CHALLENGES FACED BY THE AUTONOMOUS MANAGEMENT IN FUTURE INTERNET

ПРЕДИЗВИКАТЕЛСТВА ПРЕД АВТОНОМНИЯ МЕНИДЖМЪНТ В ИНТЕРНЕТ НА БЪДЕЩЕТО

Anastas Nikolov Nikolov
Faculty of Telecommunications, Technical University of Sofia, 8 Kl. Ohridski Blvd, 1000, Sofia, Bulgaria, phone: +359 886 891 333, e-mail: nikolov.anastas@gmail.com

Анастас Николов Николов
Факултет по телекомуникации, Технически Университет – София, бул."Кл. Охридски" 8, 1000, София, България, телефонен номер: +359 886 891 333, електронна поща: nikolov.anastas@gmail.com

Keywords: Future Internet, Autonomous management, Self-management

Резюме: *Интернет се превръща във все по–голяма инфраструктура, която крепи социалния и икономическия живот на планетата. Този факт неимоверно води със себе си и нуждата към развитие на настоящите мрежи или създаването на нови такива, които да посрещнат изискванията на потребителите и различните по вид устройства. Интернет на бъдещето е мрежова архитектура, която е насочена към осъществяването на тази идея, осигурявайки възможности за по–гъвкави и по-адаптивни мрежи. Настоящата публикация разглежда потребността от вграждане на автономност в бъдещите мрежи. Анализирани са три случая, а именно - нуждата от самоконфигуриране на услуги, от самоконфигуриране на устройства и от откриване, отстраняване на неизправности и смущения. Имплементирането на подобен тип елементи би спестило време и разходи, като същевременно би подобрило качеството на предлаганите услуги.*

Abstract: *Internet becomes more and more scalable infrastructure that steadies the social and economic life on the earth. This circumstance leads the need to develop new networks or to expand the old ones in way to meet user and device requirements. Future Internet is a network architecture which aims to realize a concept like this one, networks to be more flexible and adaptive. Current publication studies the need for implementation of autonomy in future networks. There are discussed three use cases–the necessity of self-configuration of services, of self-configuration of devices and of way to locate, to inspect and to resolve faults or intrusions. The establishment of similar properties saves much time and costs while improves the quality of the provided services.*

1. INTRODUCTION

Nowadays Internet is such a critical infrastructure that changes our way of life, work, production and consumption. Contemporary Internet faces some challenges: exhausted address space of widely adopted IPv4; lack of immanent mobile-oriented network architecture; predominant number of solutions that provide neither quality of

service management nor security functions; growth of energy consumption caused by its size increase and usage; slow and expensive applications development.

There are new technological opportunities that might be used to cope with the above mentioned limitation: wideband optical transport; advanced mobile and wireless technologies; huge capacity to store data effectively; innovations in industrial technologies especially regarding sensor, processors, memories and power supply.

The growing social role of Internet leads to more requirements to the network: ubiquitous connectivity, at any time, of everything; access to 3D content and intuitive user interface; data and knowledge engineering that are extensible and adapted to the needs; plenty of intelligent and secured applications that address users' demands.

2. THE CONCEPT OF AUTONOMOUS NETWORK MANAGEMENT

The challenges facing today's Internet, the potential requirements and the technical capabilities define critical directions for scientific research and concept reconstruction about the Internet as we know it into vision about Future Internet.

The Future Internet is envisioned as idea about fast and flexible networks, meeting the requirements of both users and machines. It is about content accessibility, applications and services that take into account both the context and user location. The evolution of Future Internet is Internet of services, things and infrastructure. During the evolution toward Future Internet the architectures of underlying networks extend the amount of necessary equipment, but at the same time it causes operational costs reduction. That assumes the necessity to embed autonomic functions as in the network equipment, so in the systems involved into the configuration operation. The future network infrastructure incorporates more autonomous features in order to keep low operational costs while deploying in large scale. This implicitly means features like self-configuration, self-healing, self-optimization and self-protection.

The autonomic computing is a concept that is influenced by biological systems and it aims development of systems capable of self management when coping with the complexity problem. The evolution toward autonomic computing includes five levels: basic, controllable, predictable, adaptive and autonomic. For automating of management tasks, reducing the response delay and management costs it is possible to use approaches like software agents, proactive networks and policy-based systems. The solution for communications complexity problem is mechanisms that allow the systems to manage the communications. The autonomic management is purposed to cope with the increasing complexity of computing systems management and to allow a possible dynamic expansion.

Self-configuration is the capability of the system to (re)-configure with respect of predetermined high-level policies and seamlessly to adapt to the changes caused by the reconfiguration. Self-optimization is the capability of the system to monitor and to manage its resources in order to improve its performance and effectiveness. Self-healing is the capability of the system to discover problems through fault-detection, diagnosis and triggering appropriate actions to prevent disruptions. Self-protection is

the capability of the system proactively to identify and protect from malicious actions or overlapping faults that self-healing can't cope with. An autonomic system implements the respective features in either reactive or proactive manner of behavior. A reactive autonomic system tries to detect faults or significant events and after that looks for appropriate action or solution. A proactive autonomic system uses preventive measures in order to sustain, improve or optimize its performance. The measures are based on analysis of current state, past and expected events, and predicted system reactions.

The deregulated markets, the open competition, the variety of digital services, the convergence of services, the convergence of communications and information technologies (e.g. virtualization/clouds) lead to new business and technological challenges. This is the reason why networks and network management must become intelligent, open, secured and autonomic i.e. to function with minimal human intervention.

3. STATE-OF-ART IN AUTONOMOUS NETWORK MANAGEMENT

The introduction of autonomy into the networks is related to the so called knowledge (wisdom) which is on top of the pyramid data-information-knowledge. The research related to autonomic management in Internet of Thing (IoT) is still at initial phase but the scientific community has realized the importance and necessity of the reduction to a minimal human intervention. The autonomic features introduction into the IoT systems for dynamic management of resource constrained devices is an effective solution considering the exponentially increasing number of connected devices. At the same time the autonomic computing allows innovative use of different security schemes.

The autonomic features are applicable to different functions, management and energy efficiency in IoT systems [1]. In [2], it is presented a state-of-art review of Machine-to-Machine (M2M) type cognitive communications from protocol stack viewpoint. The authors discuss the emerging standards and latest developments of protocols in cognitive M2M networks. Additionally, a centralized cognitive protocol for access control and a cognitive routing protocol for M2M networks are presented. An autonomic IoT architecture and communication protocol of services are proposed in [3] and both are based on the autonomic framework of IBM. When designing dynamic techniques, architectures and frameworks for future IoT the autonomous security should be considered as a priority. In [4] the authors examined and analyzed specific approaches, in relation to the autonomous security, that require minimal human intervention in IoT and thus can reduce threats. The main advantages of using an autonomous protection management in IoT are presented in [5]. In [6] the author proposes an approach based on the semi-automatic, policy-based agent for collection of personal data, which can take decisions. The agent includes algorithm for context-binding and modeling of behavior that keeps personal data under control of the user.

In addition to increased security, autonomous behavior can be used for self-healing. An extension of Open Mobile Alliance’s Lightweight M2M protocol for device management with autonomous capabilities is proposed in [7]. In [8], it is

studied the autonomous behavior of fault management of IoT services. The authors propose a scheme for fault management of self-organizing software platform on top of which IoT services are deployed, and IoT devices are connected to. A mechanism for autonomic management of services and devices which depends on the system context and locations of devices is presented in [9]. The developed mechanism is part of middleware for distributed and autonomic M2M systems and it is aimed at device authentication, device status monitoring, device management, and services reconfiguration. An autonomous system is presented in [10] that can train itself from personalized service requirements by drawing conclusion of the service usage in specific environments such as different location, temperature, time, etc., and emotional information from the user. The autonomous agents are software entities that perform multiple operations for a user or another program with a degree of independence or autonomy, using the knowledge or representation of consumer goals and desires. The autonomous agents are used within smart energy grids, processing big data and intelligent transport systems [11], [12], [13], [14].

4. ENABLING MECHANISMS

Figure 1 illustrates an abstract model of autonomous network system defined by European Telecommunications Standard Institute (ETSI). ETSI applies the classical architectural principles of autonomic computing at protocol level, network element level, and at network level. These principles identify managed entity (entities) and autonomous control element that takes decisions. The autonomous control element is a functional entity that drives the control loop tuning and adapting the behavior of managed resources by processing sensory information from managed resources and other types of information sources and by responding to the observed conditions by treating the behavior of managed resources in achieving particular goal. It is regarded as a Decision Element.

The managed entity is a protocol or mechanism implemented by a particular functional entity that performs a specific task and can be managed by autonomous control element. The autonomous control element and the managed entity form the core of an autonomous system with cognitive abilities whose behavior is reactive or proactive based on external stimuli and objectives to be achieved, principles of work, opportunities, experience and knowledge. In the case of telecommunication network, the autonomous system with cognitive abilities have capabilities for dynamic choice of network configuration through self functionality that reaches optimal solutions, taking into account the operational context (the requirements and characteristics of the environment) objectives and policies (consistent with the operational principles), profiles (corresponding to the abilities) and machine learning (for management and usage of knowledge and experience).

In order to design the control loop and abstract levels the following methods and techniques are used.

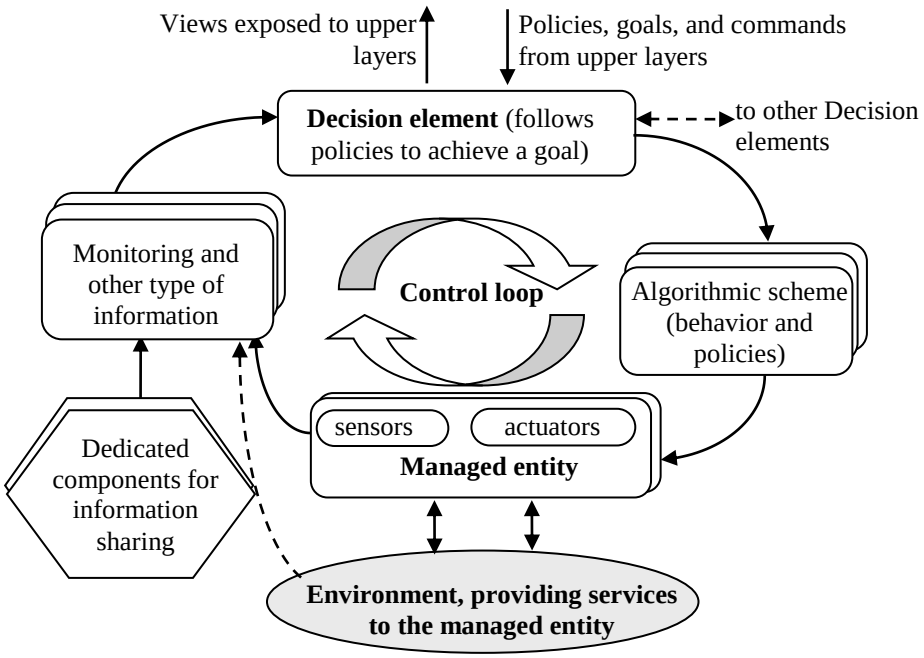

Figure 1 Model of abstract autonomous networking system (ETSI GS AFI 002)

Methods of information and knowledge management cover all mechanisms enabling information exchange and retrieval without any manual intervention and taking into account the system's dynamic. These procedures aim at designing mechanisms for data acquisition, training and management of linked knowledge, which allow creation of a self-aware system. Cognitive methods and techniques include learning and reasoning assume the system to be self-descriptive, to increase its self-awareness and to improve the decision-making process. Service models are used for proper management of network resources in order to meet different services requirements (such as availability, reliability, quality of service). Network management mechanisms are needed for policies creation and validation, to link a policy to objectives and configuration data in network profiles and to distribute these profiles over the network. Various methods of network modelling exist, which allow easier description as well as network definition and performance evaluation. An autonomous system or a system unit adapt their behaviour in response to changes in the system itself or changes in its environment. Information for such changes is obtained by means of environmental monitoring and is realized by sensors. All the information gathered is processed and distributed to other system units. In order to model, design and implement an autonomous control system, programmability of resources is used. Resource programmability provides primitives operations of management interfaces for different kinds of managed units.

5. USE CASES FOR AUTONOMOUS MANAGEMENT

The evolution to the Future Internet requires incorporation of capabilities for self-management in modern network infrastructure in meeting the needs of services and preserving the efficiency of the network. There is a need to automate multiple processes (many of which affect the business) in the networks of the future, i.e.

execution of processes based on the relevant autonomous decisions without human intervention. Modern Information and communications technology (ICT) systems have not inherent capabilities for "training" of the past (or current) experience and can not contextualize and adapt to evolutionary processes based on their own monitoring processes and training. Many ICT applications can't be developed further without embedding intelligence and cognition. In the context of the Future Internet, networks having cognitive properties are regarded as key communication next-generation technologies and it is expected to significantly improve the communication service, providing effective solutions.

A couple of research tasks in the field of autonomous management of the Internet of the future are examined in the next three subsections.

5.1 Self-configuration of services in Future Internet

When developing new services that meet new consumer demand, the number of network equipment and stakeholders is constantly increasing, while opportunities for management and cooperation have reached the limits of human capacity. Adding new service is a challenge because it is necessary cooperation between all parties. This is done manually without automatic process by considering each case individually, taking into account the limitations of each party. The service provider expects service provisioning through a common infrastructure and transparent management through virtualization of resources. Users do not have specific telecommunication skills and require ease service usage without configuration. With the introduction of new services increases the possibility of unexpected interaction between them. Unexpected interactions are resolved manually. Continuity of service is difficult to achieve as services are configured statically for a certain type of network access and multiple users. There is a need for mechanisms for self-configuration of services, detection and resolution of conflicts between services.

5.2 Self-configuration of network devices in Future Internet

With current practices for network management, network administrator initialize the network node, to create manually a configuration profile, to connect the node to the network, taking into account the requirements for scalability and network topology. With modern technology equipment, produced by the manufacturer, it only activates its default settings at initialization, while the operator manually configures its interfaces and communications protocols. The possibilities for remote configuration management are limited and implemented only after initial manual configuration of interfaces for device management. The configuration commands or data do not cover the full configuration profiles of devices. Modern technologies do not provide discovery of supported capabilities for self-management features, device description and properties notification. On the one hand, capabilities for autonomous element discovery are necessary that take control for devices configuration. On the other hand, capabilities for device self-description need to be available on managing autonomous elements. Such knowledge is required to define the role of the new device and to provide a configuration profile that is used for self-reconfiguration.

5.3 Discovery, analyses and solving faults and intrusions in Future Internet

The detection of unusual and undesirable behavior in the network requires addressing issues like fault diagnosis, troubleshooting and problem resolution. This task is hard in a distributed wireless environment, where it is necessary to correlate information from different network levels and network elements. Typical problems such as anomaly detection, fault prediction and intrusions detection are addressed by identifying undesirable behavior. Usually fault notifications and malfunction alarms follow a pattern that in recognition are used to predict the failures. This means that preventive actions are taken beforehand in order to prevent malfunction. These processes are automated with minimal human intervention. Upon detection of an anomaly, the involved network elements use alternative setting profiles and configurations. Traffic anomaly detection in the wireless environment is hard because of the unpredictable nature of radio conditions and constrained resources of mobile devices, but it is important to prevent overloading and to detect failures. In a distributed environment, it is important to collect statistics at local level, as undetected abnormality of one network level is found on another level using monitoring data at the different levels. Another problem is the intrusion detection. The used techniques in most existing systems for intrusion detection rely on training data, which is expensive and not applicable to detect new types of attacks. Therefore it is necessary to use various cognitive methods to detect anomalies that rely on unsupervised training.

6. CONCLUSION

The affair with expanding global network occurs with increasing force. Systems that are able to manage themselves resist of his push. When considering self-configuration of services it is perceptible the necessity of an appliance that resolves controversy between them. If it comes to self-configuration of network devices we talk about a mechanism with specific knowledge that defines the role of a new device and implement the necessary configuration. In case of proactive discovery of faults or intrusions methods should be developed to detect and resolve them. The true logic shows that the autonomous management plays an ever–greater role in Future Internet.

7. REFERENCES

[1] J. Wan, M. Chen, F. Xia, Di Li, K. Zhou, “From Machine-to-Machine Communications towards Cyber-Physical Systems,” Computer Science and Information Systems, ComSIS vol. 10, No. 3, 2013, pp.1105-1128, doi: 10.2298/CSIS120326018W.

[2] A. Aijaz, A. H. Aghvami,”Cognitive Machine-to-Machine Communications for Internet-of-Things: A Protocol Stack Perspective,” Internet of Things Journal, IEEE, vol.2, no.2, 2015, pp.103-112.

[3] Q.M. Ashraf, M. H. Habaebi, “Introducing Autonomy in Internet of Things,” Recent Advances in Computer Science, 2015, pp.215-221.

[4] Q. M. Ashraf, M. H. Habaebi, **“**Autonomic schemes for threat mitigation in Internet of Things,” Journal of Network and Computer Applications, vol.49, issue C, 2015, pp. 112-127.

[5] Q. M. Ashraf, M. H. Habaebi, G. Sinniah, M. Ahmed, S. Khan, S. Hameed, "Autonomic protocol and architecture for devices in Internet of Things," IEEE Innovative Smart Grid Technologies - Asia (ISGT Asia), Kuala Lumpur, 2014.

[6] B. Copigneaux, "Semi-autonomous, context-aware, agent using behaviour modelling and reputation systems to authorize data operation in the Internet of Things," IEEE World Forum on Internet of Things (WF-IoT), 2014 , pp.411-416, doi: 10.1109/WF-IoT.2014.6803201.

[7] M. Meddeb, M. Ben Alaya, T. Monteil, A. Dhraief, K. Drira, "M2M Platform with Autonomic Device Management Service," Priced Computer Science, vol.32, 2014, pp. 1063–1070, International Conference on Ambient Systems, Networks and Technologies (ANT-2014), International Conference on Sustainable Energy Information Technology (SEIT-2014).

[8] Jung I. Y. , G.J. Jang, J.M. Yang, J. Yoo, " Design of a Situation Aware Service for Internet of Things," International Journal of Distributed Sensor Networks, vol 2015, Article ID 641312, 8 pages, http://dx.doi.org/10.1155/2015/641312.

[9] C. S. Shih, K.J. Lin, J.J. Chou. C.C. Chuang, "Autonomous Service Management for Location and Context Aware Service," IEEE 7th International Conference on Service-Oriented Computing and Applications (SOCA), 2014, pp.246-251, doi: 10.1109/SOCA.2014.10.

[10] R. Kamal, J.H Lee,. C.K. Hwang, S.I. Moon, C.S. Hong, M.J. Choi, "Psychic: An autonomic inference engine for M2M management in Future Internet," sia-Pacific Network Operations and Management Symposium (APNOMS), 2013 pp.1-6, 25-27.

[11] F. Andren, G. Lauss, R. Brundlinger, P. Svec, T. Strasser, "An Open Source-Based and Standard-Complient Smart Grid Laboratory Automation System: The AIT SmartEST Approach," Industial Applications of Holonic and Multi-Agent Systems, Springer, 2015, pp.195-205.

[12] P. Kadera, M. Macas, "Applying Agents and Genetic Algorithms for Reducing Peak Consumption in District Heating,", Industial Applications of Holonic and Multi-Agent Systems, Springer, 2015, pp.206-216.

[13] M. Obitko, V. Jirkonsky, "Big Data Semantics in Industry 4.0,", Industial Applications of Holonic and Multi-Agent Systems, Springer, 2015, pp.217-229.

[14] G. Zhabelova, V. Vyatkin, "Towards a Design Methodology for Agent-Based Automation of Smart Grid,", Industial Applications of Holonic and Multi-Agent Systems, Springer, 2015, pp.181-194.