flexibility and worry about customer lock-in.

Occasional update: Typically, IoT manufacturers update security patches every three months. Operating system versions and security patches have also been updated. This gives attackers plenty of time to hack security protocols and steal sensitive data.

Embedded passwords: IoT devices store installed passwords to help technicians troubleshoot operating system issues or remotely install required updates. However, attackers can use this feature to gain access to device security.

Occasional update: Typically, IoT manufacturers update security patches every three months. Operating system versions and security patches are regularly improved. This gives attackers plenty of time to hack security protocols and steal sensitive data.

Automation: Businesses and end users often use the automated nature of IoT systems to collect data or streamline business processes. However, if you don't identify a malicious site, the built-in AI can access that source and can introduce threats into your system.

Remote access: IoT devices use various network protocols for remote access, such as Wi-Fi, ZigBee, and Z-Wave. In general, there is no mention of specific restrictions that can be used to prevent online activity. Therefore, attackers can establish malicious connections through these remote access protocols.

Wide variety of third-party applications: There are many software applications available on the Internet that allow organizations to perform specific tasks. However, it was not easy to determine the truth of these claims. When end users and employees install or access these applications, threat actors automatically enter the system and compromise the installed database.

Improper device authentication: Most IoT applications do not use authentication services to limit network threats. As a result, the intruder breaks down the door and threatens privacy.

Remote access: IoT devices use various network protocols for remote access, such as Wi-Fi, ZigBee, and Z-Wave. In general, there is no mention of specific restrictions that can be used to prevent online activity. Therefore, attackers can establish malicious connections through these remote access protocols.

Wide variety of third-party applications: There are many software applications available on the Internet that allow organizations to perform specific tasks. However, it was not easy to determine the

truth of these claims.

Improper device authentication: Most IoT applications do not use authentication services to restrict or limit network threats. In this case, attackers enter the door and threaten privacy.

Weak Device monitoring: Typically, all IoT manufacturers configure specific device identifiers to monitor and track their devices. However, some manufacturers do not maintain security policies. Therefore, tracking online activities is very difficult.

Conclusions

In this paper, I present the CIoT concept to solve the problem of lack of knowledge, model the CIoT network topology, and design technologies related to cognitive processes. Our cognitive process is a collaborative process based on proposed TCR and TNA. Computing operations are autonomous and cooperative processes that are triggered when a node is unable to perform its cognitive function. We analyze the results of regional cooperation based on game theory. This shows that these new designs can bring intelligence to IoT and significantly improve system performance.

References

1. H. Ning and Z. Wang, “Future Internet of Things Architecture: Like Mankind Neural System or Social Organization Framework,” IEEE Communications Letters, Vol. 15, No. 4, 2011, pp. 461-463.
2. L. Atzori, A. Iera and G. Morabito, “SIoT: Giving a Social Structure to the Internet of Things,” IEEE Communications Letters,Vol. 15, No. 11, 2011, pp. 1193-1195.
3. X. Li, R. Lu and X. Shen, “Smart Community: An Internet of Things Application,” IEEE Communications Magazine, Vol. 49, No. 11, 2011, pp. 68-75.
4. A. Castellani, N.Bui and P. Casari, “Architecture and protocols for the Internet of Things: A case study,” the Proc. of IEEE PERCOM, Mannheim, Germany, 2010.
5. S. Hong, D. Kim and M. Ha, “SNAIL: an IP-Based Wireless Sensor Network Approach to the Internet of Things,” IEEE Wireless Communications, Vol. 17, No. 6, 2010, pp. 34-42.
6. J. Mitola III and G. Q. Maguire, Jr, “Cognitive Radio: Making Software Radios More Personal,” IEEE Personal Communications,Vol. 6, No. 4, 1999, pp. 13-18.
7. R. Urgaonkar and M.J.Neely, “Opportunistic Scheduling with Reliability Guarantees in Cognitive Radio Networks,” the Proc. Of IEEE INFOCOM, Phoenix, AZ, 2008.
8. E. Dall'Anese, S. Kim and G.B. Giannakis, “Power Allocation for Cognitive Radio Networks under Channel Uncertainty,” the Proc. of IEEE ICC, Kyoto, Japan, 2011.
9. R. W. Thomas, D. H. Friend and L. A. DaSilva, “Cognitive Networks: Adaptation and Learning to Achieve End-to-End Performance Objectives,” IEEE Communications Magazine, Vol, 44, No. 12, 2006, pp. 51-57.
10. C. Fortuna and M. Mohorcic, “Trends in the development of communication networks Cognitive networks,” Computer Networks, Vol. 53, No. 9, 2009, pp. 1354-1376.