Volume 5, Issue 12, December 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

An Analysis of Effective Machine-to-Machine Communication for Nuclear Power Plant through Neural Support Algorithm

Priyadharshini SP
P.G. Student, Department of Computer Science and Engineering,IFET College of Engineering, Villupuram, Tamilnadu, India

Rajesh R
Assistant Professor, Department of Computer Science and Engineering, IFET College of Engineering, Villupuram, Tamilnadu, India

Abstract— Machine-to-machine (M2M) communications is a subset that enables networked devices to exchange information among each other as well as with business application servers and therefore creates the Internet-of-Things (IoT) environment. In this paper, the analysis and the design work of the specific IoT industrial automation application is depicted. At present, IoT industrial application field such as Nuclear Power Plant (NPP) faces several issues in security and the devices lack in neural analysis are discussed in this paper. Neural Support Algorithm (NSA) is designed to support the integration of neural analysis and neural learning of things with secured communication. The neural analysis of the devices in NPP can be done by categorization technique which functions based on set of parameters. Backtracking algorithm is used further to make modifications in the problem-solving methodologies. Neural learning of devices can be empowered by redistributing the set of received suggestions and finding out the best rated solution then store it into the available heuristics.

Keywords— Internet of Things (IoT), Machine to Machine (M2M), Nuclear Power Plant (NPP), Heuristic, Neural Support Algorithm (NSA).

I. INTRODUCTION

The term Internet of Things (IoT) is defined as the network of highly connected various kind of devices such as smart sensors, actuators, smartphones, RFID tags, backend servers, etc.. Machine to Machine (M2M) Communication enables those interconnected network of heterogeneous objects to interact and exchange information among each other and therefore creates the IoT environment practically possible. Machine to Machine (M2M) Communication made the practical realization of interconnected intelligent devices to communicate information and to coordinate decisions. M2M Communications are realized through a range of technologies and networks of various devices. IoT enables any physical objects to be connected and provides smart communication between those connected devices through M2M communication in order to reduce human intervention.

Even though the devices connected together in IoT environment generates smartness in information and communication technologies, they still facing several challenges in their technical and application aspects.A huge amount of interconnected objects as envisioned for the IoT will create a major challenges in terms of security in data exchange, privacy concern, constrained resources, device heterogeneity, sensor anonymity, decision making support and so on. A fundamental challenge in M2M communication is that ever increasing number of connected IoT devices.

According to Ericsson, survey on IoT states that around 50 billion connected devices will exist by 2020. This may create a major challenge towards the existing M2M communications in terms of security and privacy of data concern.

Decision support systems are still a major problem in machine to machine interaction network i.e., IoT since they highly aim to reduce the human interventions during their communication.

To overcome the decision support limitations of interconnected devices in the Nuclear Power Plant (NPP), Neural Support Algorithm (NSA) which integrates several existing neural network functionalities have been proposed. The aim of this paper is to suggest several integrated neural network algorithms into devices to improve their decision making support while devices provides communication among themselves in IoT environment such as Nuclear Power Plant (NPP). To enhance the best possible secured way of communication among Machine-to-Machine interactions in NPP.

II. MACHINE-TO-MACHINE (M2M) COMMUNICATION

Machine-to-machine (M2M) communications is a subset of IoT which enables networked devices to exchange information among each other as well as with business application servers and therefore creates what is known as the Internet-of-Things (IoT).

It provides ubiquitous connectivity between devices along with an ability to communicate autonomously requiring no human intervention. M2M communications acts as an enabling technology for the practical realization of Internet-of-Things (IoT). M2M communications will be realized through a range of technologies and networks.

Types of M2M Network:

M2M networks can be divided into two broad domains:

- capillaryM2M network
- cellularM2M network

Capillary M2M Network:

In capillary M2M networks, M2M devices form a device area network wherein connectivity is provided through short-range communication technologies (such as ZigBee and Wi-Fi). Wide area connectivity is provided through a gateway.
Capillary M2M networks are generally characterized by a huge number of low-cost and low-complexity devices, requirements of high energy efficiency and reliability, unplanned deployments, high packet loss ratios, use of low power link layer technologies, etc. In literature, this type of networks is also referred to as low power and lossy networks (LLN).

Cellular M2M Network:

In cellular M2M networks, M2M devices are equipped with embedded SIM cards and have the ability of communicating autonomously with the cellular network like a normal user equipment. Cellular M2M has unique characteristics of small data transmissions, mostly mobile-originated (uplink) traffic, little or no mobility of devices, service requirements of high energy efficiency, etc.

III. EXISTING METHODOLOGY

In this paper, the analysis and design study of Nuclear Power Plant (NPP) a very sensible industrial application area is considered. Nuclear Power Plant (NPP) is the field of highly interconnected devices where the device that are embedded into the power plant station such as sensors, back-end server, mobile devices, actuators, etc… can provide communication among themselves and assures the better way of data processing.

Nuclear Power Plants enabling M2M Communication:

The nuclear industry and government organizations are showing an increasing interest in the implementation of NPP. Many nuclear power plants have increased their availability factors by more than 10 percent over the last decade and they aim to reach availability levels well above 80%. Nuclear energy is a major part of power generation mix of many countries in the world. More than 430 nuclear power plants (NPPs) are operating and spreading all over the inhabited land.
The Power plant chamber holds diverse set of sensing elements which maintains a uninterrupted data communication with the power plant's back-end server for intimating and updating the process occurs inside the chambers. Sensors with heterogeneous functionality provide their individual process acts as an input device that initiates M2M communication in the field of NPP. Here those input elements and the server device make processing to minimize the human intervention. Although there were only a few NPPs accidents, social and environmental impacts were too high.
Several impacts have made the nuclear power safety a controversial issue. Computer technology is fast evolving and ever changing. What is considered to be 'state-of the-art' one year can become outdated and classified as obsolete a few years later. One of the challenges facing the IT organization is to provide power plant users with software that fills their needs and also stands the test of time.
From the existing process the fundamental safety objective of protecting people through NPP by individually and collectively and the environment has to be achieved without unduly limiting the operation of facilities or the conduct of activities that give rise to radiation risks. First the network needs to improve the scalability to support various participants this system involves huge hardware/software investments and high maintenance cost. The network site should customize the access control to see which seekers can see which part of the data shared.
Data fusion is termed as binding together data from multiple sources to create new sight. Browsing through a large data set would be difficult and time consuming. Due to Increase in the amount of data in the field of applications, environmental research and many others, it has become difficult to find, analyze patterns, associations within such large data. The data are measured as solutions or suggestions. Several suggestions are stored in research center as a track record when needed the data can be collected. The need for the suggestions is requested when fault occurs.

Early Warning System:

An Early Warning System or EWS is a core type of IoT information system used for environment disaster risk and effect management. It helps prevent loss of life and reduces the economic and material impact of disasters. In 2011, it has been estimated that the cost of installing an EWS for tsunami detection in the Indian Ocean was between $30 to $200 million dollars, depending on the number of sensor buoys used, the precision of the measurements and that the benefit to cost ratio was 4:1, i.e., every dollar spent on mitigation saved society four US dollars.
Specific parts of natural environments for weather forecasting are instrumented with fixed sensors to monitor them. These represent IoTs in the physical environment. This sensor data is then transmitted (upstream) to either an onsite, or remote, data processing centre, or to both when federated. These data centres run the (downstream) routine operational event detection, special event detection, event handling decision processes and command-control work-flows. Typical workflows are pre-planned and include: Geographical Information System (GIS) processing to capture, store, analyze and present the spatial -temporal context of the environment as customized maps; sensor data-fusion processing, decision analysis and support for information alerts to authorities and citizens.

IV. PROPOSED METHODOLOGY

To overcome the limitations in the existing system, Neural Analysis and Neural Learning is provided to the specific NPP through Neural support algorithm (NSA). It also enhances decision making support to the devices to solve the newly occurred problems in the power plant station.

Heuristic Problem Solving

In Nuclear Power Plant stations, several unidentified problems may occur during its process. At present those kinds of issues requires an expert in the power plant to feed the appropriate solution to the problem. Heuristic Problem Solving methodology into the database servers of the NPP enables the devices to find and rend the relevant solution to the problem that occurs in an instant.

Heuristics problem solving maintains a record of possible problems history along with their relevant optimal solution in the back-end database servers of NPP, which in turn helps the devices to recognize the absolute solution for any possible problem. Heuristics record maintenance highly helps to minimize the human intercession.

Neural Support Algorithm

Neural analysis process facilitates the things or devices to be capable of providing decision support towards massive storage of data. Several neural network training functions are depicted into the proposed neural support algorithm to generate out the neural analysis among the devices.

Processing Steps of NSA:

- Neural network training functions are organized in order to provide neural analysis to the devices
- Newly occurred problem gathered from the sensing elements are send as a request to the cloud database server from the specific Power plant server
- Cloud data server processes the request by send it to several other smart devices of various power plants.
- Suggestions from all other power plants are clubbed and forwarded to the requested NPP.
- Through prediction and classification functions of trained neural analysis set the optimal solution for the problem is defined with respect to certain threshold limit.
- Determined optimal solution is applied and verified for its feasibility.
- Alert system is used to indicate the optimal range of the applied solution.
- Best optimal solution is then stored into the heuristics record for the future purpose.

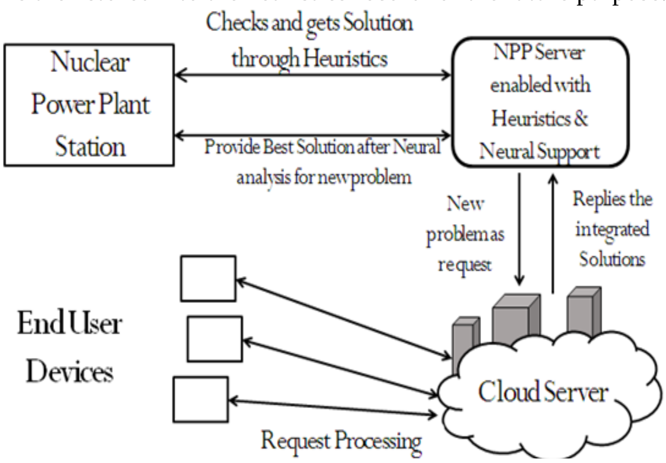

Fig.1 Overall System Architecture

Fig. 1 describes the diagrammaticrepresentation of the process flow. In the desired Power Plant Station, inputs for the process were gathered through several sensors which is in heterogeneous form. The complete process inside the station was updated to the backend server of the NPP. The possible Problems are resolved using Heuristic Problem solving strategy and the newly occurred problem is processed as a query with the help of a cloud server that which provides communication with several other expert end user devices.

Advantages of Proposed System:

- Proposed system is not meant for single application. This can be used in different applications.
- When there is prolonged use of data, instead of performance degradation there will be performance up-gradation.
- Improved Problem-Solving ability through Heuristics.
- Devices are capable of finding out the best solution.

V. CONCLUSION AND FUTURE WORK

In this paper, the possible problems occurred in NPP are solved by using heuristic problem solving methodology which detects the problem and enhances several solutions for that problem. The proposed neural support Algorithm (NSA) capably supports the devices to solve the new undefined problems. For accurate solution Neural analysis deals with several researchers for exact solution. Then the suggestions by best researchers are rated and by cumulative result the solution is applied for the problem. Thus the NSA acts as a supporting process for decision making system.

Our future work focuses on developing and Implementing Neural Support Algorithm (NSA) into devices to supportand enhance the decision-making support during M2M communication. As well as analyzing the performance of proposed work with the existing mechanisms.

REFERENCES

[1] Kim Thuat Nguyen, Maryline Laurent, Nouha Oualha, "Survey on Secure communication protocols for the Internet of Things," Elsevier Adhoc Networks, vol. 32 Issue. C, Pages 17-31, Sep 2015.

[2] Stefan Poslad, Stuart E. Middleton, Fernando Chaves, Ran Tao, Ocal Necmioglu and Ulrich Bügel, "A Semantic IoT Early Warning System for Natural Environment Crisis Management," IEEE Transactions on Emerging Topics in Computing, 2015.

[3] FriederGanz, Daniel Puschmann, Payam Barnaghi, "A Practical Evaluation of Information Processing and Abstraction Techniques for the Internet of Things," IEEE Internet of Things Journal, vol. 2, no. 4, August 2015.

[4] ShyamSundar Prasad, Chanakya Kumar, "An Energy Efficient and Reliable Internet of Things," International Conference on Communication, Information & Computing Technology (ICCICT), 2012.

[5] BoyiXu, Li Da Xu, "Ubiquitous Data Accessing Method in IoT-Based Information System for Emergency Medical Services," IEEE Transactions on Industrial Informatics, vol. 10, no. 2, May 2014.

[6] Yanuarius Teofilus Larosa and Jiann-Liang Chen, Yi-Wei Ma, Sy-Yen Kuo, "Socio-Organism Inspired Model Forming Multi-Level Computational Scheme for Integrated IoT Service Architecture," 2nd Baltic Congress on Future Internet Communications, 2012.

[7] Huansheng Ning and Ziou Wang, "Future Internet of Things Architecture: Like Mankind Neural System or Social Organization Framework?," IEEE Communications Letters, vol. 15, no. 4, April 2011.

[8] Adnan AijaZ and A. Hamid Aghvami, "Cognitive Machine-to-Machine Communications for Internet-of-Things: A Protocol Stack Perspective," IEEE Internet of Things Journal, vol. 2, no. 2, April 2015.

[9] Michele Nitti, Luigi Atzori, and Irena Pletikosa Cvijikj, "Friendship Selection in the Social Internet of Things: Challenges and Possible Strategies," IEEE Internet of Things Journal, vol. 2, no. 3, June 2015.

[10] Andrew Armenia and Joe H. Chow, "A Flexible Phasor Data Concentrator Design Leveraging Existing Software Technologies," IEEE Transactions On Smart Grid, vol. 1, no. 1, June 2010.

[11] Debiao He and Sherali Zeadally, "An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography," IEEE Internet of Things Journal, vol. 2, no. 1, February 2015.

[12] Sriram N. Premnath and Zygmunt J. Haas, "Security and Privacy in the Internet-of-Things under Time-and-Budget-Limited Adversary Model," IEEE Wireless Communications Letters, vol. 4, no. 3, June 2015.

