Software Defined Networking and Network Function Virtualization in the Industrial Internet

Manihatty Bojan, Viswanathan & Gurtov, Andrei
viswanathan.manihattybojan@aalto.fi , gurtov@hiit.fi

***Abstract*—Industrial Internet is the most recent research interest in the technology world. This network integrates industrial machines with one another and allows them to communicate independently. They help in developing a system that can read the state of a machine continuously and act immediately in case of any issues. And in such intelligent systems, there is always a necessity for a controlled network architecture. Software Defined Networking(SDN) and Network Function Virtualization(NFV) addresses this requirement by providing a centralised control of the network architecture, and thereby providing better management of the network resources.**

This article discusses in detail the implementation of SDN and the NFV architectures in an Industrial Internet environment. It provides an insight into the network requirements and security implications by implementing the SDN and NFV in an Industrial Internet environment. Additionally, this araticle also provides an overview of implementing the Openflow architecture and their relative benefits in the Industrial Internet.

KEYWORDS: Industrial Internet, SDN, NFV

I. Introduction

There has been a very strong association between the mankind and the machines for a long time since the Industrial Revolution. Later, the Internet revolution emerged that helped in connecting the mankind with one another. And today, we are in the next era of revolution where the machines interact among themselves with minimal intervention from people. This is the age of Industrial Internet where intelligent machines are able to monitor their own state with the help of sensors and machine-learning procedures. The machines interact with one another with the help of the Internet and exchange data. The collected data is then sent to cloud systems where they are analysed by powerful software. The software then understands the state of the machine and identifies any faults that are present in the system. In case of any issues, the software notifies the respective team about the state of the issue and its severity. Later, the technical team works on the issue and the problem is addressed. In this way, Industrial Internet helps in taking proactive steps in maintaining the health of the machines, and thereby eliminating the chances of any unforeseen outages[1]. Fig. 1 represents a typical workflow of an Industrial Internet of Things(IIoT) environment.

Industrial Internet technology is very promising and implementing it in real time can benefit the industries of various sectors. Here, the machines need to communicate and exchange data with one another in a coordinated manner in order to deliver the machine related statistics to the centralised cloud storage for analysis purpose. And this can be achieved only through implementing strong networking concepts. Therefore, computer networking forms a crucial part of the Industrial Internet system. However, the level of modularity and abstraction in computer networks is still questionable as they are difficult to manage. This can result in an unexpected scenario in an Industrial Internet environment which has been designed to act proactively. Hence, it is mandatory to look for options that can favour a controlled network management. And this can be achieved through SDN and NFV.

SDN and NFV are two recent developments in the field of computer networking that offer a controlled network flow. Implementing the SDN and NFV concepts in Industrial Internet systems can propel the growth of the industries. This article primarily focuses on the requirements and possibilities of implementing SDN and NFV in the Industrial Internet.

II. An Overview of SDN and NFV

Modularity with abstraction is how any system evolves. Both modularity and the abstraction can be embedded in those systems which help users to understand and manage easily. Computer networks are hard to manage and there is a lack of formal principles

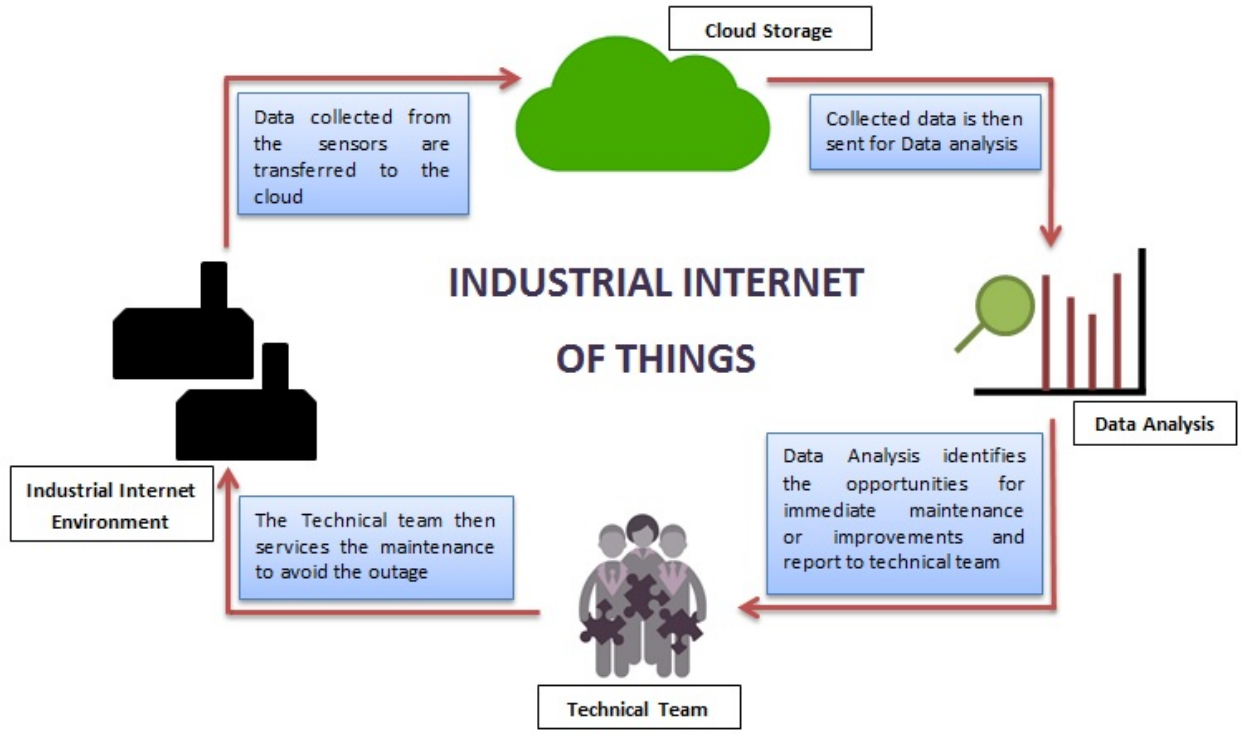

Fig. 1. *A sample Industrial Internet of Things(IIoT) workflow model*

available to understand the organisation of networking. A lot of network specific hardware devices have been developed to offer better performance, however, with a lower flexibility. SDN and NFV are two developments in the networking field that offer both higher efficiency and easier management of the network devices through virtualisation techniques [2].

Every switch used in the computer networks has a Data plane and a Control plane. The Data plane deals with processing and delivery of the packets. On the other hand, the Control plane deals with computing the forward state. This involves understanding the network configuration, network constraints and the most efficient algorithms that can be employed, which helps in successful and effective delivery of the packets to the destinations [3]. SDN primarily focuses in delivering the abstraction in the Control plane. The primary idea behind implementing SDN is to move the control plane outside the switches and enable external control of data through a logical software entity called controller. SDN provides simple abstractions to describe the functionality of the components and the protocol to manage the forwarding plane from the remote controller through a secure channel [4].

NFV is a network architecture that employs the idea of virtualizing the network related functionalities. That is, NFV helps in providing the network related functionalities by means of a software implemented on Virtual machines, that are hosted on a standard hardware platform [5]. Similar to any other cloud based system, they are created on demand. NFV based systems offer better scalability, portability and elasticity, and are stable. The basic premise of NFV is that the network functions have their software implementations decoupled from the computations, storage, and network resources that they use [4]. They help in easy deployment of the network services and makes way for enabling network functions with additional enhanced capabilities and options[2].

III. Network Requirements for Industrial Internet

Network stability and security are two primary features that need to be acknowledged in an industrial internet environment. This is because the quality of the work and the industry's revenue generation depend on these aspects of the networks. The following section discusses the network requirements and the security implications in an industrial internet environment[6].

- *Performance*: An Industrial Environment has a very stringent network latency requirement of less than 1 ms and a packet loss of less than 10^{-9} [7]. Hence, there is a necessity for high performance in an industrial environment. In terms of network, low latency and high throughput produce better performance. The low latency helps the smart machines to communicate with one another instantaneously. High throughput helps the machines to transfer larger data. Along with the above two parameters, the jitter also plays a pivotal role in determining the performance of the network systems in an industrial environment.
- *Reliability*: Industrial environment is susceptible to disruptions and failures. In such instances, it is very important for the machines to maintain their state. The network connectivity during such failures should promise a faithful degradation which in turn minimizes the destructive loss. At the same time, it is also important for the network connectivity to regain its state when the conditions are impeccable. In this way, the network should prove to be reliable.
- *Scalability*: The industrial environment has always been a growing sector. With the advent of the industrial internet in the sector, it formulates a path for additional equipment and resources to be integrated together. Hence, it is mandatory for the network connectivity to scale according to the demand.
- *Durability & Interoperability*: The industrial internet systems have a longer lifespan and as a result, the hardware components associated in such a system are not readily changed. However, the network software components that are a part of the system need to support regular updates. Finally, it is essential for the Industrial Internet systems to support the interoperability and thereby support the information exchange process in a heterogeneous network.
- *Fault Tolerant Networks*: It is essential for the Industrial Internet network architecture to be fault tolerant. SDN management approach in an Industrial environment can help in delivering a fault tolerant network system along with continuous Quality of Services(QoS). The authors in the paper [8] first decide on selecting the path based on the Dijkstra's algorithm. Later, the determined path is then removed and a completely independent backup path is then decided. Whenever there is a change in the network topology, the switches notify the SDN controllers to implement a new network topology. The switches then reroute the packets over the backup route and thereby notify the other switches in the system regarding the updated topology. The experimental results showed that there were no packet loss upon the changed topology configuration and the packets were being delivered to the destination in a very short timeframe of less than 350 ms. In this way, a complete redundant system can be built in an Industrial Internet environment with the help of SDN.

In an industrial environment setup, it is necessary for the machines to react quickly under all conditions. It is the responsibility of the network connectivity to support this responsive behaviour. Hence, it becomes important to configure the network in a controlled manner. The authors in [9] study the behaviour of SDN QoS controllers in an Industrial Internet environment. The results show that the delay incurred in an SDN controlled system was comparatively very much lower compared to an independent network system or in Amazon AWS cloud systems. Additionally, the paper also recommends implementing Industrial Internet systems in a controlled and configurable environment which in turn can be brought by SDN. Considering the role of NFV here, we need to understand that the NFV must work in a hybrid network environment composed of both the legacy physical network appliances and the virtual network appliances. NFV provides an opportunity by making the software appliances operate in a standardised and open infrastructure. And they can be made to use the existing north bound interfaces to control the traffic among the switches. SDN and NFV technologies can then be assimilated together where the network function virtualisation orchestration system can control the forwarding behaviours of the hardware switches using SDN.

IV. 5G Technology in Industrial Internet

Today, internet connected devices are based on the 4G technology. However by 2020, there will be a substantial growth in the amount of network traffic because of the huge number of interconnected devices. 5G technology is needed because there is a growing demand for both capacity and the capability of the network. The capacity can be brought by making more spectrum available for the usage. The demanding capability includes networks with higher bandwidth and very low latency.

Project METIS(Mobile and Wireless Communication Enablers for Twenty-twenty(2020) Information Society), which is co-founded by the European Commission is playing a prominent role in the development of 5G technology. The deliverable D1.5 under the METIS project discusses the updated scenarios, requirements and the Key Performance Indicators(KPIs) for 5G mobile and wireless system[7].As per the report, the technical goals are set to provide:

- 1000 times higher mobile data volume per area,
- 10 times to 100 times higher typical user data rate,
- 10 times to 100 times higher number of connected devices,
- 10 times longer battery life for low power devices, and
- 5 times reduced end to end latency

at a similar cost and energy consumption levels as today's system.

One of the key challenges of the Industrial Internet is the ubiquitous networking between the components involved in the Industrial Internet environment. 5G technology can be a key contributor in delivering these capabilities. The control applications residing in an Industrial Environment have a very stringent network latency requirement of less than 1 ms and a packet loss of less than 10^{-9}. It is mandatory for the Industrial Internet architecture to support such distinctive access technologies and the smooth communication between them. According to the Bosch Group[BOSCH-Web], the aforementioned requirements of the Industrial Internet cannot be fulfilled by the existing 3G and the 4G technologies. And as disclosed by the requirements of the METIS project as a part of 5G mobile technology construction, we can understand that 5G technology can help in benefitting the Industrial Internet environment to a great extent[7].

As already discussed, 5G eventually leads to a large number of interconnected devices. This results in a need for elastic scaling of the network traffic demand which needs to be effectively handled. Authors in [10] have concluded that the use of SDN in the 5G mobile networks can help in handling the network traffic demand. The authors have tried to bring the network control of 5G as a group of SDN applications which includes the Base Station, Backhaul, Mobility, Access and Service Delivery applications. They consider these application to be present in the controller Northbound API to support multiple SDN applications.

V. Security Implications in Industrial Internet

Despite being a successful innovation in the world of technology, the Industrial Internet has its own share of factors that might hinder its growth. The World Economic Forum conducted a survey in the year 2014 regarding the key barriers to adopting the Industrial Internet[11]. It was conducted in North America and Europe and the results showed that more than two thirds of the respondents considered security and interoperability as two main barriers in adopting Industrial Internet. Hence, cyber security management plays a key role in deciding the success of Industrial Internet. This includes both network security and the security of the physical hardware devices.

As per NIST SP800-82 R2[12], Guide to Industrial Control Systems(ICS) Security, some of the factors that currently contribute to the increasing risk of the control systems are:

- *Adoption of standardised protocols and technologies with known vulnerabilities*. The initial intention of making the proprietary protocols open was to help third party manufacturers in building compatible software that can be run on the ICS. However, this improvement also made the ICS systems prone to cyber attacks.
- *Integration of the ICS with the public and the corporate networks*. This increases the vulnerabilities and makes the ICS an easy target. Earlier, the integration of the ICS with the corporate networks was achieved with the help of the servers and gateways, which offers better reliability. However, in the past decade, the connections have been implemented using the Transmission Control Protocol/ Internet protocol (TCP/IP), and with the help of standardised applications like File Transfer Protocol(FTP). These

connections were implemented without understanding the potential risks. With the availability of Internet for communication purposes, these systems play an important role in data transfer but also act as potential vulnerabilities where the data can be hacked.

Additionally, the interconnection between the ICS and the corporate networks often involves systems with different communication standards[13]. As a result, the engineers often give importance to the successful transmission of the data and fail to study the risks involved in the system.

As per NIST SP800-82 R2[12], Guide to Industrial Control Systems(ICS) Security, one of the novel solutions to overcome the aforementioned security overheads is to separate the ICS network from the corporate network. Both are different network architectures and deal with different networking aspects. Internet access, email, FTP and remote access form a part of the corporate network while change control procedures for network equipment, configuration and software changes form a part of the ICS. It is necessary that network traffic between both the different systems should be kept minimal and the traffic that is allowed on the other system needs to be intercepted for any potential risks.

NIST SP800-82[12] suggests allowing the traffic between the systems through the firewall and a demilitarized zone(DMZ). A DMZ is a network segment that connects directly to the firewall. DMZ is an additional level of security that is implemented at a point where the organisation's secured network comes in contact with the untrusted open network, usually the public internet. Here in the Industrial environment, the ICS data can be made available on the DMZ network segment and the corporate networks can be provided with a restricted access to the data that is available only on the DMZ segment. In this way, minimal traffic can be guaranteed in a completely secured environment.

By enabling an SDN architecture in such a restricted environment, a better control of the network traffic in the ICS is achieved. The SDN architecture can be housed on the systems that interact with the DMZ. Whenever there is a change in the network traffic in the ICS or when there is a necessity for software upgradation associated with the hardware switches, the information and the software patches can be sent from the corporate network to the DMZ segment of the ICS network over a secured channel or Virtual private network(VPN). The SDN controllers can then receive the details and implement them in the underlying data plane. However, when SDN and NFV are implemented together, there might be a requirement to implement an additional layer of security when the SDN controller interacts with the virtualised data plane. A very similar approach of minimal traffic should be guaranteed when the controller interacts with the virtualised network devices.

VI. Enabling OpenFlow Protocol of SDN

Generally, SDN can be referred to the various ways to use software to manipulate and manage the networks. In this regard, SDN can be classified as three models:

- *Open SDN with OpenFlow*: OpenFlow is the first standard communication interface defined between the control plane and the data plane of an SDN architecture. This is used to define the functionalities and update the software of the networking devices[14].
- *SDN via Application programming interface(API)*: The developers are provided with an API in order to control the functionality associated with the networking devices lying at the infrastructure layer.
- *SDN via Overlays*: Virtual Extensible LAN (VXLAN) tunnels are used across in the network infrastructure. The VXLANs are used in the place of VLAN and provide better flexibility and scalability when integrated with an SDN environment[15].

Here, we shall be focussing more on employing the openflow protocol in the SDN architecture that can be implemented in industrial internet. With OpenFlow, we can create an open interface on the networking devices and create an abstraction layer(SDN controllers like Open Networking Operating System) through which the functionality of the networking devices can be controlled on a continuous basis. That is, the SDN controllers make use of the OpenFlow protocol in order to communicate and control the network forwarding elements such as the switches[16].

The Industrial Internet system is built on a heterogeneous network architecture. This is because of the varied industrial requirements. SDN-based orchestration tools can be used to deploy, configure and update any OpenFlow supported networking devices irrespective of the vendors. In this way, a centralised control is established in a multi-vendor environment. Secondly, the OpenFlow based SDN offers a flexible network

automation and management framework, which is one of the primary features of the Industrial Internet. In this way, the network instability can be reduced. Finally, it is possible to define the network configurations which are then transferred through the Openflow protocol to the flow tables of the switches to behave accordingly. Even if there is an urgent requirement to update the software of the virtual network devices, it can be taken care through the OpenFlow protocol. This increases the network reliability, which is another important factor to be considered in an Industrial Internet system[14].

The OpenFlow protocol helps in designing fault tolerant SDN systems. The authors in [16] have conducted a practical experiment in order to test the fault tolerance behaviour of the OpenFlow enabled switches. The implementation made use of a redundant L2 network with SDN controller(OpenDaylight) to calculate the network topology. Two paths were decided using the Dijkstra's algorithm under two strategies: first strategy was based on establishing a connection with the disjoint paths and the second strategy was based on establishing a backup connectivity under the failure conditions. During the experiment, some of the links between the switches were broken and packet loss was measured during the failure. Together, the time taken by the SDN controller to calculate the new network topology was also calculated. The results proved that there are no packet loss when there was a backup route available. Similarly, it took 611 ms for the network to regain stability when there was no backup route. This resulted in the loss of information. However, in the presence of a backup route, there was no information loss.

VII. Conclusions

This article provides an overview of the Industrial Internet and the possibility of adopting the SDN-NFV architecture in the Industrial Internet environment. A high level analysis on the network requirements in such an environment is studied along with the security implications associated with the Industrial Internet platform. On studying the earlier works in regard to the field, we can understand that employing the SDN architecture in the industrial environment can help in reducing the complexity associated with the network. In the presence of SDN, the network devices in the infrastructure plane can be programmed to provide an efficient, safety, fault tolerant and centrally manageable system guaranteeing QoS. All these parameters are key components of an Industrial Internet network system. And hence, deploying the SDN driven network architecture can enhance the growth of the Industrial Internet. Together with SDN, the idea of transferring the functionality aspect of the hardware network devices to the cloud environment (as a part of NFV) can help in delivering an industial internet environment that can be effectively managed.

References

[1] Peter C.Evans and Marco Annunziata, "Industrial Internet:Pushing the Boundries of Minds and machines," General Electric, Tech. Rep., November 2012, http://www.ge.com/docs/chapters/Industrial_Internet.pdf.

[2] Wood, Timothy and Ramakrishnan, KK and Hwang, Jinho and Liu, Grace and Zhang, Wei, "Towards a software-based network: integrating software defined networking and network function virtualization," *Network, IEEE*, vol. 29, no. 3, pp. 36–41, 2015.

[3] Omnes, Nathalie and Bouillon, Marc and Fromentoux, Gael and Le Grand, Olivier, "A programmable and virtualized network & IT infrastructure for the Internet of things: How can NFV & SDN help for facing the upcoming challenges," in *2015 18th International Conference on Intelligence in Next Generation Networks (ICIN)*. IEEE, 2015, pp. 64–69.

[4] Madhusanka Liyanage, Andrei Gurtov,Mika Ylianttila, *Software Defined Mobile Networks (SDMN): Beyond LTE Network Architecture*, 1st ed. John Wiley & Sons, 2015.

[5] Chi, Po-Wen and Huang, Yu-Cheng and Lei, Chin-Laung, "Efficient NFV deployment in data center networks," in *2015 IEEE International Conference on Communications (ICC)*. IEEE, 2015, pp. 5290–5295.

[6] "Industrial Internet Reference Architecture," Industrial Internet Consortium, Tech. Rep., June 2015, http://www.iiconsortium.org/IIRA-1-7-ajs.pdf.

[7] "Updated scenarios, requirements and KPIs for 5G mobile and wireless system with recommendations for future investigations," Mobile and wireless communications Enablers for the Twenty-twenty Information Society (METIS), Tech. Rep., May 2015, https://www.metis2020.com/wp-content/uploads/deliverables/METIS_D1.5_v1.pdf.

[8] P. Goncalves and J. Ferreira and P. Pedreiras and D. Corujo, "Adapting SDN datacenters to support Cloud IIoT applications," in *2015 IEEE 20th Conference on Emerging Technologies Factory Automation (ETFA)*, Sept 2015, pp. 1–4.

[9] Hu, Peng, "A System Architecture for Software-Defined Industrial Internet of Things," in *2015 IEEE International Conference on Ubiquitous Wireless Broadband (ICUWB)*. IEEE, 2015, pp. 1–5.

[10] Costa-Requena, Jose and Kantola, Raimo and Llorente, Jesús and Ferrer, Vicent and Manner, Jukka and Ding, Aaron Yi and Liu, Yanhe and Tarkoma, Sasu, "Software defined 5G mobile backhaul," in *2014 1st International Conference on 5G for Ubiquitous Connectivity (5GU)*. IEEE, 2014, pp. 258–263.

[11] "Industrial Internet of Things: Unleashing the Potential of Connected Products and Services," World Economic Forum, Tech. Rep., 2015, http://www3.weforum.org/docs/WEFUSA_IndustrialInternet_Report2015.pdf.

[12] K. S. Keith Stouffer, Joe Falco, "Guide to Industrial Control Systems (ICS) Security," National Institute of Standards and Technology, Tech. Rep., June 2011, http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf.
[13] D. Meltzer, "Securing the Industrial Internet of Things," Information Systems Security Association, Tech. Rep., https://c.ymcdn.com/sites/www.issa.org/resource/resmgr/journalpdfs/feature0615.pdf.
[14] "Software-Defined Networking:The New Norm for Networks, ONF White Paper," Open Networking Foundation, Tech. Rep., April 2012, https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf.
[15] "VXLAN: Eliminating Cloud Boundaries with SDN," ARISTA, Tech. Rep., https://www.arista.com/assets/data/pdf/VMworld_Demo_Brief.pdf.
[16] Pedro Goncalves,Andre Martins, Daniel Corujo, Rui Aguiar, "A fail-safe SDN bridging platform for cloud networks," in *2014 16th International Telecommunications Network Strategy and Planning Symposium (Networks)*. IEEE, 2014, pp. 1–6.

AUTHOR'S BIOGRAPHY

Manihatty Bojan, Viswanathan

Manihatty Bojan, Viswanathan is a final year Masters student at Norwegian University of Science and Technology (NTNU), Norway. His major is in the field of Security and Mobile Computing. His research interest includes system security, computer networks and cloud computing. You can contact Viswanathan at *viswanathan.manihattybojan@aalto.fi*

Gurtov, Andrei

Gurtov, Andrei received his M.Sc (2000) and Ph.D. (2004) degrees in Computer Science from the University of Helsinki, Finland. He is presently a Principal Scientist at the Helsinki Institute for Information Technology HIIT. He is also adjunct professor at Aalto University, University of Helsinki and University of Oulu. He was a Professor at University of Oulu in the area of Wireless Internet in 2010-12. Previously, he worked at TeliaSonera, developing 2.5G and 3G systems and was a visiting scholar at the International Computer Science Institute (ICSI), Berkeley in 2003, 2005 and 2013. Dr. Gurtov is a co-author of over 150 publications including three books, research papers, patents, and five IETF RFCs. His book on HIP was placed on IEEE "Best Readings" list in Communications and Information Systems Security (CIS). He is a senior member of IEEE, ACM Distinguished Scientist, IEEE ComSoc Distinguished Lecturer, Vice Chair of IEEE Finland Section, and an Editor of the International Journal of Distributed Sensor Networks and IEEE Journal on Internet of Things. Email: gurtov@acm.org, Mail: PO Box 15400, 00076 Aalto, Finland. You can contact Andrei at *gurtov@hiit.fi*