Baltic J. Modern Computing, Vol. 4 (2016), No. 4, 1058-1073
http://dx.doi.org/10.22364/bjmc.2016.4.4.28

Secure Communication and Data Processing Challenges in the Industrial Internet

Andrei GURTOV[1], Madhusanka LIYANAGE[2], Dmitry KORZUN[3]

[1]IDA, Linköping University and ITMO University
[2] Centre for Wireless Communications, University of Oulu
[3] Petrozavodsk State University

gurtov@acm.org, madhusanka.liyanage@oulu.fi, dkorzun@cs.karelia.ru

Abstract. The next industrial revolution is foreseen to happen with upcoming Industrial Internet that combines massive data collected by industrial sensors with data analysis for improving the efficiency of operations. Collecting, pre-processing, storing and analyzing such real-time data is a complex task with stringent demands on communication intelligence, QoS and security. In this paper we outline some challenges facing the Industrial Internet, namely integration with 5G wireless networks, Software Defined Machines, ownership and smart processing of digital sensor data. We propose a secure communication architecture for the Industrial Internet based on Smart Spaces and Virtual Private LAN Services. It is a position paper, describing state-of-the-art and a roadmap for future research on the Industrial Internet.

Keywords: Automation, Networking, 5G, VPLS, smart spaces, IoT, cybersecurity

1. Introduction

Introduction of steam engine, electricity and digital economy have made revolutional changes in the world economy. Nowadays, utilizing sensor data from machinery can make similar impact in manufacturing, transportation, energy and health sectors. By performing big data analysis, switching to preventive maintenance and on service-oriented production can boost efficiency, but even 1% reduction in costs in major sectors of economy could provide dramatic results. The Industrial Internet will enable transitions from regular machinery maintenance to prediction-based preventive maintenance. Manufacturing will move from mass production from one model fits all principle to tailored products suited to customer needs. More and more revenue would come from providing the service rather than selling a product. For instance, selling miles flown by an aircraft engine rather than the engine itself. Remote operation and on-demand maintenance of devices will be a common practice. Yet, the gap between industrial and Internet experts, knows as OT/IT divide, makes it challenging to develop the Industrial Internet.

Internet-of-things (IoT) is making a rapid progress in the Internet by providing connectivity to consumer devices such as toasters to enable their remote monitoring and

integrated smart-home solutions. On the industrial side, such approach is referred to as Machine-to-machine or Machine-type Communication, with latest support in ETSI standards. However, the Internet economics presently revolves around mining user data and providing targeted advertisement by giant companies including Google and Facebook. Thus, the best minds in network applications are focusing on creating the best algorithms to overcome ad blocking software and sell something to the users. Industrial Internet aims at changing the game by focusing the talents on data science application to design algorithms to predict machine maintenance needs and streamline operations based on machine sensor output.

In this paper, we overview the networking and security challenges facing the Industrial Internet. Then, we take a close look at two enabling technologies for IIoT: Smart Spaces for intelligent data processing and Virtual Private LAN Services (VPLS) for transparent secure interconnection of industrial networks. We do not claim that the list of challenges and relevant technologies to be exhaustive, as the Industrial Internet is a new research area.

The rest of the paper is organized as follows. In Section 2, we survey the concept of Industrial Internet and its networking aspects. In Section 3, we outline networking challenges for the Industrial Internet, namely integrating 5G infrastructure, cloud computing, software defined machines and sensors. In Section 4 and 5, we propose secure communication and smart data processing architecture for the Industrial Internet. Section 6 concludes the paper.

2. Industrial Internet of Things

The Industrial Internet is a novel concept introduced by General Electric in 2014. Therefore, there is not a lot of research literature on this subject and conferences in this area just start to appear. However, industrial automation is a mature area focusing on connectivity of cyber-physical systems such as Supervisory Control and Data Acquisition (SCADA) and Process Control Systems (PCS).

The term IoT was initially proposed to refer to uniquely identifiable interoperable connected objects with radio-frequency identification (RFID) technology. Now the most common view of IoT refers to a giant dynamic global network infrastructure for the ubiquitous connection of numerous physical objects (e.g., everyday things equipped with RFIDs, various sensors and actuators, embedded and mobile electronic devices, low capacity and powerful computers) that rely on advanced communication and information processing technologies. IoT aims at fusion of real (physical) and virtual (information) worlds, and the IoT concept evolves to service-oriented information interconnection and convergence (Kortuem, 2010), (Wang, 2013), (Perera, 2014), (Korzun, 2016).

IoT is expected to offer effective solutions to transform the operation and role of many industrial systems (Xu, 2014). This expectation leaded to the concept of Industrial Internet of Things (IIoT) or Industrial Internet for short. Similar ideas are also developed under such names as Smart Industry, Smart Factories, Advanced Manufacturing, Cyber-Physical Systems (CPS), and Industry 4.0 (the fourth industrial revolution). In particular, a CPS is composed of physical entities such as mechanisms controlled or monitored by computer-based algorithms. A CPS creates virtual counterparts to physical components, acting in the networked system as smart objects, similarly to the IoT vision.

Although IIoT applications are still in the early stage, several pilot prototypes are being developed and even experimentally deployed in various industries. Examples

include healthcare service industry (Domingo, 2012), transportation and logistics (Karakostas, 2013), food supply chains (Pang, 2015), and building automation (Han, 2014). The basic goals that an Industrial Internet System (IIS) should support are: a) increasing the productivity, b) reducing the process maintenance costs, c) providing safety for personnel, and d) making the work attractive.

Analyzing existing IIoT applications we define the following characteristic properties of an IIS.

Participation of all interested parties: Any player of application processes (either human or machine) acts as a smart IoT object. Such industrial objects are autonomous; they interact by network i.e., forming a system with massive and cooperative information sharing and processing. A large family of industrial objects is defined by sensors that measured data for process control and actuators that implement decisions coming from process control. The objects are often mobile.

Sensing automation: System perception based on incoming data flows from many distributed sensors is automated. This property essentially distinguishes the IIoT case from a traditional enterprise automation system. The automated data acquisition aims at making the system of quick response, even when the application processes are highly dynamic and operate in large-scale distributed conditions. As a result, capture of and access to real-time information become facilitated, and all vast edges of an enterprise operate closer to the process control.

Big data analytics: Participation of extremely many objects, when each continuously provides sensed data, leads to voluminous collections of raw data. Those need to be operatively processed to provide knowledge for decision-making objects of the control process. In contrast to traditional enterprise automation systems, this type of information processing becomes service-oriented and involves cloud-based solutions.

Control intelligence: The traditional approach of solving a global optimization problem for enterprise-level planning and control is not effective in IIoT due to the dynamicity and large-scale. IIS aims at provision of smart services that represent a tool for operative local decision making. A dynamic change does not necessarily lead to recalculation of the global optimal solution, since a rational reaction can be done locally, on the situation. Decision making is not automated in the mechanical sense, when the reaction is fully determined. Instead, recommendations are provided to appropriate participants to assist humans responsible for the control decisions.

In-depth rather than traditional perimeter-based security: Since the traditional firewall and VPN-based security model continues to fail repeatedly resulting into many reported break-ins to industrial network, a novel host-identity based communication architecture is needed to provide safe Industrial Internet.

3. Challenges for Industrial Internet

Although the opportunity of IIoT for manufacturing and business processes are widely accepted by majority of players in many industrial sectors, the number of practically deployed IISs is not growing very fast. One of the reasons is the large scale requirement, which consequently meets with certain technological challenges. In this section we consider some of these challenges, related to network and data problems, and propose possible solutions based on novel technologies.

3.1. Approach

We consider the following important challenges for IIoT: 1) ubiquitous connectivity, 2) network virtualization, 3) information intelligence, and 4) security requirements. They are summarized in Table 1 together with possible solution directions.

Table 1. IIoT challenges

Challenge	Enabler technology	Solution direction
Ubiquitous connectivity	5G	Low-latency, ultrareliable, long-range sensor communication
Network virtualization	SDN, NFV	OpenFlow-based connectivity of industrial machinery under IP controller running in Virtual Machines.
Information intelligence	Smart Spaces	A semantic layer is introduced to share system semantic information by participants themselves.
Security requirements	VPLS, Watermarking	Secure VPN tunnels are established between LANs to encrypt the user data. Sensor data ownership.

Ubiquitous connectivity of sensors in a noisy industrial environment presents a challenge. The sensor data needs to be periodically collected and securely delivered to clouds storage or smart spaces for processing. 5G networks under development envisage long-range but power-efficient communication for IIoT. However, several new technologies, including Software SIMs, low-latency, power-efficient and ultrareliable data delivery needs to be developed.

Software Defined Networking (SDN) is making its way in data center and enterprise networks. Adapting SDN approach e.g. based on existing OpenFlow protocol in a different world of industrial network protocols such as ModBus is a major challenge. On the one hand, additional latency for new flow setup with packet forwarding to a controller can cause unacceptable delays for real-time industrial communication, especially if the factory is geographically dispersed. On the other hand, full security of machine-controller channel is not provided by the latest OpenFlow specifications.

The smart spaces technology creates an intelligent environment for a given IIS where services are constructed with cooperative knowledge processing over information shared in the smart space. In fact, such a smart space introduces an additional layer providing functions of an information hub to the system. Each participant can publish own information to the smart space, detect information events formed by others' information publication activity, and derive knowledge from the collaboratively collected semantics.

In the past, the security of Industrial (also known as OT) networks was easy to ignore, since those networks were isolated from other IT networks and were mostly immune to the kinds of threats IT networks faced. The IP connectivity had not been used in industrial systems. Industrial systems were not even on a network at all, but rather connected through serial communications. With the evolution on IIoT, the IP based communication and networking concepts were adopted. It also introduced new security challenges to Industrial networks. Secure connectivity is mandatory requirement of

present IIoTs, VPLS is a technology that provides any-to-any bridged Ethernet transport among several customer sites across a service provider infrastructure. By integrating IPsec tunneling, secure VPLS networks can offer the secure connectivity for IIoTs

Below we describe the challenges with their relation to existing and emerging technologies, which can be enablers for solutions to overcome the challenges.

3.2. Ubiquitous Connectivity or Here Comes 5G

The standardization process for 5G networks is soon starting with the goal to have complete specifications by 2020. However, first deployments based on experimental platforms are expected already in 2018. 5G has the goal to increase 100-1000 times the peak bandwidth and the number of connected devices. At the same time, significant reductions in communication latency and battery consumption especially for IoT devices are expected. The radio interface properties are yet open, but the use of ultrahigh frequencies in millimeter wavelengths are expected to gain advantage of available spectrum. Tight integration with 4G systems and the use of cognitive radio approach is on the agenda as well.

5G is meant to support IoT and Industrial Internet by design. Examples of planned applications include control of autonomous vehicles, smart city implementation with a help of parking and light sensors, smart home wireless networks, haptic and 3D Internet and augmented reality. In the Industrial Internet domain, collection of data from a large amount of sensors and its delivery to cloud for analytics will be the primary application.

Depending on the type of data in industrial setting, different classes of traffic appear. One example is low-rate but ultrareliable communication for emergency control of industrial equipment. Other class is low-latency communication for real-time control of robotic manufacturing systems. Yet another class is long-rage low-power communication for data collection from battery-powered sensors.

Application of 5G in Industrial Internet will face multiple non-technical challenges including ownership and management of wireless networks in a factory. Will the factory owner trust a single telecommunication provider to operate the network and manage subscription of new devices? Will it operate in a specially licensed spectrum for a particular factory, a common publicly allocated spectrum or in new unlicensed bands?

Security in 5G networks remains an open design issue. In 3G and 4G systems, security worked relatively well and was based on traditional symmetric cryptography using authentication with the Authentication and Key Agreement (AKA) protocol. The keys stored in a (U)SIM card and Home Subscriber Server (HSS) require connections to home network while roaming thus exposing the user to tracking and SIM card cloning. Public/private key systems could avoid this with the help of ephemeral key exchange and perfect forward secrecy at the expense of additional overhead in managing certificates and Certificate Authorities. In fact, the critics claim that building a scalable authentication system for the billions of devices had succeeded so far only using traditional symmetric cryptography.

In the industrial setting, providing a physical SIM card identity to each sensor would present a hard logistics and management overhead. Instead, a robust device identity could be provided using software-based SIM or a hybrid architecture with short-range communication from a sensor to a SIM-enabled gateway.

3.3. Network Virtualization or Software Defined Machines

Present industrial environments are largely based on vendor-specific communication protocols that suffer from the lack of interoperability. Visibility of operations over an entire factory is difficult while updating machines is difficult and requires expensive downtime in operations. Thus, deploying integrated and open communication architecture in the Industrial Internet will increase productivity, increase lifespan of machines through their upgradability, and reduce operational costs.

While companies such as GE promote their own solutions including Predix for creating Software Defined Machines (SDM), reliance on open network standards could be helpful to avoid vendor lock in. In the consumer Internet infrastructure, the use of Software Defined Networks (SDN) is quickly changing the landscape of network operations and management. SDN places the intelligence in a centralized controller that connects to switches and routers using a standardized protocol, such as OpenFlow.

Network Functions Virtualization (NFV) takes a forward step from SDN by implementing entire network segments in software running on Virtual Machines. That can include middleboxes such as firewalls, NATs, load balancers, caches as well as switches and routers.

In the latest revision of OpenFlow specifications, 1.5 the use of Transport Layer Security (TLS) to secure the communication between switches and the controller is made optional. The reason for this are configuration difficulties that operators face to configure the certificates correctly. This is a worrisome trend especially if same technology will be applied in the industrial environment to control the machines.

Therefore, it is important to study how current protocols used in industrial automation could be integrated with IP-based OpenFlow standard especially with industrial real-time and security requirements in mind.

3.4. Information Intelligence in Smart Spaces

The characteristic properties of IIS immediately lead to a large-scale system with many data sources, control flows, and service recipients, even in the case of a single enterprise. In addition, dynamics of mobile participants is high; real-time information has short-life relevance; computing environment is subject to frequent changes, failures, and intermittent operation.

This set of problems is close to the generic definition of a smart service, which is considered as information fragment constructed when the need appears and delivered to all appropriate participants (Korzun, 2016). In the IIoT case, construction of such a fragment, even a small one, needs processing of many heterogeneous data sources, e.g., some data sources are from manufacturing processes of machines and others from human activity of personnel. Relations between such data sources cannot be covered by a small set of deterministic scenarios, and more intelligence is needed to realize this way of service construction.

Note that traditionally this construction is made by humans when personnel analyze the system state using the enterprise automation system and traditional communication channels (e.g., phone calls), detect events when control intervention is needed, and make appropriate decisions. This way is slow due to the following reasons: (i) non-fully automated sensing of enterprise edges (including information from remote personnel)

and (ii) the need of human intelligence to analyze the recent situation in the context of its relation to all involved participants and data.

The challenge of information intelligence can be considered as a (partial) automation problem of relation of all involved participants and data for the recent situation. As a result, personnel smaller pieces of processed information and derived knowledge on the events that need control intervention. In fact, reason (i) makes all IIS components closely connected, despite of their physical status (human, thing, or machine) and of location (in control center, in manufacturing department, on transport vehicle, or remote from the subject place). Reason (ii) makes human closer to the informational essence of the situation, when a lot of preliminary information processing is done, and the personnel can focus on the defined problem.

Importantly, this kind of automation does not replace a human by machines. In the IIoT case a smart service describes the situation and provides recommendations. The same description and recommendations can be constructed by a human, while it requires more time. Decision making is still in responsibility of human personnel. Nevertheless, some simple decisions, which have deterministic rules, can be delegated to machines (e.g., temperature control in a manufacturing department).

3.5. Security Requirements or Who Owns the Data?

The ownership of data produced by sensors imbedded to products is an important aspect of the Industrial Internet architecture that needs addressing. From the customer's point of view, they should be in full control of the equipment they purchased for their production environment. However, the equipment supplier may want to retain data ownership produced by machines to be able to sell additional services, such as maintenance, and prevent the customer to purchase third party services. This is especially likely if the machines are not sold but leased according to a service contract. In healthcare, we often observe examples that the patients are not considered owners of their medical records and in some cases are even denied access to data, for instance from Implanted Cardio Defibrillators.

When multiple entities have access to the same set of sensor data, questions of liability and non-disclosure to third parties arise. Such production sensor data can be sensitive and could be disclosed to competitors deliberately or as a result of hacking attacks. Therefore, it appears important to attribute the sensor data to a particular user. Digital water marking had been proposed as a way to mark sensor data individually for each user (Zhang, 2008). Such marking should not affect decisions made by data analytical algorithms but should be retainable even when data is aggregated, samples or transformed during processing. Therefore, developing such watermarking algorithms and their evaluation on industrial data sets appears a promising research area.

4. VPLS Based Cyber-Physical Security Architecture

Network segmentation acts as the first line of defense on mitigating network breaches. It helps to limit the propagation of threats and breaches, to isolate workloads and makes the compliance and audits easier. However, segmentation is a broad term and is not really new. Most of the enterprises have the ability to segment their network traffic for years using IP VPNs (Virtual Private Networks).

Among the different VPN technologies, Ethernet based VPLS networks gained enormous popularity in industrial enterprise networks as convenient, high speed and lost cost virtualization techniques. Initially, VPLS interconnects the premises-wide SCADA (Supervisory Control and Data Acquisition) and process control devices by using the shared networks such as Wi-Fi networks. However, VPLS are now used to interconnect geographically distributed customer sites over wide area networks such as the Internet.

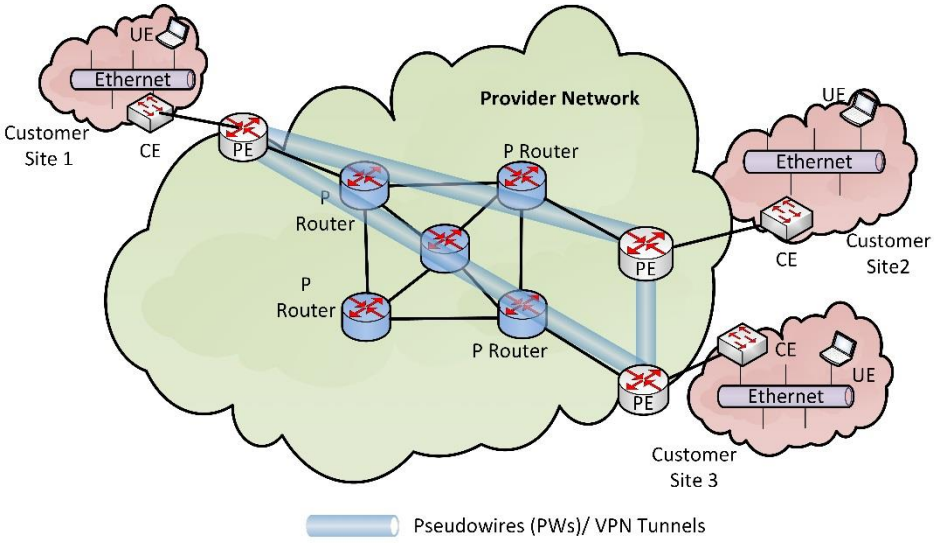

Figure 1: Virtual Private LAN Services

VPLS is a transparent, protocol-independent, multipoint solution to interconnect remote locations over IP or MPLS (Multiprotocol Label Switching) based provider networks. In operation, VPLS offers the same connectivity experienced for all the customer devices as they are attached to the same Ethernet switch regardless of their locations. Moreover, VPLS auto-discovery and service provisioning functions simplify the addition of new sites without interrupting the connectivity for existing sites. A VPLS has five main components namely, User Equipment (UEs), Customer Edge Equipment (CEs), Provider Edge Equipment (PEs), Provider (P) routers and the provider network. PE devices contain all the VPN intelligence. The provider establishes a full mesh of VPN tunnels over the IP/MPLS based provider network to interconnect these PEs. CE devices are the interfacing devices between the customer and provider networks. Moreover, VPLS networks use control protocols to maintain the operation.

Initially, the Internet Engineering Task Force (IETF) defined two standard frameworks to design a VPLS network by using Border Gateway Protocol (BGP) (Kompella, 2007) and Label Distribution Protocol (LDP) (Lasserre, 2007). In (Kompella, 2007), authors proposed a use-case for BGP to establish and maintain a full mesh of VPN tunnels between PEs in VPLS. Here, BGP is used as the control protocol to provide the auto discovery and signaling functions. In (Lasserre, 2007), authors proposed to establish full mesh LDP sessions between PEs in the VPLS. Later, these LDP sessions were used to establish PWs and provide control signaling. A detailed analysis of the deployment and

performance aspects of these frameworks was presented (Gu, 2011). A simplified version of VPLS is proposed as an IP-only LAN Service (IPLS) in (Shah, 2007). The IPLS provides a VPLS-like service and is used exclusively for IP traffic only. All these architectures are flat VPLS architectures and they suffer from various scalability issues.

Hierarchical VPLS architectures are designed to overcome the inherent scalability issues of the flat VPLS architectures. The first functional hierarchical VPLS architecture was proposed in (Lasserre, 2007). Some other research studies also focused on enhancing the features of H-VPLS networks (Cisco, 2011), (Zelig, 2007).

The first secure VPLS architecture was proposed as a Host Identity Protocol (HIP)-enabled virtual private LAN Service (HIPLS) (Henderson, 2011). There, the authors proposed a use-case for HIP to provide a secure VPLS over an untrusted network. HIPLS enables many useful security mechanisms such as authentication, payload encryption, secure control protocol and protection from IP based attacks.

Two advanced versions of HIPLS were proposed as Session key based HIP VPLS architecture (S-HIPLS) (Liyanage, 2014), (Liyanage, 2013) and Hierarchical HIP VPLS architecture (H-HIPLS) (Liyanage, 2015a). Similar to the original HIPLS, S-HIPLS is also a flat VPLS architecture. Here, authors proposed to use a session key based security mechanism to achieve forwarding and security plane scalability for HIPLS. Later, a hierarchical version of S-HIPLS is proposed as H-HIPLS to increase the control plane scalability as well.

Secure VPLS architectures are used in many industrial applications as well, for instance in aerospace (Henderson, 2008). Identity-Defined Networking architecture is based on HIPLS (Tempered, 2016). The performance of open-source secure VPLS architectures and its commercial versions are analyzed in (Liyanage, 2015b).

Due to the simple, protocol-independent and cost efficient operation, VPLS is becoming attractive for IIoT. However, IIoT requires ‘defense-in-depth’. It is implying the idea of creating a multilayered approach to improve security, which is considered the industry best-practice. However, while adding more security layers can help minimize breaches, without flexible network management business operations could be hampered. To prevent this, network segmentation and segregation tools should provide:

- A centralized controller making it easier to apply and manage policies.
- Network programmability to fine-tune the network parameters based on real-time network performance.
- End-to-end encryption with identity-based segmentation over an existing network, without affecting any elements in the path.
- Network-wide monitoring
- Segmentation that allows operators to create policies based on location, network topologies, bandwidth allocation, or various packet transformations services (video transcoding or threat signature scanning).

A novel SDN based VPLS (SoftVPLS) architecture is proposed to provide these new features. SoftVPLS is an advanced approach to design dynamic, manageable, cost-effective, and adaptable networks. SDN plays the key role as an enabler for future 5G

networks. It utilizes OpenFlow switches as PEs and OpenFlow protocol to install flow rules in each PE. Here, VPLS tunnel management functions and network segmentation functions are managed by a centralized controller. SDN offers three new features namely centralized control, network programmability and abstraction (Liyanage, 2015). A dynamic tunnel management mechanism can be developed which estimates the tunnel duration based on real time network statistics provided by PEs. Therefore, the network controller can dynamically change the tunnel duration based on real-time network statistics.

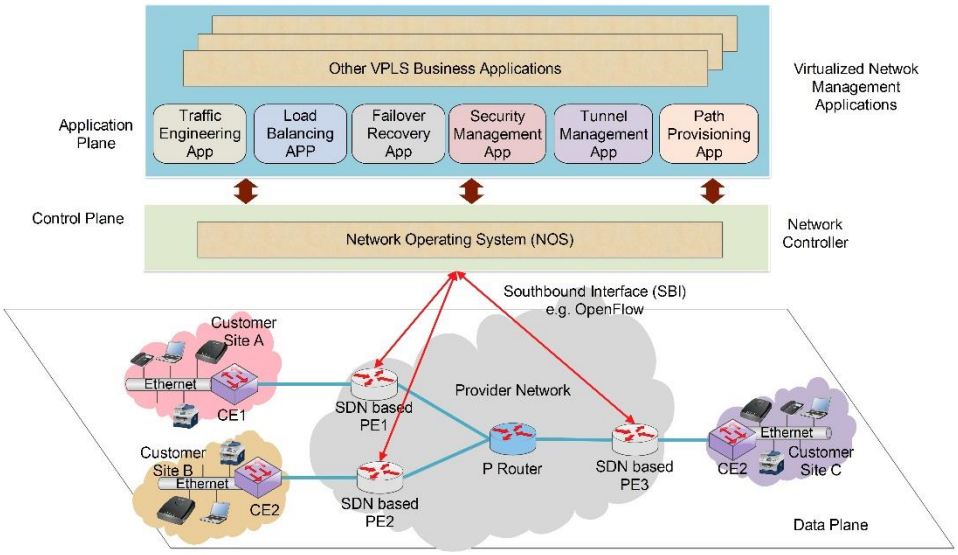

Figure 2: SDN based VPLS Architecture

SoftVPLS architecture also provides the Software Defined Monitoring (SDM) and Software Defined Segmentation (SDS) functions as well. VPLS adds encryption to network segments, while concealing the data traffic. Furthermore, VPLS makes it possible for endpoints to create virtual network connections over the physical network between geographically remote sites making it appear like all devices and services are on the same network segment (regardless of location). These encrypted segments are further partitioned by a host of new tunneling protocols that wrap a UDP packet around our L2 frame so we can break that 4K labeling barrier and allow finer grained partitions. This new form of network segmentation is called overlay tunneling.

Transferring network monitoring functions to a software working in conjunction with configurable hardware accelerators using a scheme called Software Defined Monitoring (SDM) is one promising way to attain the dynamism necessary for the monitoring of the next generation-networks. SDM possesses series of promising features that can well address the limitations of current monitoring solutions.

Software defined segmentation (SDS) is a software-defined network (SDN) tool used to segment network elements. These elements can be identified and trusted, and therefore authorized to establish peer connections with path assurances which include network cloaking and military grade encryption. These software segments allow to

dynamically manage the network using APIs (Application Programmable Interface), enabling greater control and visibility.

The described architecture is being prototyped and validated in (Tempered, 2016) (Liyanage, 2016), which combines SDN-style secure networking architecture with centralized GUI management.

5. Smart Spaces for the Industrial Internet

Our approach to development of IIoT services is creating an intelligent environment in the form of a smart space deployed for a given IIS. As a result, the services are constructed with cooperative knowledge processing over information shared in the smart space. In this section, we introduce a concept model of a smart space deployed in IIoT environment. We discuss the opportunities that this concept provides for IIS development.

The common approach for industrial automation is employing an enterprise information system (EIS) (Olson, 2010), as Figure 3 shows. There are two kinds of resources: human resources (personnel) and industrial equipment. These resources are combined to implement technological processes of product development, following the enterprise business and technology logic. The global-state information on the processes is accumulated in the EIS database. Therefore, global planning and corresponding control become possible and in the automated manner. In turn, the resources are applied in accordance with the current plan and control decision-making from the planning and control processes.

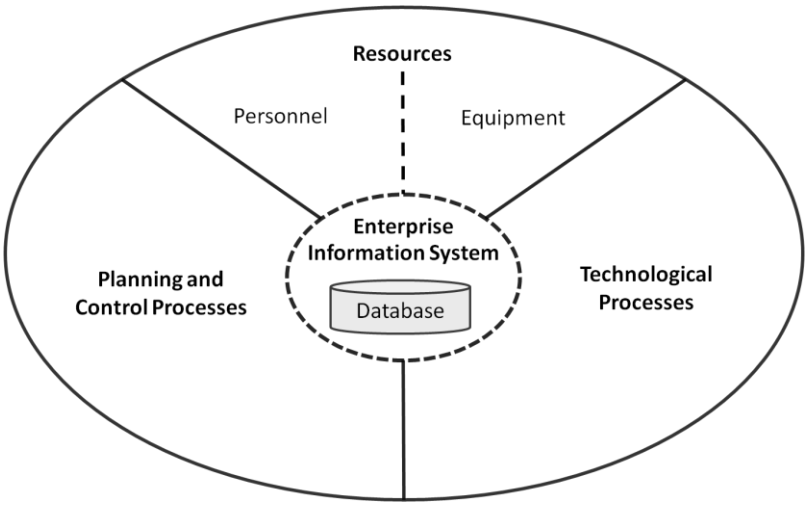

Figure 3: EIS integrates and coordinates business processes

We propose to enhance this EIS approach using a smart space deployed in the IIoT environment. In general, a smart space is an information-centric extension of the IoT-aware connection of physical and virtual objects (Korzun , 2016). The extended system

is called a smart environment or an intelligent environment (Augusto, 2013), (Cristea, 2013). It enables information sharing in a given IoT environment, supporting construction of advanced digital services by the participants themselves. The term "smart" or "intelligent" means that any participant of the environment can make decisions (in the service form of information provision), which are based on knowledge derived from the whole environment (i.e., due to activity of many participants), not on local observations only. Such services are also referred as "smart", emphasizing the new level of service recognition (detection of user needs), construction (automated preprocessing of large data amounts), and perception (derived information provision to the user for decision-making).

For the case of IIoT environment, the concept model of a smart space for IIS is shown in Figure 4. Being deployed the smart space introduces the semantic layer to share all related semantic information by participants themselves (see the information intelligence challenge in Section 4). Enterprise resources, technological processes, EIS, and planning and control processes become smart space participants represented by their software agents. This way, the participants are connected into information sharing cyber-physical system. The connection efficiency is due to the IoT communication technology, primarily including wireless and mobile communication.

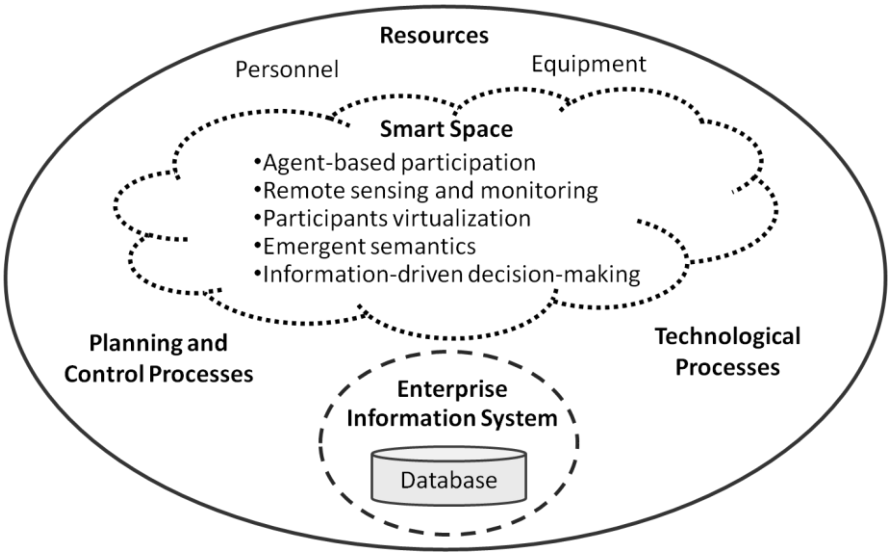

Figure 4: Enhancing the EIS approach: a smart space deployed in the IIoT environment

This smart space approach supports the characteristic properties from Section 3. Participation of all interested parties is achieved using the agent-based operation: integration of a new object needs a corresponding agent that acts on behalf of the object. Some agents are associated with sensors, leading to sensing automation.

Some participants have explicit representation in the smart space, forming a virtual online description of ongoing processes. Although the sensed data are collected in the appropriate modules of the EIS database, the smart space accumulates semantics of the

sensed data, i.e., the case of emergent semantics. The semantics are also represented in the form of relations between information objects stored in the smart space. This virtual representation augmented with the semantics and linked with the database meets big data analytics, and some smart space participants can represent data-processing services from cloud systems.

The knowledge derived by the participants can be iteratively shared in the smart space, supporting information-driven decision-making by the participants that represent planning and control processes. This way of decision-making follows the control intelligence property when the participants construct recommendation and deliver them as services to the personnel.

According to the general communication architecture discussed in Section 4, most of SmartSpace components would be running in a cloud, connected using VPLS to the industrial network which collects sensor data from machinery. However, quick decisions on sensor data requiring low-latency communication are best done close to the industrial network. Therefore, smart space architecture should be partitioned into real-time processing and longer-term data analysis components.

6. Conclusion

In this paper, we described and analyzed the secure communication and data processing challenges for the upcoming Industrial Internet which is foreseen as a new revolution in manufacturing efficiency and flexibility. Realizing the Industrial Internet requires novel technologies including 5G wireless networks, software defined networking and digital watermarking of sensor data. Furthermore, we argued for the need of in-depth rather than perimeter-based network security for Industrial Internet, and described a communication architecture based on Virtual Private LAN Services. Finally, smooth delivery of massive sensor data to cloud infrastructure for storage and processing is best facilitated by applying the concept of smart spaces.

As the Industrial Internet is a new research area, this paper only outlined the main challenges in communication and data intelligence. More work is needed to experiment, develop, standardize and formalize the architecture of the Industrial Internet. We are presently expanding our VPLS and sensor test lab with capabilities to experiment with wide-area SDN, long-range sensor communication, wireless cognitive networks and encrypted data processing in the clouds.

Acknowledgments

This applied research is financially supported by the Ministry of Education and Science of Russia within project # 14.574.21.0060 (RFMEFI57414X0060) of Federal Target Program “Research and development on priority directions of scientific-technological complex of Russia for 2014–2020”.

References

Augusto J., Callaghan V., Cook D., Kameas A., Satoh I. (2013). Intelligent environments: a manifesto. Human-centric Computing and Information Sciences, vol. 3, no. 1.

Bruner J. (2013). Industrial Internet. The machines are talking. O'Reilly.

Cisco (2011). H-VPLS N-PE Redundancy for QinQ and MPLS Access. Technical report, CISCO Corporation.

Cristea V., Dobre C., Pop F. (2013), Internet of Things and Inter-cooperative Computational Technologies for Collective Intelligence. Springer Berlin Heidelberg, ch. Context-Aware Environments for the Internet of Things, pp. 25–49.

Domingo M.C. (2012). An overview of the internet of things for people with disabilities. Journal of Network and Computer Applications. Vol. 35, Issue 2, pp. 584–596.

Evans, P. C., Annunziata M. (2012). "Industrial internet: Pushing the boundaries of minds and machines." General Electric White Paper.

Gu R., Dong J., Chen M., Zeng Q., Liu Z. (2011). Analysis of Virtual Private LAN Service (VPLS) Deployment. Internet Draft.

Han S., Lee G., Crespi N. (2014). Semantic context-aware service composition for building automation system. IEEE Transactions on Industrial Informatics. Vol. 10, Issue 1, pp. 752–761.

Henderson T. (2008). Boeing HIP Secure Mobile Architecture. [Online]. Available: http://www.ietf.org/proceedings/73/slides/HIPRG-0.pdf

Henderson T., Venema S., Mattes D. (2011). HIP-based Virtual Private LAN Service (HIPLS).

Hu C., Yuan C., Liu K. et al. (2009). Enhanced H-VPLS service architecture using control word. US Patent 7,570,648.

Juniper (2010). DEMYSTIFYING H-VPLS. Technical report, Juniper Networks, Inc.

Soderi S., Viittala H., Saloranta J., Hamalainen M., Iinatti J., Gurtov A. (2013). Security of Wi-Fi On-board Intra-vehicular Communication: Field Trials of Tunnel Scenario, in proc. of ITST.

Tempered Networks (2014). Secure Your Oil & Gas Production Environment, White paper. http://www.temperednetworks.com/docs/TemperedNetworks-OilGas-UseCase.pdf

Karakostas B. (2013). A DNS architecture for the internet of things: A case study in transport logistics. Procedia Computer Science. Vol. 19, pp. 594–601.

Khandekar S., Kompella V., Regan J., et al. (2002). Hierarchical Virtual Private LAN Service. Internet Draft.

Kompella K., Rekhter Y. (2007). Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling. RFC 4761

Korzun D. (2016). On the Smart Spaces Approach to Semantic-driven Design of Service-oriented Information Systems. In Proc. 12th Int'l Baltic Conf. on Databases and Information Systems (DB&IS 2016), G. Arnicans et al. (Eds.). Springer International Publishing, CCIS 615, pp. 1–15.

Kortuem G., Kawsar F., Sundramoorthy V., Fitton D. (2010). Smart objects as building blocks for the internet of things, IEEE Internet Computing, vol. 14, no. 1, pp. 44–51.

Kuptsov D., Khurri A., Gurtov A. (2009). Distributed authentication architecture in Wireless LANs, in Proc. of the 10th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM'09).

Lasserre M., Kompella V. (2007). Virtual private LAN service (VPLS) using label distribution protocol (LDP) signaling. RFC 4762.

Liyanage M., Gurtov A. (2014). Securing virtual private LAN service by efficient key management. Security and Communication Networks 7(1): 1–13.

Liyanage M., Gurtov A. (2013). A Scalable and Secure VPLS Architecture for Provider Provisioned Networks. In: IEEE Wireless Communication and Networking Conference: WCNC 2013.

Liyanage M., Ylianttila M., Gurtov A. (2016). Improving the Tunnel Management Performance of Secure VPLS Architectures with SDN. in Proc. of 13th IEEE Annual Consumer Communications & Networking Conference (CCNC): 530-536

Liyanage M., Ylianttila M., Gurtov A. (2015). Secure Hierarchical VPLS Architecture for Provider Provisioned Networks. Access, IEEE 3: 967–984.

Liyanage M., Ylianttila M., Gurtov A. (2015). Software Defined Mobile Networks (SDMN): Beyond LTE Network Architecture, Wiley and Sons

Liyanage M., Ylianttila M., Gurtov A. (2013). Secure Hierarchical Virtual Private LAN Services for Provider Provisioned Networks, in Proc. of 1st IEEE Conference on Communications and Network Security'13.

Liyanage M., Okwuibe J., Ylianttila M., Gurtov A. (2015). "Secure Virtual Private LAN Services: An Overview with Performance Evaluation," in IEEE ICC 2015 - Workshop on Advanced PHY and MAC Techniques for Super Dense Wireless Networks. IEEE, pp. 1–7

Olson D.L., Kesharwani S. (2010). Enterprise Information Systems: Contemporary Trends and Issues. World Scientific.

Pang Z., Chen Q., Han W., Zheng L. (2015). Value-centric design of the internet-of-things solution for food supply chain: Value creation, sensor portfolio and information fusion. Information Systems Frontiers. Vol. 17, Issue 2, pp. 289-319.

Perera C., Zaslavsky A., Christen P., Georgakopoulos D. (2014). Context Aware Computing for the Internet of Things: A Survey. IEEE Communications Surveys & Tutorials. Vol. 16, No. 1, pp. 414–454.

Shah H. ER., Heron G. (2007). IP-Only LAN Service (IPLS). Internet Draft.

Sodder A., Ramakrishnan K., DelRegno C., Wils J. (2003). Virtual Hierarchical LAN Services. Internet Draft.

Tempered Networks (2016). [Online]. Available: http://www.temperednetworks.com/

Wang J., Zhu Q., Ma Y. (2013). An agent-based hybrid service delivery for coordinating internet of things and 3rd party service providers. Journal of Network and Computer Applications. Vol. 36, issue 6, pp. 1684–1695.

Xu L.D., He W., Li S. (2014). Internet of Things in Industries: A Survey. IEEE Transactions on Industrial Informatics. Vol. 10, Issue 4, pp. 2233-2243.

Zelig D., Bruckman L., Kotser Y (2007). Hierarchical virtual private LAN service protection scheme. US Patent 7,283,465.

Zhang W., Liu Y., Das S. K., De P. (2008). Secure data aggregation in wireless sensor networks: A watermark based authentication supportive approach, Pervasive and Mobile Computing, Volume 4, Issue 5, Pages 658-680, ISSN 1574-1192, http://dx.doi.org/10.1016/j.pmcj.2008.05.005.

Authors' information

Andrei Gurtov is an associate professor at Linkoping University and an adjunct professor at Aalto University, University of Helsinki, and University of Oulu. He is also a scientific leader of ITMO University's SCA Research Lab. His research interests include Internet protocols, peer-to-peer communication, Industrial Internet, and wireless and sensor network security. Gurtov received a PhD in computer science from the University of Helsinki. He visited ICSI in Berkeley multiple times. He is an ACM Distinguished Scientist, IEEE ComSoc Distinguished Lecturer and Vice Chair of IEEE Finland section.

Madhusanka Liyanage is a project manager at the Centre for Wireless Communications, University of Oulu, Finland. His research interests are SDN, 5G, NFV, mobile networks, VPNs and network security. He received the B.Sc. (2009) degree in electronics and telecommunication engineering from the University of Moratuwa, Sri Lanka, the M.Eng. (2011) degree from the

Asian Institute of Technology, Thailand and the M.Sc. (2011) degree from University of Nice Sophia Antipolis, Nice, France. In 2016, Liyanage received a PhD in communication engineering from the University of Oulu, Finland. In 2011-2012, he was a research scientist at I3S Laboratory and INREA, Sophia Antipolis, France. He is a co-author of over 30 publications including one edited book with Wiley. He is also a management committee member of EU COST Action IC1301, IC1303, CA15107 and CA15127 projects.

Dmitry Korzun received his B.Sc. (1997) and M.Sc (1999) degrees in Applied Mathematics and Computer Science from the Petrozavodsk State University (PetrSU, Russia). He received Ph.D. degree in Physics and Mathematics from the St.-Petersburg State University (Russia) in 2002. He is an Associate Professor at the Department of Computer Science of PetrSU (since 2003). Previously he was a part-time Research Scientist at the Helsinki Institute for Information Technology HIIT, Aalto University, Finland (2005-2014). Since 2014 he acts as Vice-dean for Research at the Faculty of Mathematics of PetrSU (now Faculty of Mathematics and Information Technology) of PetrSU and as Leading Research Scientist. Dmitry Korzun serves on technical program committees and editorial boards of a number of international conferences and journals. His research interests include analysis and evaluation of distributed systems, discrete modeling, ubiquitous computing and smart spaces, Internet of Things, software engineering, algorithm design and complexity, linear Diophantine analysis and its applications, theory of formal languages and parsing. More than 150 research and educational works have been published since 1997.

Received September 28, 2016, accepted November 29, 2016