Approach for Securing Network Communications Modelling Based on Smart Multipath Routing

A. D. Dakhnovich,^{*} D. A. Moskvina,[†] and D. P. Zegzhda[‡]
*Peter the Great St. Petersburg Polytechnic University,
29 Polytechnicheskaya Str, 195251 St. Petersburg, RUSSIA*
(Received 18 August, 2020)

Digital transformation, or Industry 4.0, is already changing manufacturing processes as it brings more automation to standardized Industrial Control Systems (ICS) based systems such as Supervisory Control and Data Acquisition (SCADA) systems. It is performed by the means of cyber-physical systems such as Internet of Things (IoT). For now, these “Things” are communicating in a new network area, where peer-to-peer communications are widely used. Such networks are responsible for real life processes safety. However, such shift also extends a threat vectors and entry points for an adversary inside the industrial segments. In the paper, new cybersecurity challenges on the Industrial Internet of Things network segments are considered as well as known practices to mitigate some of them. As a result, a peer-to-peer smart multipath network routing based on garlic routing is proposed to model secure network communications in IoT field. An approach is aimed to be used on the IoT field to tackle all of the network-scoped cybersecurity challenges.

AMS Subject Classification: 68M10, 68M12

Keywords: digital manufacturing, smart manufacturing, industrial control system, internet of things, cyber-physical systems, scada

DOI: <https://doi.org/10.33581/1561-4085-2020-23-4-386-396>

1. Introduction

Industrial Internet of Things (IIoT) is becoming a new standard to automate manufacturing, make it predictable and cost-efficient. In context of cybersecurity, IIoT is considered as a network segment based on a Cyber-Physical System (CPS) and the appliance of Information Technologies (IT). It also can be treated as a replacement of the Control network, or Level 0, which is mentioned in standards like NIST SP 800-82 [1], SANS and ICS-CERT.

To understand cybersecurity issues in the IIoT main differences between IIoT and Industrial Control Systems should be considered. The IIoT systems are a convergence of IT and OT technologies. The NIST SP 800-82 standard and IIC IIRA document, as well as Zegzhda *et*

al. [2], describe clearly differences between OT-systems such as ICS and IT-systems. In the paper, following ones are taken into account as they affect on communications requirements and cybersecurity challenges:

- ICS is a real-time system, while IT is not;
- ICS availability and reliability requirements are significant;
- ICS use many proprietary and standard communication protocols and IT only standard TCP/IP stack;
- ICS software maintenance and service support usually done via a single vendor while IT-systems allow diversified support styles.

Thus, these differences are also valid for IIoT and ICS comparison. The incidence of the IT-systems into the OT-systems also changes the

^{*}E-mail: add@ibks.spbstu.ru

[†]E-mail: moskvina@ibks.spbstu.ru

[‡]E-mail: dmitry@ibks.spbstu.ru

FIG. 1. (color online) IIC IIRA function domains and control flows.

place where the decisions and control commands are made. That means that in IIoT some of base intellectual decisions are made on network gateways or even on IoT-devices.

The IIC IIRA [3] identifies five functional domains, where the lowest, Control domain, is highly autonomous and gets control commands as the input, corrects physical processes, and brings the result back to the Information domain for decision-making (Figure 1).

The IIoT Control domain is highly autonomous due to the benefits that IoT ecosystems can provide. The IoT segment layout has no standard for now but usually treated as the network of specific gateways, IoT-devices and communications between them. The NIST SP 800-183 [4] authors give the view on how such segment can look like (Figure 2).

Thus, in the IIoT there are two main assets that must be secured: endpoints and networks between them. Endpoint security is out of the scope of this paper and can be explored in documents and standards like IIC Security Framework, ISA/IEC 61508 series and ENISA

Baseline Security Recommendations for CII [5] etc. In this research network security threats and communication security challenges are taken into account as the main threat vectors for remote adversary to influence on the industrial processes.

In the paper, based on main differences between ICS and IIoT systems mentioned in the introduction, cybersecurity issues, threats and challenges while manufacturing transformation are mentioned (Section 3). Then some known practices to mitigate them are pointed out (Section 4). After that new method based on peer-to-peer garlic routing is proposed (Section 5).

2. Related works

As the Internet of Things becomes the main conception of Digital Manufacturing deployment there are several research works around the IoT security challenges. Sadeghi *et al.* [6] describes new attack vectors in the Industrial Internet of Things and the main security challenges in CPS are building secure architecture, provide integrity verification of CPS and secure IoT device management. Varga *et al.* [7] in a research gives comprehensive list of security issues in automation of IoT and propose a new layered approach to address attacks on each level.

Some researchers also consider a necessity of a new secure architecture as IoT segments require to exchange information through boundaries. Sajid *et al.* [8] in his research describes security issues in utilization of SCADA systems based on IoT segment and backed with a Cloud services and gives some methods to mitigate these issues. Ulltveit-Moe *et al.* [9] also consider problems of secure information sharing caused by collaboration between stakeholders, integrators and developers of IoT devices. Xu *et al.* provides a view on a current state of the IoT in Industry context, where a challenge of providing Quality of Service on a network layer of IoT systems takes its place.

FIG. 2: (Color online) NIST SP 800-183 “Network of Things” architecture.

3. IIoT threat model

The main cybersecurity challenge for ICS systems is to provide its function safety [10]. Already there are standards and documents that describes clearly how to implement ICS properly: already mentioned NIST, SANS and ICS-CERT publications, as well as ISA/IEC 61508 series. The information security issues are not considered in ICS a lot due to the attack vectors and threat sources: in ICS the only information attack vectors without physical access to the Control domain is improperly configured network gateway, such as firewall, that provides network segmentation and segregation of Control, Plant, and Enterprise network segments. Any other harmful influence on the ICS, such as viruses or systems outages, could be gained via physical presence inside the perimeter: infected PLC logic; infected USB-devices; insecure local communications etc (Figure 3). As it could be notices, network attacks are not the real

problem in the ICS context and are reduced to network gateway tampering from the outside and physical access to local network bus for the inside adversary.

FIG. 3. (color online) ICS information threats vectors.

For IIoT systems, such threat vectors are also valid. However, in addition to them, new threats are actual when the manufacturing leverages IoT ecosystem. The ENISA Baseline

Table 1: Security measures to mitigate IIoT threats.

Threats	Technical measures
Counterfeit by malicious devices	Endpoint authentication via routing tables
DDoS	P2P architecture
Network reconnaissance and information gathering Information interception and hijacking Replay and delay of messages	Network access control; Secure and trusted communications: data authenticity via device trust management, CIA of data in transit via cryptography methods (e.g. TLS protocol); Communication channels isolation into control, data and management channels.
Software/system failures and vulnerabilities	Secure software / Firmware updates via patch-management;
Network outage	Communication channels redundancy (e.g. via peer-to-peer networking or distributed systems)

FIG. 4: (color online) The IIoT threat vectors.

security recommendations for CII provides a comprehensive view on the threat taxonomy.

The list of threats weighed in the paper is divided into three sections (Figure 4):

- malicious activities;
- network attacks;
- outages.

Malicious activities include following threats:

- counterfeit by malicious devices;
- DDoS.

Network attacks include following threats:

- network reconnaissance and information gathering;
- information interception and hijacking;
- replay and delay of messages.

Outages include following threats:

- software/system failures and vulnerabilities;
- network outage due to interruption or failures in the network supply or physical attacks on some of the communication channels.

Technical measures to prevent described threats do exist.

4. Cybersecurity challenges and existing technical measures to meet them

While organizing IIoT-driven manufacturing there are not only actual cybersecurity threats but also some challenges to be meet and requirements to satisfy.

4.1. IIoT cybersecurity challenges

Comparing to ICS production equipment, there are some novation in security requirements. First, any IoT-device must support lightweight cryptography. Another requirement is to have separated channels for information flows:

- management channel for endpoint device management;
- data channel for data gathering from the Control domain to the Information domain;
- control channel for control commands dispatching from the Operations domain to the Control domain.

Providing IIoT and CPS systems sustainability and resilience is also a cybersecurity challenge. It is considered as the main challenge in Stepanova *et al.* [11], Pavlenko *et al.* [12], and Zegzda *et al.* [13] works that are devoted to mark sustainability as the new criteria for CPS cybersecurity estimation and to provide new approaches of ensuring CPS resilience. Resilience is a property of the system to perform its assigned mission operations while adversarial influence. From the point of network attacks resilience is provided via network redundancy to provide data delivery assurance. One of the approaches is to use peer-to-peer networking pattern to ensure communication channels redundancy.

Peer-to-peer networking is also recommended by IIC Security Framework. For now, event-driven messages with broker-centered servers and gateways are used to gather data from IoT-devices. However, centralized broker is a single point of failure. So distributed mechanisms are preferred. One of such technologies is Data Distribution Service (DDS), a brokerless implementation of publisher-subscriber data messaging.

Except already mentioned IIC document, the peer-to-peer networking and mesh-networks is considered as a main routing pattern in IIoT

by other researchers, e.g., Germanus *et al.* [14], Li Da Xu *et al.* [15].

One of the significant abilities that IIoT networks should support is a fine-grained access control. This problem is also pointed in Sadeghi *et al.* [6], Ulltveit-Moe *et al.* [9], Sajid *et al.* [8] works. Such ability could be used in prospect for secure software and firmware updates, e.g. from the Enterprise tier or from multiple vendors as a part of a support program, and resource sharing, e.g., in supply chains, or by multiple factories that uses same production equipment.

4.2. Cybersecurity technical measures

There are some known practices and requirements to mitigate these issues that are also described in ENISA Baseline Security Recommendations and IIC Security Framework (Table 1).

5. Proposed method

To tackle such security requirements a new method for peer-to-peer network between IoT-devices is proposed. The method is based on garlic routing and is trying to accomplish all of the mentioned in Section 4 security requirements and meet cybersecurity challenges.

5.1. Garlic routing terminology

FIG. 5: (color online) Garlic routing concept.

The mathematician Mikel Freedman described the terms “Garlic Routing” and “Garlic Encryption” in the year 2000. Garlic encryption is built on an Onion routing principals, where only the receiving node can decrypt packets addressed to it thus unchaining one layer of the onion packet. However, the main difference is that in garlic routing all packets, called “cloves”, are encrypted separately by each sender and then packed in a one with a fixed size, called “garlic”, while sending between nodes (Figure 5).

Then “garlic” packet is encrypted entirely by each node of the network graph as in the Onion routing scheme. Every clove message is unpacked and decrypted only on the receiving node so any other participants cannot read it. They can only retranslate it to the next hop of the network. The main appliance of Garlic routing for now is an I2P overlay network where this technic provides anonymity of any clients and servers (in terms of I2P called nodes), as well as defence against traffic analysis (Figure 6).

Thus, to secure communications between to clients and servers I2P network utilizes information security methods listed below:

1. Appliance of public key cryptography for data encryption and signing node data (every node has its own two pairs of public and private keys).
2. Appliance of multi-layered onion-like encryption for outgoing and ingoing tunnels, where every node can decrypt only its own layer.
3. Different tunnels for outgoing and ingoing channels are utilized, where the second one is used for notifications about delivery status of messages sent through the outgoing tunnel. Every tunnel has its own life time.
4. Every packet, called “garlic” transferred between nodes through tunnels, consist of multiple messages, called “cloves”.

Thus I2P network mitigates cyberattacks:

1. Man-in-the-Middle by data encryption and signing.
2. Attacks concerned with the data amount analysis technics and timing attacks, as every “clove” has its own addressee and is transferred via temporary tunnels that have short living time.

5.2. Appliance for securing IIoT communications

Information security methods provided by garlic routing can be slightly used for securing IIoT communications and meet cybersecurity challenges. However, its implementation in the I2P network must be adjusted to meet specifics of manufacturing challenges. The proposed method can be used inside one network segment as well as between them to provide fine-grained access to the IoT-devices.

Let us consider the following scenario: two network segments i and j need to link some of their endpoint devices (nodes) to each other but not all. So the whole network could be considered as the Mesh-network which is a graph of network nodes (endpoint devices) (Figure 7).

Network segment here is treated as a group of devices that use similar routing tables or a particular endpoint device that stores the routing tables by its own (Figure 8).

Every segment i should control two tables for each communication list to another segment j :

1. Outbound table – list of remote segment j nodes addresses that current segment i can communicate with. This table must be synchronized with the corresponding inbound table of the remote segment j .
2. Inbound table – list of current segment i nodes that the remote segment j can communicate with. This table must be synchronized with the corresponding outbound table of segment i .

FIG. 6: (color online) I2P routing scheme.

FIG. 7. (color online) Segments and endpoints in IIoT.

Inbound table «Field»	
P-1	...
P-2	...
P-3	...
P-6	...
Outbound table «Field»	
S-1	...
S-3	...
S-5	...

FIG. 8. (color online) Segments and endpoints routing tables.

The address in any table is the match between the network address (e.g. IP-address) and two public keys. If node k of segment i can send data to the node l of the remote segment j then in routing table of segment i will have entry two public keys: PK_{jl} and PK_{ik} . The key PK_{jl} is the public ciphering key of the node l from segment j and is used for data encryption sent only to the node l . Key PK_{ik} is the public signing key of node k from segment i and is used for signature verification when data is transferred from node k to the current node. E.g., the outbound routing table of segment i will contain such entry:

$$RA_{jlik} = (PK_{jl}, PK_{ik}),$$

where RA_{jlik} is a remote address of node l from segment j that node i from segment k can send information to; PK_{jl} and PK_{ik} are public keys, the first one is the public key of node l from segment j for data encryption, the second is the public key for signature of node k from segment i verification.

The PK_{jl} and PK_{ik} keys should be synchronized with the remote Inbound table entry in segment j for correct integrity checking and data decryption. Thus, the corresponding Inbound table of segment j will have the same entry:

$$RA_{ikjl} = (PK_{ik}, PK_{jl}),$$

where RA_{ikjl} is the address of the node l from current segment j that the node k from the remote segment i can send information to.

When the node receives packet, it takes only the message that is addressed to it by decrypting the headers. Other packets are transferred further to another nodes and instead of the received packet another packet is inserted (empty or not depending on the current state of particular node).

5.3. Method advantages

The proposed method implements on the architectural level cybersecurity technical measures that is a big benefit and can accelerate implementation of digital manufacturing (Table 2).

Firstly, network based on garlic routing principals is implemented as a P2P-network, protects from single point of failure and, thus, network outage. Each message can be routed through the available for the particular segment nodes. Also P2P-architecture implements load-balancing by itself so messages will not be sent only through the one physical channel. Thus, this measure protects from network outage and DoS/DDoS attacks on the IoT-infrastructure.

This option also minimizes message interception threat and gives an opportunity to set time limit on message delivery. When the message is sent, a sender waits for the delivery status message. This message is send back via different route from the receiver to the sender also to tackle network threats. If delivery status message is not received, the sender routes message through another available route. So, each message delivery time and status is controlled by sender and receiver. Thus, method protects against replay and delay of messages.

Each message is only a small fixed-sized piece of data. So if one endpoint communicates with another endpoint and sends vast amount of data, it will be partitioned into small messages ("cloves"). As this messages are sent via different

routes, information cannot be gathered by an adversary listening somewhere on the network communication channel. Thus, method provides defense against information gathering.

Each packet consists of multiple messages of the fixed size cyphered with an according to each message key. Thus, each packet which is transferred via network has also a fixed size, so, method provides protection against network reconnaissance from internal as well as external adversary.

Used in I2P network cryptography methods can also be implemented in IIoT garlic routing scheme. This will meet a data-in-motion cryptography protection requirement: data is encrypted with the usage of public key of one key pair to ensure it will not be disclosed while transferring; data is digitally signed with a private key of another key pair to guarantee its integrity so any data modification while transferring will be noticed. Thus, method provides protection against MitM-attacks, data leakage and information hijacking.

5.4. Perspectives of the proposed method

As the method implements routing tables where each device has its own pair of keys. This keys are used to identify each endpoint in the network. So access control from the nodes and segments to the network is provided "out-of-the-box". Moreover, such routing tables and device authentication will bring a fine-grained access control between endpoints: even if network segment i consists of N nodes, access for the segment j nodes can be granted not for all of them, but only for $n \in N$ without the particular network features and technical processes disclosure. Thus, granting access to the network endpoints does not lead to network reconnaissance. This scenario can be used to isolate communication channels into control, data and management, and thus, can be used to secure software and firmware updated.

FIG. 9: (color online) Fractalizing garlic routing architecture.

The garlic routing is originally used in the I2P network, which is an overlay network. This option can also be treated as an advantage while implementing IIoT network on existing manufacturing. There are terms like greenfield and brownfield, that are also used by IIC Security Framework. Greenfield means that the IIoT network is built from the ground without the usage of legacy devices. Brownfield, on the contrary, is an approach when the digitalizing of the technical processes is going slightly. In practice, brownfield approach will be used wider as existing ICS systems will be adopted to the IIoT not in one day. So, the endpoints that are working on different communication protocols will be taken into account for some time. Garlic routing overlay nature can also tackle this problem as it does not depend on particular network protocol.

While IoT infrastructures and Cloud-based services for data management will grow up, the proposed method can be extended in fractal manner, i.e., garlic routing can meet cybersecurity

challenges also if it will be implemented on geographically distributed communication systems. The network can be scaled the way where each segment can be treated as an endpoint and organize garlic routing segments of the higher order (Figure 9).

In perspective garlic routing can be implemented upon the DDS messaging system as its security extension with some additional components such as routing tables (Table 2).

Table 2: Garlic routing security measures to mitigate IIoT threats.

Technical measures	Multipath routing mitigation technic
Network access control	Endpoint authentication via routing tables
Load balancing; Communication channels redundancy	P2P architecture
Network reconnaissance and information gathering	Endpoint authentication via routing tables; End-to-end encryption between communicating nodes; Communication channels isolation with fine-grained access control via routing tables; Fixed packet (garlic) and messages inside (cloves) sizes
CIA of data in transit via cryptography methods	End-to-end encryption between communicating nodes; Digital signature; Message delivery status notification
Secure software / Firmware updates	Communication channels isolation with fine-grained access control via routing tables

6. Conclusion

The paper is aimed to consider main cybersecurity challenges and threats which are actual for the new digital factories. These challenges usually cannot be tackled with common and well-known practices that were utilized in IT or OT networks separately, thus, new approaches occur. One of the approaches based on the appliance of anonymous network garlic routing model is proposed in the paper. This routing model and its security measures are appropriate for cybersecurity challenges which is shown in paragraphs above and it can substitute multiple technical solutions, such as redundant channels, firewall and cryptographic

gateways, VPN, access control systems and VLAN networking only by itself. Further works will focus on estimating of the method applicability on real systems via building programs for routing equipment.

Acknowledgements

The reported study was funded as the part of the State Task for Basic Research (code of theme: 0784-2020-0026); suppl. agreement to the Agreement for the financial support No.075-03-2020-158/2, 17.03.2020 (internal No.075-GZ/SCH4575/784/2).

References

- [1] K. Stouffer, V. Pillitteri, S. Lightman. *Guide to Industrial Control Systems (ICS) Security*. NIST Special Publication 800-82 rev.2. (2015).
- [2] Yu.S. Vasil'ev, D.P. Zegzhda, M.A. Poltavtseva. Problems of security in digital production and its resistance to cyber threats. *Automatic Control and Computer Sciences* **52**, no. 8, 1090–1100 (2018).
- [3] S. Lin, M. Crawford, S. Mellor. The Industrial Internet of Things Volume G1: Reference Architecture. Automatic Control and Computer Sciences. (2017).
- [4] J. Voas. Network of “Things”. NIST Special Publication 800-183 (2016).
- [5] M. Ross, T. Hannes, A. Jara. *Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures*. (2017).
- [6] A. Sadeghi, C. Wachsmann, M. Waidner.

- Security and privacy challenges in industrial Internet of Things. In: *52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*. Pp. 1–6 (2015).
- [7] P. Varga *et al.* Security threats and issues in automation IoT. In: *IEEE 13th International Workshop on Factory Communication Systems (WFCS)*, 2017. Pp. 1–6 (2017).
- [8] A. Sajid, H. Abbas, K. Saleem. Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges. *IEEE Access* **4**, 1375–1384 (2016).
- [9] N. Ulltveit-Moe *et al.* Secure Information Sharing in an Industrial Internet of Things. ArXiv abs/1601.04301 (2016).
- [10] D.P. Zegzhda, E.Yu. Pavlenko. Digital manufacturing security indicators. *Automatic Control and Computer Sciences*. **52**, no. 8, 1150–1159 (2018).
- [11] D. Zegzhda, T. Stepanova. Achieving Internet of Things security via providing topological sustainability. 2015 Science and Information Conference (SAI), Pp. 269–276 (2015).
- [12] E. Pavlenko, D. Zegzhda. Sustainability of cyber-physical systems in the context of targeted destructive influences. 2018 IEEE Industrial Cyber-Physical Systems (ICPS), Pp. 830–834 (2018).
- [13] D. Zegzhda. Sustainability as a criterion for information security in cyber-physical systems. *Automatic Control and Computer Sciences*. **50**, no. 8, 813–819 (2018).
- [14] D. Germanus, A. Khelil, N., Neeraj. Increasing the Resilience of Critical SCADA Systems Using Peer-to-Peer Overlays. *Architecting Critical Systems*, Pp. 161–178 (2010).
- [15] L.D. Xu, W. He, S. Li. Internet of Things in Industries: A Survey. *IEEE Transactions on Industrial Informatics*. **10**, no. 4, 2233–2243 (2014).