This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Call: FP7-SEC-2013-1
Activity: SEC-2013.2.5-4: Protection systems for utility networks – Capability Project
Project Number: 608090

HyRiM

Hybrid Risk Management for Utility Networks

Collaborative Project

Deliverable 4.2
Guidelines on surveillance technologies to secure utility networks

Due date of deliverable: 31-03-2016
Actual submission date: 02-05-2016

Start date of project: April 1, 2014 Duration: 36 months

Organisation name of lead contractor for this deliverable
University of Passau

Dissemination Level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

HISTORY

Version	Date	Reason	Reviewed by
00.01	11-03-2016	First draft version	Xiaobing He (UNI PASSAU)
00.02	29-03-2016	Data protection issues	Zhiyuan Sui (UNI PASSAU)
00.03	04-04-2016	Internal review	Ali Alshawish (UNI PASSAU)
00.04	08-04-2016	Internal review	Andreas Fischer (UNI PASSAU)
00.05	08-04-2016	Internal review	Florian Niedermeier (UNI PASSAU)
00.06	28-04-2016	Internal review	Antonios Gouglidis (ULANC)
00.07	29-04-2016	Internal review	Paolo Giacalone (AKH)
01.00	02-05-2016	Final version	Xiaobing He (UNI PASSAU)

AUTHORS LIST

Organization	Name
UNI PASSAU	Xiaobing He (xiaobing.he@uni-passau.de; phone number:+49 0851 509 3054)
UNI PASSAU	Zhiyuan Sui (zhiyuan.sui@uni-passau.de ; phone number: +49 0851 509 3055)
UNI PASSAU	Hermann de Meer (Hermann.deMeer@uni-passau.de; phone number: +49 0851 509 3051)
AKH	Paolo Giacalone (paolo.giacalone@akhela.com; phone number: +39 070 2466 1415)
AKH	Marco Soro (marco.soro@akhela.com; phone number: +39 070 2466 1035)

Table of Contents

EXECUTIVE SUMMARY

This HyRiM deliverable D4.2 provides a practical set of guidelines for utility providers on how to use surveillance technologies to secure their utility networks. These guidelines are addressed to those who decide to use surveillance technologies for utility networks protection purposes and are responsible for their operations. This typically includes the analysis of suitability of surveillance, the selection of surveillance technologies and the location and configuration of surveillance systems. In addition, these guidelines also aim to suggest assignment of responsibilities among staff members of a utility network and other relevant stakeholders and to help assessing potential security risks in a utility network. These guidelines suggest addressing privacy and security at the surveillance system design stage, from both regulation and advanced technologies points of view. Moreover, these guidelines list steps of surveillance data preparation for risk assessment, elaborate the application of surveillance data to compute risk levels, discuss the possible impact of novel surveillance technologies on risk levels, and advocate a data retention period depending on specific purposes of surveillance systems.

ABBREVIATIONS

Term	Meaning
BYOD	Bring Your Own Device
CCTV	Closed-circuit Television
DPA	Data Protection Authority
DPO	Data Protection Officer
ECIs	European Critical Infrastructures
EDPS	European Data Protection Supervisor
FCC	The Federal Communications Commission
FISC	Foreign Intelligence Surveillance Court
SCADA	Supervisory Control and Data Acquisition

1 INTRODUCTION

1.1 The guidelines

These guidelines are designed to help utility providers securing their utility networks using surveillance technologies. The term "surveillance technologies" includes all kinds of hardware, software or code (such as phones, notebooks, sensor nodes, intrusion detection systems, data-surveillance, and so forth) that can be used to monitor one specific area, event, or person. The objective of these guidelines is to build a list of recommendations that can be employed in applications where either an existing surveillance perimeter shall be upgraded with new monitoring technologies or a new surveillance grid is about to be implemented. These guidelines also provide advices on compliance with privacy and data protection rules in the context of surveillance data for risk management purposes. With these guidelines, utility providers should be able to understand what preparations are needed, which areas should be noted and what results may be obtained.

1.2 Scope of the guidelines

These guidelines focus on surveillance technologies for typical security purposes including security incident prevention. These guidelines are also applicable to more complex or more specific security operations. The following issues are addressed in these guidelines:

- advices for decision on surveillance systems/technologies;
- security risks of perimeters in utility networks;
- general principles for designing privacy and security for surveillance;
- suggestions for responsibility assignment among stakeholders;
- application of surveillance data to computer risk levels;
- surveillance data retention period.

These guidelines do not address the following scenarios and topics:

- staff using surveillance technologies for personal purposes (even if brought to the utility networks, e.g., mobile devices);
- risks that are not related to the protection of personal data (e.g., protection of intellectual property or classified information);
- processing of electronic communication data for detection of unauthorized use of surveillance technologies.

1.3 Structure of this deliverable

This deliverable structures the list of guidelines as follows:

- Section 2 "*Suitability of surveillance*" discusses the purpose of surveillance systems when new surveillance is going to upgrade the existing surveillance grid or is going to be implemented where no surveillance grid is existing. The content of this section also include the considerations of surveillance areas and resources used to operate the surveillance system.
- Section 3 "*Deciding which surveillance technology to use*" presents merits and demerits of both traditional surveillance technologies and novel surveillance technologies.
- Section 4 "*Selection, location, and configuration of the surveillance system*" lists recommendations for selecting, positioning and configuring surveillance systems, using a realistic use-case scenario from a refinery in EU.

- Section 5 "*Assignment of responsibilities*" and Section 6 "*Security risks in utility networks*" present recommendations for responsibilities assignment among data protection officer (DPO), staff and other stakeholders and suggestions for risk identification, respectively.
- Section 7 "*Privacy and security by design*" discusses in more detail the privacy and security issues related to surveillance systems. This section also suggests solutions for privacy and data protection issues at the national or even the EU level.
- Section 8 "Regulatory requirement on surveillance" lists main principles to follow when it is necessary to inform people about the new surveillance system.
- Section 9 "From surveillance data to risk levels" presents steps to prepare data for further risk assessment, elaborates the application of surveillance data to computer risk levels and discusses the possible impact of novel surveillance technologies on risk levels.
- Section 10 "Selection of retention data and period" lists possible retention periods for different type of surveillance data and their corresponding regulation/lawful compliance.

2 SUITABILITY OF SURVEILLANCE

Surveillance can be used to identify hazards, manage risk and enable, typically, a preventive, protective or reactive response, or the collection of data for preparing such a response in the future [1]. Surveillance devices are used in every field of endeavour, from domestic, governmental, and residential security to intelligence and military applications [2] [3] [4]. Utility networks are susceptible to various environmental, organisational, technical and intentional/unintentional human factors, as discussed in HyRiM's deliverables D1.1 "*Report on (cyber) risk trends in utility network operator requirements*" and D3.1 "*Analysis of human and organisational factors in utility vulnerability and resilience*". The decision to use surveillance systems should be taken carefully. It should be documented in writing and supported by historical data that security incidents happened. Also, an assessment of potential benefits and analysis of possible impact on privacy rights and other legitimate interests of those in the area of coverage is required. This section guides utility providers on analysing the purpose of surveillance, identifying surveillance areas and addressing resources to operate the surveillance system.

2.1 Purpose of surveillance

Before deciding to install a new surveillance system, the utility network must firstly identify the purpose of the surveillance system and must make sure that this purpose is legitimate. For example, the surveillance system must not be used to monitor workshop attendances or the work of employees. The purpose of the system indicates why surveillance systems are required for securing utility networks. The purposes and objectives of the system shall include, but are not limited to, the planned use of its data, serving as a frame of reference for evaluating components (core facilities or extended perimeters) in utility networks. The purpose and objectives of the surveillance system should be clear, specific and explicit. Being specific about the purpose of the surveillance can help utility networks to comply with the law, assessing the success of their system, and explaining to their staff and members of the public why a surveillance system is needed.

The limitations on the use of the data must be clearly established, especially if this is requested by staff representatives or other stakeholders. Further, it must be ensured that the data are not used for unforeseen purposes or disclosed to unforeseen recipients (who might use them for additional, incompatible purposes) except authorised ones. A surveillance system for securing utility networks is dependent on a clear case definition for the security-related event under surveillance. The case definition of a security-related event can include a fire breaking out in a component in utility networks, virus checking information (place, time and frequency), or other specific behaviours. The use of a standard case definition increases the specificity of reporting and the integration with other systems. A flow chart of the surveillance system should be drawn and if appropriate, legal authority for the data collection should be cited.

The following example questions may help to identify the purposes and operations of the surveillance system:

- What will the surveillance system be used for (security and access control)?
- What is the period of time of the data collection?
- What data are collected and how are they collected?
- What are the reporting sources of data for the system?
- How are the surveillance data managed (e.g., the transfer, entry, editing, storage, and back up of data)?
- Does the system comply with applicable standards for data formats and coding schemes?
- How are the surveillance data analysed and disseminated?
- What policies and procedures are in place to ensure data privacy, data confidentiality, and system security?
- What is the policy and procedure for releasing data?
- How are the surveillance data disposed?

2.2 Areas under surveillance

The surveillance system may include a number of sensor nodes, cameras, or X-rays located either in one fixed place or moving around the utility network. The surveillance system is not allowed to monitor any areas that are sensitive to privacy such as individual offices, leisure areas or toilet facilities. The location or routine of surveillance devices must be carefully reviewed to ensure that they minimise the monitoring of areas that are not in relation to the intended purposes.

2.3 Resources used to operate the surveillance system

Certain resources are directly required to operate a surveillance system for utility networks. These resources describe the monetary, personnel, and other resources needed to operate the surveillance system of interest.

- **Funding sources:** specify the source of funding for the surveillance system.
- **Personnel sources:** estimate the time it takes to operate the system, including the collection, editing, analysis, and dissemination of data (e.g., person-time expended per year of operation).
- **Other sources:** include travel, training, supplies, computer and other equipment and related services (hardware and software maintenance, computer support and Internet connections, etc).

3 DECIDING WHICH SURVEILLANCE TECHNOLOGY TO USE

When it comes to implement a new surveillance system, the first aspect that has to be defined is which kind of surveillance technology to use. In the context of securing utility networks, the selected surveillance technologies should be effective to contribute to the prevention and control of security-related events, including an improved understanding of the implications of such events. A surveillance technology should not be implemented, if it cannot achieve its purposes (for example, if the purpose is to control access to a building, but the installation of cameras does not help prevent unauthorised access). This section discusses limitations and challenging issues of traditional surveillance technologies. Moreover, it also points out the need for novel surveillance technologies, identifies advantages and drawbacks of novel surveillance technologies.

3.1 Traditional surveillance technologies

Current surveillance technologies are widely used in various application scenarios [5] [6] and they can be categorised according to the physical nature of the technology itself, the kind of data derived and the nature of the surveillance with respect to the awareness of the person being surveilled. Deliverable 4.1 "*Physical and cyber risk prediction modelling using surveillance systems*" of the project HyRiM gives a review of surveillance technologies in Section 5.2 "*Review of surveillance technologies*". A description and applications of traditional surveillance technologies can be found in "*Handbook of surveillance technologies*" [7]. In [7], acoustic surveillance (sounds within and beyond human hearing) is categorized into three sections: audio surveillance, infrasonic/ultrasound surveillance and sonar surveillance; electromagnetic surveillance, based on specific electromagnetic phenomena or its dependency on electromagnetic phenomena, is grouped into radio, radar, infrared, visual, ultraviolet and X-rays surveillance and biochemical surveillance (biochemical features) is divided into chemical/biological, biometric, animal and genetic surveillance. Magnetic surveillance, cryptographic surveillance and computerized surveillance, which are not technically electromagnetic, are also presented in [7]. From the form of collected data point of view, these following paragraphs elaborate limitations and challenging issues of surveillance technologies which are categorised in [7].

1) **Audio Surveillance: technologies within human hearing ranges**
   - Vulnerability with wireless transmissions
   - Technical expertise is needed to install components
   - Difficult to obtain access to the inside or near-outside of the premises for installation
   - Radiation emissions: may interfere other devices or be compromised by radiation from other sources
   - Change of equipment is not easy
   - Limited recording times and vulnerable to detection
   - Phone tapping devices can be detected and defeated

2) **Infra/Ultrasound Surveillance: sounds at frequencies neither below nor above human hearing**
   - Passive infrasound and ultrasound do not pose direct risks to physical structures or human health
   - Active infrasound should be used with a certain amount of caution

3) **Sonar Surveillance: some sonar sounds are within human hearing ranges but many are not**
   - Attenuation, discontinuity (the gradual loss of signals)
   - Interference of signals

4) **Radio Surveillance**
   - Power consumption: surveillance is in remote areas, where access to power is limited or absent; while renewable energy resources are not practical in all situations
   - Availability of Bandwidth: stringent bandwidth allocations and licensing requirements for the frequencies used and the strength of the signals
   - Communication confidentiality/privacy problems

5) **Radar Surveillance: a remote-sensing technology for detecting and interpreting radio signals**
   - Interpretation of displays and radar data: dependent on the mode of representation, the kind of display, the speed at which the display is updated, etc.
   - Antennas: the used frequencies are limited by the size and shape of the transmitting and receiving antennas
   - Radar countermeasures: radar-reflecting barricades, radar-absorbent or radar-scattering paints and filaments and frequency jamming
   - Bandwidth and frequency: multiple diverse power stations existing and signals transmitted at the same frequency interfered with one another

6) **Infrared Surveillance**
- Separating the target from the clutter: the thermal radiation from the components used to build detectors can interfere with the function of sensitive detectors
- Eliminating noise and interference become areas of concern: nuclear and space radiation create noise spikes in infrared detectors

7) **Visual surveillance**
- Visual devices with high capabilities are expensive
- Digital video and still cameras are lacks of "tamper-proof"
- Limited recording times for tapes or digital flash cards

8) **Ultraviolet surveillance**
- Invisibility: data-or light-conversion techniques must be used to detect or image ultraviolet sources
- Hazard to humans and other living things

9) **X-rays surveillance**
- Hazardous radiation to living tissue
- Vigilance: the effectiveness of X-ray devices relies on X-ray operators; X-ray operators must highly concentrate on their work in case of interference
- Expense and inconvenience

10) **Chemical & Biological surveillance**
- Problems related to health, safety, and contamination of evidence
- Individual chemical and biological hazards

11) **Biometric surveillance: humans have many unique attributes (fingerprints, toeprints, and basic voice characteristics) that provide biometric measures**
- Forensic identification of fingerprints
- Optimizing iris and retina scans
- Reliability

12) **Animal surveillance**
- Narcotic-sniffing false positives
- Relocation of animals

13) **Genetics surveillance: DNA testing and analysis**
- Sampling: DNA profiling is dependent on the quantity and quality of the samples
- Processing
- Storage
- Population demographics: database of large numbers of profiles is needed to analyse statistical relationships with known or reference populations
- Discrimination

14) **Magnetic surveillance**
- Magnetic interference
- False alarms
- Theft and tampering
- Detection speed and processing

15) **Cryptologic surveillance: discovery and analysis of coded and hidden information**

- Inconvenience: encryption systems add time to any task
- The human element: no encryption system can be completely secure
- Arrogance: new encryption systems are claimed by their designers to be unbreakable
- Politics: law-enforcement and secret service agents; balance between the needs of national security and the global competitive needs of business

16) Computerized surveillance

- Social issues
- Information management

The installation of the abovementioned surveillance devices requires the assistance of professionals. Moreover, once they are installed, there is no chance for them to move to another place or the movement cost is relatively high. The cost of remote camera placement cannot presently be justified. Failures/damages of surveillance devices or battery drain would directly lead to the compromise of monitored environments. Additionally, for wired communication based surveillance devices, it is easy for unauthorized people to disable the monitoring system by cutting the network wires. The time and cost problem resulting from using traditional surveillance devices and wired communication channel will limit their services provided. Most importantly, traditional surveillance systems have no awareness of surrounding context such as location and speed. In addition, duplicate and unwanted information can be transferred on the network causing significant delay for other more important information and there is no information priority. For example, information reporting a fire is more important than information about pressure measurement. In summary, the challenges and issues associated with traditional surveillance technologies can be listed in the following:

- **Infrastructure.** Securing an area (such as power sources, road or even walls) that lacks infrastructure can be difficult. How cameras can be powered and deployed, how security guards access remote sites and how surveilled data securely transmitted from multiple surveillance devices to a central monitor or hub will be monitored needs to be reconsidered.
- **Reliability.** Many traditional surveillance methods can miss vital or suspicious activities for a number of reasons. Thus they offer less-than-ideal reliability. For example, pan-tilt-zoom cameras often fail to capture important footage because they are focused on something else.
- **Cost-prohibitive pricing**. Traditional surveillance technology may become far more expensive than original expected. For example, when a camera system requires the operator to dig new power and data cables, or when a large perimeter requires the operator to invest in several dozen cameras, costs can easily spiral out of control.
- **Sustainability.** The sustainability of financial cost for operating a surveillance grid is not optimized. Most video surveillance are running 24 hours a day, seven days a week. Over time, the financial and environmental costs of these always-on devices can have a significant impact on a company's bottom line and sustainability initiatives.
- **Flexibility.** Most traditional surveillance devices are immobile in nature and are limited by the hardware. They need to be carefully installed and configured by skilled personnel. Additionally, system failures cannot be addressed in timely and cost-effective manner, resulting in gaps and holes in the surveillance grid.

However, though there are limitations and challenges, traditional surveillance technologies are widely applied in realistic scenarios. As technologies are continually evolving, it is believed that challenging issues will be taken into account and tackled.

3.2 Novel surveillance technologies

Traditional surveillance systems are mostly wired and use a PC as a surveillance terminal, which causes new dependencies on the underlying networks. By now, there is a mature market for such kind of surveillance

systems and their costs are relatively high. However, they cannot meet the need to move their devices to surveille any place appointed, where there is strict needs on performance and reliability. With the advances of technologies and the proliferation of sensing devices of every-day use, such as renewable energy generators, mobile phones and tablet PCs, more and more new surveillance technologies are emerging to overcome the shortcomings of their traditional counterparts [8] [9]. Just as people's demand for mobile phones emerged after the popularity of landline telephone, there is increasing need for novel surveillance systems. With the evolution of new technologies, possible solutions are available for the development of on-demand surveillance technologies. For example, wireless bandwidth is larger and larger in 3G (or even 4G) technology, which makes it possible to develop content-rich applications for mobile sensing devices and provide a basement for the realization of context-aware surveillance system at the same time.

These novel technologies (such as wireless sensor networks, cell phones or other networked device using appropriate sensors) are highly mobile and flexible. This flexibility opens up the possibility of using dynamically active sensors of a wireless sensor node, depending on the current situation of the surveilled perimeter. These technologies enable surveillance devices to be used on an on-demand basis, reducing cost and overhead compared to an "always-on" solution. The advantages of novel surveillance technologies are summarised in the following:

- **Situation awareness:** typical surveillance systems have focused on tracking location and activity and biometrics systems have focused on identifying individuals. Novel surveillance technologies can provide joint location identity and activity awareness, which when combined with the application context, become the basis for situation awareness. Such systems can provide useful information to the situation recognition phase of the threat awareness, as introduced in HyRiM's deliverable 1.1 "*Report on (cyber) risk trends in utility network operator requirements*".
- **Re-deployment and portability:** allow users to place surveillance devices whenever and wherever of interest.
- **High sustainability:** on-demand basis.
- **Ease of integration:** cables are not necessarily needed. Minimized deployment time and reduced business interruption.
- **High scalability:** can easily be expanded on demand.

Example: BYOD used as surveillance system

In nowadays work life, the demand to use personally owned devices (e.g., smartphones, tablets, etc.) in the office environment increases. An estimated 50% of employees use their personal mobile devices in some way to access their company's networks. This is due to the fact that employees want to and often need to be available outside the office hours and therefore need to process office information (e.g., emails, documents, etc.) also on their private devices. This topic is generally known as "Bring your own device" (BYOD). In the surveillance world, this type of fluidity is especially valuable. New mobile applications enable security personnel to accomplish two very important tasks:

- Whenever and wherever to access live and archived video on mobile devices;
- Use their mobile devices, in fact, as surveillance cameras by streaming real-time video to the central system.

What employees need in/outside of the office is a connection to an IP wireless network, and the ability to gain immediate, real-time access to their facility's security system using an Android or iOS device. These mobile apps enable users to manually stop and start recording, search and play back recorded video, control cameras and trigger a panic alarm to instantly notify personnel on-site of a security event. Other apps let users use their mobile devices as IP video cameras, streaming live footage directly onto the surveillance network. Security personnel can quickly and easily capture video while patrolling a facility's perimeters, within interior locations that lack video coverage and in any other area that needs additional coverage. BYOD helps security officials to gather more information and more relevant surveillance data.

Beside various advantages, novel surveillance technologies also have their own drawbacks. Taking smartphone-based surveillance for example to illustrate, smartphones are increasingly becoming an attractive target for "smartphone dumpster divers" (who retrieve information that could be used to carry out an attack on a smartphone). Smartphones can be used as an integral part of a person's daily life, by an employee in a business or government organization, or by a high or top-level official in a business or government organization. Vulnerabilities present in a smartphone may include patching weakness, limited capabilities for 3rd party security solutions, covert channels/weak sandboxing, user permissions fatigue, encryption weaknesses, no privacy protection best practices, lack of user awareness, and so on [10].

Example: Malware propagation via BYOD

Employees in a utility network could be allowed to use their private devices (laptops, mobile phones, etc.). This enables them to perform their work more efficiently, however, it also bears a higher potential for a malware infection. For example, an employee is working with his private laptop from home, using his standard internet connection. The personal device may be inflected by a malware via browsing the Internet and accidentally clicking on pop-ups. When the employee connects to the internal company network, the malware is behind the firewall and is able to propagate into the internal network.

4 SELECTION, LOCATION AND CONFIGURATION OF THE SURVEILLANCE SYSTEM

After deciding which surveillance devices to use in the utility networks, the next step is to evaluate how to integrate them with existing control systems and/or networks/IT systems. This section provides a real example scenario from a refinery located in EU to guide utility operators to select, cite and configure the surveillance system correspondingly for their own utility networks. Utility providers can similarly analyse their utility networks and select, position and configure their surveillance systems.

The refinery is one of the biggest high complexity refineries in EU, with over several hundred thousand barrels per day of refining capacity. The refinery has a huge large surface with many different plants and buildings inside. Being such a big area, the protection of its perimeter is of paramount importance and for this reason installing a video surveillance systems is a priority.

When selecting a video surveillance system, the maximum control level over the area has to be achieved. Video surveillance technologies available today offer a very high level of control. An optimal solution is to position fixed surveillance cameras every 30 meters along the border that has to be surveilled and to equip with an intelligent video analysis system, which is able to detect intrusions inside the perimeter. In addition to the fixed cameras it may be useful to install speed dome cameras, controlled by a video analysis software, which is able to zoom automatically to the area where the alarm was generated.

The basic components of a network video system is the network camera, the video encoder (used to connect to any existing analog cameras), the network, the server with the storage unit and the video management software. The network camera and video encoder, since they are based on computer equipment, have features that an analog CCTV camera cannot offer. The network, the server and storage units all use standard IT equipment. The ability to use standard consumer equipment is one of the main benefits of network video technology.

Some of the advantages are:

Remote accessibility: Network cameras and video encoders can be configured and managed remotely, allowing multiple authorized users to view live and recorded videos at any time.

High quality image: In a video surveillance application, high image quality is essential to allow users to capture clear images of an event in progress and identify persons and objects involved. Using progressive scan technology and a specific megapixel resolution, a network camera can provide superior image quality and higher resolution than an analog CCTV camera. In addition, a system with network video enables more easily to maintain the image quality rather than an analog video surveillance system. With today's analog systems that use a DVR system as a recording instrument, many conversions are performed from analog to digital: in the first place, the analog signals are converted into the digital camera, and then back to analog for transport; subsequently, the analog signals are digitized for recording. The quality of the scanned images decreases with every conversion from analog to digital and vice versa, as well as because of the wiring distance: the greater the path that the analog video signals must make, the worse the quality. In an IP-surveillance system, images of a network camera are digitized once and remain digital with no unnecessary conversion activities and the image quality is not deteriorated by the many network transfers;

Event management: Advanced network cameras and video encoders with integrated analysis functions can solve this problem by reducing the number of uninteresting recordings and enabling the use of programmed responses. These features are not available in an analog system. Network cameras and video encoders have some built-in functions available, including the functionality for the detection of moving objects in video, audio detection alarm, active tampering alarm, the connections input / output (I/O) and functions for the management of alarms and events. These features enable the network cameras and video encoders to

constantly analyze inputs to detect an event and to automatically respond with actions such as video recording and sending alarm notifications. The functions for the management of events can be configured using the product user interface with network video or a video management software program. Users can define the alarms or events by setting the trigger type to use and when to use them. It is also possible to configure the answers (for example, recording at one or more sites, locally and / or remotely for security purposes, the activation of external devices such as alarms, lights and doors and the sending of notification messages users);

Easy integration and better scalability: The products with open standards-based network video system can be easily integrated with information systems based on Ethernet communication and computers, audio or security systems and other digital devices, in addition to software for video management and applications. A system with a network video system can be easily expanded according to users' requirements;

Flexibility and convenience: An IP-surveillance system has typically a lower total cost of ownership than an analog CCTV system. Also management and equipment costs are lower because the back-end applications and storage units use servers are based on standard open systems and not on proprietary hardware.

5 ASSIGNMENT OF RESPONSIBILITIES

5.1 Data protection officer

A utility network may appoint one or a team of persons to be its DPO to oversee the data protection responsibilities within the organization and ensure compliance with the national Data Protection Directive. First and foremost, plans to install or update a surveillance device (a traditional or novel) should be communicated to the DPO of the utility. He or she should be consulted in all cases and should be involved in all stages of the decision-making, from the initial determination whether to use surveillance system to how to provide information to the public.

5.2 Staff and other stakeholders

Staff and other stakeholders should be consulted in any case as widely as possible. For example, in the refinery, many departments have to be consulted about setting up a new surveillance system. These departments to be consulted are the engineering office, the maintenance department, the personnel department and the purchasing department. Each of them has to carry out different evaluations, which are specific to the activities they manage inside the refinery. The engineering department plays however the most important role, since it has to define the technical aspects of the implementation of the new surveillance system and has to manage all scouting activities related to the identification of the best possible video surveillance technology for the perimeter that has to be secured. The maintenance department is involved in the decision process when it comes to the integration with the existing control systems that operate near the perimeter and has to take into account all integration aspects of the new surveillance systems with all existing systems and networks. The personnel department has to take all measures to inform all people that a new video surveillance system is in place and has to ensure that specific informative signs are installed in the vicinity of the cameras, both outside and inside the refinery perimeter.

6 SECURITY RISK IDENTIFICATION IN UTILITY NETWORKS

Risk management is a core duty in utility networks as operated by utility providers. Risk identification is of paramount importance for utility operators to decide the target objects of surveillance systems.

Risk assessment is broader than just the risk of violence to others, though this is the most relevant concern to the public and media. Before applying any surveillance technologies to secure his/her networks, the utility provider should have knowledge about what kind of risks exist, or could happen in his/her utility networks that would affect their business, market, operation, and so on. One of the notable risks in interdependent utility networks in the potential cascading effects of the failure of individual utilities [11]. For instance, a scenario in which control systems of a water utility provider are attacked could prove disastrous. To illustrate a simple and well-known, but still effective attack-example we point to the following: it would be possible for someone without a deep IT security background to look for control network components (e.g., the popular Simatic S7 PLCs) via specific search engines (e.g., shodanhq.com) and to access these to tamper with the configuration or to hijack the configuration, as described in HyRiM's deliverable 2.1 "*Future trends SCADA-related attack, mitigation and prevention tools*". Access may be achieved via default user names and passwords or via vulnerabilities of the operating systems of the control units for which numerous exploits exist, especially if they are outdated. Failures due to such an incident in said water supply can result in reduced availability of water for the cooling of, e.g., refineries. This can result in a shortage of gas for heating and for petrol to power our fossil-fuel-driven vehicles.

Example: identify risks in extended perimeters in a refinery in EU

Inside an environment like a refinery, it is not easy to talk about specific threats, because a refinery can be subject to very different risks and the relevant scenarios are numerous. Considering the physical and IT levels, for each of them very different risks should have to be considered. Limiting, for example the focus to video surveillance systems, they can be a target of cyber attacks. Apart from cyber security risks, another important aspect that poses a threat to the quality of controls of the perimeter that has to be secured is represented by vapour coming out from pipelines. This is an extremely important issue when it comes to install a video surveillance system inside an industrial plant. As a matter of fact, the presence of vapour near the video surveilled perimeter can cause the system to produce false positives when the systems detect vapour and send an alarm mistaking the vapour for a person. In the long term, people responsible for the control systems may not carry out appropriate controls in presence of a false positive due to a possible vapour which in reality is not a false positive but is indeed a real intrusion of a person that has entered the controlled area.

7 PRIVACY AND SECURITY BY DESIGN

7.1 Building privacy and security into the design of surveillance system

Security is the basis of the surveillance systems. The most important functionality of traditional surveillance systems is keeping track of people and recording their behaviours. From a utility provider's side, threats are not only from cyber attacks, but also from physical attacks. Surveillance systems are necessary to monitor those threats in utility networks to detect misbehaviors, identify crimes, protect infrastructure and provide auditing evidence in the future.

In utility networks, trustworthiness is the cornerstone of surveillance systems. The basic meaning of trust is still under argument, but there is consensus on the fact that, trust is developed over time but can be lost quickly. Same as other network technologies, surveillance networks are vulnerable to cyber attacks, such as replay attack and fake data injection. Untrustworthy data sharing in the network can misinform the control center. If the surveillance system is for utility networks, it would cause pecuniary loss. More than that, the failure of a utility usually affects people's daily lives and businesses. In surveillance systems, the data collector has to ensure the data integrity. Besides technological aspects, a data collectors' reputation is also tested to the utmost. The potential use of surveillance data gives rise to a sharp dilemma. Should the data collector use basic surveillance data to identify potential risks and put them under extra scrutiny? If not, the surveillance system gives up its important precaution functionality. If so, it may lead to discrimination. In addition, public webcams and surveillance systems open a novel area to public security nowadays.

Apart from audit, an internal analysis of the security risks must be carried out to determine what security measures are necessary to protect the surveillance system, including the personal data it processes. Measures must be taken to ensure security with respect to

- Transmission;
- Storage;
- And access.

Transmitted data are usually with users' sensitive privacy information. Users would not like to leak those important information to other third parties because that affects users' daily life. With the development of Internet technology, the application of wireless communication also open some new vulnerability at the same time. Interception of transmission can typically happen in three ways: by eavesdropping on the transmission; by injecting false data to the current transmission, and by gaining access to the surveillance devices themselves. Transmission must be routed through secure communication channels (frequency hopping could be applied) and the transmitted data must be encrypted or equivalent protection must be provided.

Outsourcing data to cheaper and cheaper cloud servers is a promising approach to relieve the control center from the burden of such a large amount of data storage. Since cloud servers are separated administrative entities, data outsourcing is actually out of the utility provider's control over the fate of their data. At the same time, the correctness of the surveillance data in the cloud is being put at risk. Firstly, although the infrastructures in the cloud are much more powerful and reliable than personal computing devices, they are still facing the broad range of both internal and external threats for data integrity. Examples of outages and security breaches of noteworthy cloud services include Apple's iPad subscriber privacy leakage [12], Amazon S3's recent downtime [13], and Gmail's mass email deletion [14]. Secondly, for the benefits of their own, there do exist various motivations for cloud service providers to behave unfaithfully towards the cloud users regarding the status of their outsourced data. In short, although outsourcing data into the cloud is economically attractive for the cost and complexity of long-term large-scale data storage, it does not offer any guarantee on data integrity and availability. This problem, if not properly addressed, may impede the successful deployment of the cloud architecture.

Surveillance devices support high-security authentication via encrypted digital certificates, unlike simple password authentication, which can guarantee to not be guessed or discovered by data eavesdropping. Any data connection of surveillance devices not in use needs to be shut down, so there is no chance of them being hijacked. The location of the surveillance device (especially the holder of a mobile devices) must not be accessible to unauthorized personnel. In case of any inadvertent disclosure of personal information, a process must also be in place to appropriately respond to. The security analysis as well as the measures taken to protect the surveilled data must be adequately documented. If appropriate, an information security policy

should be adopted. Security operators in utility networks need to be involved in the drafting of the security policies from the very early stages.

However, security is a challenging task in surveillance systems considering privacy issues. As surveillance system collects and records crimes and malicious behaviours. To identify those, an innocents' sensitive information is also recorded by the system. That information can expose people's privacy. Besides regular surveillance systems, people's privacy are leaked due to more and more convenient mobile surveillance technologies. People's mobile phones, travel cards and credit cards can reveal where they are, who they are, and what they are doing, since those devices should be registered with people's real names.

Besides the utility provider, cloud servers also have threats on privacy. Monitoring data stored in cloud servers affects Smart Grids' quality of services. On one hand, unauthorized entities should not have the right to access the corresponding usage data. On the other hand, even consumers' usage data queried by authorized customer cannot expose consumers' privacy information. To achieve that, multiple trustworthiness and privacy features should be achieved.

Theoretically, laws can preserve a user's privacy in utility networks. However, for one thing, such laws are often delayed and much more expensive than preservation based on technologies. For another, laws also require technology that provides evidence for future judgement. However, privacy safeguards should be built into the design specifications of surveillance systems that the utility networks used. Privacy-friendly technological solutions should be used.

Privacy preservation and surveillance are two conflict requirements for technologies. On one hand, users would like to share as little information as possible to preserve their privacy. On the other hand, a surveillance system requires enough information for security. Currently, there have been a number of anonymous surveillance schemes already offered to detect potential crimes. Various encryption, pseudonym, anonymity, and access control schemes are proposed for security and privacy preservation in surveillance systems, including anonymous surveillance, anonymous digital cash, and so forth.

7.2 Addressing data protection issues

Data protection is an important aspects of privacy preservation. It controls the personal information and ensures that only the correct organizations, businesses and the government can access the data.

For example, according to the UK data protection act 1998 [15], data protection should adhere to the following principles:

- *Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless the data subject has given his consent to the processing;*
- *Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes;*
- *Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;*
- *Personal data shall be accurate and, where necessary, kept up to date;*
- *Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes;*
- *About the rights of individuals e.g. personal data shall be processed in accordance with the rights of data subjects (individuals);*

- *Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data;*
- *Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.*

When installing or updating a surveillance system, an initial data protection assessment should be carried out and comply with corresponding regulations/standards or even laws. For example, EU Data Protection Directive (Directive 95/46/EC) [16]. This directive has been adopted by the European Union and it is designed to protect the privacy and protection of all personal data collected for or about citizens of the EU, especially as it relates to processing, using, or exchanging such data.

Additionally, an employee education should be established to raise awareness on how to protect personal data collected by surveillance systems. The employee education should follow certain policies/standards/directives and should be evaluated and updated periodically. The training may be obligatory regularly as a "refresher course" for every stakeholder who has the access to personal data. Training provided for new member of staff and workshops on data protection compliance issues should be offered at least once every two years for all staff with access to personal data. Training should be held when a new surveillance system is installed, when significant modifications are made to the system, when a new person takes up his/her duties, as well as periodically afterwards at regular intervals.

8 REGULATORY REQUIREMENTS ON SURVEILLANCE

Informing people about surveillance systems in place has to be done according to the data protection law/regulations, for example, at the EU level -- Directive 95/46/EC or at the national level – Italian Data Privacy code (Legislative Decree 196/2003) and Italian Legislative Decree 151/2015 which redraws the rules governing the workers remote control, by amending Article 4 of the Law 300/1970 ("*Workers' Statute*") and adapting it to the technological level of modern companies.

The main principles which have to be followed are

1) Citizens transiting a controlled area must be informed with signs, visible in the dark, if the surveillance system is active during the night.

    - The signs must be placed at such locations and be large enough that data subjects can notice them before entering the monitored zone and can read them without difficulties;
    - The signs posted in the languages (local language, international language or both) must be generally understandable.

2) Surveillance systems installed by public and private subjects connected to the police forces require specific information board, on the basis of the form of data protection authority (DPA).

    - Brief description of the coverage of the surveillance system;
    - The legal basis of the surveillance system;
    - Who has the access to the surveillance data, and to whom the data may be disclosed;
    - How the information is protected and safeguarded;
    - How long the data are kept.

9 FROM SURVEILLANCE DATA TO RISK LEVELS

The collected surveillance data may vary in terms of surveillance technologies. For example, data-surveillance may output different types of alarm messages and CCTV may produce video streams. In a utility network, there may be cases that several different surveillance technologies are utilised to establish one surveillance grid and those surveillance devices may provide different type of data. For example, when smartphones with an Android system are used for surveillance purpose, the video format may differ because of the Android version or hardware support.

The steps for preparing surveillance data, which will be further used for risk assessment could include:

- Firstly, surveillance data collection. For example, live streaming video of the surveilled perimeter. If a surveillance device monitors the surveilled perimeter continuously, like cameras, the surveillance data will be collected continuously. However, if a surveillance device works on an on-demand basis, surveillance data will be collected in discrete times;

- Secondly, context data storage. Raw data or aggregated data or sampled data can be stored in remote server or other data processing places;

- Thirdly, data analysis and processing. Collected data will be analysed by means of pattern recognition and data fusion. The surveillance data standardization is also included in this step;

- Fourthly, loss distribution compilation. This step aims at compiling distributions for the processed surveillance data. After compiling loss distribution, Hybrid Risk Metrics developed in the project of HyRiM could take loss distributions as input to compute an equilibrium and further to give utility providers suggestions on enhancing the security in an optimal way.

Application of surveillance to compute risk levels

In the attached paper A, we provide an example application scenario on how to compute and forecast risk levels from surveillance data in communication networks of power systems (which has the possibility to be applied to communication networks of other critical infrastructures). Paper A establishes a surveillance architecture to monitor message transactions among nodes in communication networks. A security belief model is built to interpret surveillance observations as Dirichlet-distributed security events with certain probabilities. By taking the interaction between possibly suspicious nodes and the security operator as a transmitting-monitoring game, a game-theoretic risk assessment framework is presented to computer and forecast risk of network security impairment.

Discussion: Impact of novel surveillance technologies on risk levels

As discussed in Section 3, there are different kinds of surveillance technologies available to establish a surveillance grid and to collect surveillance data. Suppose the data prepared for risk assessment is alarm information from detection software of the surveillance grid. Here an example application of surveillance devices for controlling access to a room's facilities is given.

In this scenario, both mobile phones and CCTV cameras are used to monitor a room's facilities. A CCTV would be installed and fixed in one place. A control operator could choose to turn on cameras all the time or only turn on them after working hours. The control operator could also use his mobile phone to check the room every 5 minutes, or every 15 minutes or even every 30 minutes. An attacker (an unauthorized person) would choose to enter the room after working hours or check whether there is a chance to launch a potential attack to facilities every 5 minutes, every 10 minutes, or even 15 minutes. For each combination of strategies from both attacker and control operator, surveillance data are collected and alarm messages (perhaps no) are produced by the detection software. It is assumed if anybody enters this room, an alarm information is produced. The people who are entering this room has their own patterns (e.g., faces, badges). Alarm information could be classified into clusters based on persons' patterns. According to security levels defined by the control operator, there may be many cases: a person is authorized to enter that room, such that his risk to facilities is low; a person is unauthorized, the risk when he enters that room could be high; an unauthorized person is accompanied with an authorized person, the risk could be medium, and so forth. Combining the occurrence number of each pattern from alarm messages and the risk level of each pattern, the loss distribution could compiled. Suppose the loss distribution α_{ij} for a strategy *i* from the attacker and a strategy *j* from the control operator is the entry of a model matrix **A**, such the model matrix **A** between the game of the attacker and the control operator could be

Model matrix **A**		Strategies from the surveillance grid				
Strategies from an adversary		Turn on cameras all the time	Turn on cameras only after working hours	Check the room every 5 minutes	Check the room every 15 minutes	Check the room every 30 minutes
	Enter the room after working hours	α_{11}	α_{12}	α_{13}	α_{14}	α_{15}
	Check the room every 5 minutes	α_{21}	α_{22}	α_{23}	α_{24}	α_{25}
	Check the room every 10 minutes	α_{31}	α_{32}	α_{33}	α_{34}	α_{35}
	Check the room every 15 minutes	α_{41}	α_{42}	α_{43}	α_{44}	α_{45}

As shown in the model matrix **A**, for each combination of strategies from both players, there is a different loss distribution α_{ij}. The use of novel surveillance technologies (e.g., mobile phones aforementioned) directly influence the entries of the model matrix: a different distribution from that of traditional surveillance technologies (i.e., cameras in this case). For example, the alarm messages from using mobile phones can lead to a high occurrence of unauthorized persons, who have the highest risk level. After computing the game, it could be the case that the payoff from using novel surveillance technologies is always the maximum and the novel surveillance technology is suggested as the optimal strategy that a control operator should take to secure his networks. However, there will also be cases that a strategy taken by a traditional surveillance technology leads to a maximum payoff. Thereafter, instead of taking novel surveillance technologies, the utility provider would take that specific strategy of the traditional surveillance technology to secure his networks.

10 SELECTION OF RETENTION DATA AND PERIOD

10.1 Retention period

Surveillance data must not be retained longer than necessary for the specific purpose for which they were made. European Data Protection Supervisor (EDPS) recommends that video data for typical security purposes should not be retained for longer than one week. In case the surveillance covers any outside area and it is not possible to avoid that passers-by or passing cars are caught on the cameras, EDPS recommends reducing the retention period to 48 hours or otherwise accommodate local concerns whenever possible. Additionally, EDPS also recommends shorter retention periods or live monitoring only when this is necessary to minimise the intrusion into the privacy and other fundamental rights and legitimate interests of those within the range of the cameras[1]. For example, if there is any peaceful protest in the coverage of utility's surveillance systems, in the absence of detection of a security incident related to the utility network, the surveillance data including the recordings of each peaceful protest should be deleted within two hours of the end of the protest. However, the surveillance data retention period depends also on the utility type and policies inside the organization.

Example: Retention period of video data in a refinery in EU

In the IGCC control room of a refinery in EU, data processed are kept in the distributed control systems for a few months but are then stored for a few years in Aspen InfoPlus.21, which is a process historian data repository and application platform. Aspen InforPlus.21 represents the international standard for the integration of enterprise and control systems.

10.2 Data retained beyond the retention period

If surveillance data need to be stored to further investigate or evidence a security incident, they may be retained as required. Their retention beyond the normal retention period has to be rigorously documented and the need for retention should be periodically reviewed.

[1]https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-03-17_Video-surveillance_Guidelines_EN.pdf

Furthermore, a register – whenever possible, in an electronic form – should be held to keep track of any recording that is retained beyond the normal retention period, but yet important for security operators to analyse security trends and to refer to, indicating

- The surveillance data and its timestamps;
- the location of surveillance devices;
- A short description of the security incident;
- The reason why it should be retained;
- The expected data of the review of the necessity to retain the data any longer.

Example: data retained beyond the retention period in the refinery

Data used in real time by board operators for plants management are stored inside the distributed control system in order to obtain operational trends that have to be read and analyzed immediately. These data are transferred via Ethernet to a server which stores them for a long term and make them accessible to the Aspen InfoPlus.21 platform. It is important to note that processed data are not categorized.

CONCLUSIONS

This derivable focuses on providing guidelines on surveillance technologies to secure utility networks across four main aspects:

- The need for a surveillance system and corresponding surveillance technologies to secure a utility network. Efforts should be made to identify the purpose of surveillance, the surveillance area, the decision of surveillance technologies (either traditional ones or novel ones) and the configuration of surveillance system to enhance utility network protection.

- The identification of security risks in utility networks. Before implementing a new surveillance grid or upgrading an existing surveillance grid with new monitoring technologies, which kind of security risk existing (target objects of a surveillance system) in one utility network, or more specifically, perimeters in the utility network should be identified and discussed in detail. Furthermore, data preparation for risk assessment and the application of surveillance to compute risk levels are elaborated. The possible impact of novel surveillance technologies on risk levels are also discussed.

- The building of privacy and security into the design of surveillance system and regulatory requirements on surveillance. The data protection issues are suggested to be addressed before the implementation of a surveillance system. A training plan is also recommended to educate new staff members or refresh other corresponding staff to protect personal data in surveillance systems. Additionally, the main principles that should be followed, when informing people about a surveillance system, are also discussed.

- The responsibility assignment among stakeholders and surveillance data retention period. In the utility network, who is responsible for what part of the surveillance system should be explicitly elaborated. Moreover, the retention period of surveillance data should be compliant with policies within an organization.

In this deliverable, we have provided guidelines for utility providers to secure their networks using surveillance technologies. We believe there has to be more investigation on how to apply surveillance technologies to support utility network security. Our primary readers for these guidelines are utility providers directly involved in the utility network implementation and protection. For a more detail knowledge about the mathematic model behind the risk assessment methodologies – Hybrid Risk Metrics, described in Section 9, we refer readers to deliverable 1.2 "*report on definition and categorisation of hybrid risk metrics*" of the project of HyRiM.

REFERENCES

[1] C. van Gulijk, H. Vagts, S. Höhn and O. Yaroyvi, "SURVEILLE Deliverable 2.1: Survey of surveillance technologies, including their specific identification for future work," 2012.

[2] M. Nieto, K. Johnston-Dodds and C.W. Simmons, Public and private applications of video surveillance and biometric technologies, California: CRB Pub. , 2002.

[3] C-Y. Lee, S-J. Lin, C-W. Lee and C-S. Yang, "An efficient continuous tracking system in real-time surveillance application," *Journal of network and computer applications,* vol. 35, no. 3, pp. 1067-1073, 2012.

[4] D.H.S. Lima, A.L.L. Aquino H.S. Ramos, E.S. Almeida and J.J.P.C. Rodrigues, "AOSys: An opportunistic and agile system to detect free on-street parking using intelligent boards embedded in surveillance cameras," *Journal of Network and Computer Applications,* vol. 46, pp. 241-249, 2014.

[5] J. K. Petersen, Understanding surveillance technologies: spy devices, their origins & applications, CRC Press LLC, 2001.

[6] A.S. Koyuncugil and N. Ozgulbas, Surveillance technologies and early warning systems: data mining applications for risk detection, IGI-Global, 2010.

[7] J. Petersen, Handbook of surveillance technologies, CRC Press Taylor & Francis Group, 2012.

[8] X. Chen, Y. Ruan, J. Yu and Q. Chen, "A surveillance system of Android smartphone with context-awareness," *Sensors & Transducers,* vol. 166, no. 3, pp. 173-180, 2014.

[9] L.M.R. Peralta and A.M.M. Abreu and L.M.P.L. Brito, "Environmental monitoring in museums based on wireless sensor network via cell phone," *Journal of Communication and Computer,* vol. 11, pp. 194-202, 2014.

[10] ENISA, "Smartphones: Information security risks, opportunities and recommendations for users," 2010.

[11] J.P. Peerenboom, R. Fischer and R.G. Whitefiled, "Recovering from Disruptions of Interdependent Critical Infrastructures," in *Workshio on mitigating the vulnerability of critical infrastructures to catastrophic failures*, Virginia, 2001.

[12] J. Morris, "iPad breach update: more personal data was potentially at risk," 15 June 2010. [Online]. Available: http://techcrunch.com/2010/06/15/ipad-breach-personal-data/. [Accessed 02 May 2016].

[13] C. Miller, "Amazon could failure takes down web sites," 21 April 2011. [Online]. Available: http://bits.blogs.nytimes.com/2011/04/21/amazon-cloud-failure-takes-down-web-sites/. [Accessed 02 May 2016].

[14] M. Arrington, "Gmail disaster: reports of mass email deletion," 28 December 2006. [Online]. Available: http://techcrunch.com/2006/12/28/gmail-disaster-reports-of-mass-email-deletions/. [Accessed 02 May 2016].

[15] "http://www.legislation.gov.uk/ukpga/1998/29/section/1," [Online].

[16] " http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML," [Online].

Paper A

Game-theoretic Risk Assessment in Communication Networks

Xiaobing He, Zhiyuan Sui and Hermann de Meer
Department of Computer Networks and Computer Communications
University of Passau
Innstr.43, 94032, Passau, Germany
{xiaobing.he, zhiyuan.sui, hermann.demeer}@uni-passau.de

***Abstract*—Two-way communication networks enable near real-time interactions in modern smart power systems. Also, computer and communication security systems have become one of the main factors of security in power systems. The need for methods to appropriately assess currently existing cyber risks and forecast possible future risks to a reasonable extent has become more important than ever before. This work establishes a surveillance architecture to monitor message transactions among nodes in communication networks. A security belief model is built to interpret surveillance observations as Dirichlet-distributed security events with certain probabilities. By taking the interaction between possibly suspicious nodes and the security operator as a transmitting-monitoring game, a game-theoretic risk assessment framework is presented to compute and forecast risk of network security impairment.**

Keywords*—surveillance; risk assessment; game theory; Dirichlet distribution; risk prediction.

I. Introduction

Two-way communication networks rapidly gain importance in modern smart power systems, as they enable near real-time interactions between customers and their respective service providers. Well-known examples for such interactions are, e.g., advanced metering infrastructures and demand-response services. Computer and communication security systems have gradually become one of the main factors influencing the security of power systems [1], [2]. Cyber attacks in communication security systems will firstly downgrade the performance of communication networks of the power grid. Consequently, the performance degradation of the communication network will disturb the control process of the power grid, which will further lead to power system instability. To mitigate these risks, proper risk assessment and prediction need to be in place. However, quantitative risk analysis is an important, yet challenging task. Therefore, instead of providing accurate numerical risk estimates, qualitative risk assessment (based on expert judgment and limited ranges of risk attributes) is recommended (e.g., by the German Federal Office for Information Security). However, model-based quantitative approaches are more effective in determining risk indices, by taking into account the potential damage of assets, service interruptions, the likelihood of successful attacks, and so on. Risks associated with cyber attacks on communication networks in smart power systems reverberate directly across society.

A power system, which can effective assess risk, is likely to be more resilient to potential disasters (e.g., large-scale blackouts). The need for methods to appropriately assess cyber risks and forecast possible future risks to a reasonable extent has become more important than ever before. Game theory has drawn more and more attention in risk assessment, because of its role in Decision Making and Control Theory [3]. Game theory lays the foundation for our proposed risk assessment framework. Though there are numerous risk assessment methodologies existing [4], [5], [3], [6], the data acquisition and data interpretation for risk assessment and prediction have not been intensively explored. This work monitors nodes' message transactions in communication networks of power systems using a surveillance architecture, builds a security belief model for possible monitoring security events, establishes a game-theoretic risk assessment framework, and informs security operators when their security measures (i.e., surveillance configurations) should be reconsidered.

The main contributions of our risk assessment and risk forecasting approach include the following: (i) A surveillance architecture. Instead of analyzing information (security patches, software updates, vulnerabilities) from the underlying system, a multiagent system architecture is established to monitor message transactions among nodes in a communication network with surveillance technologies; (ii) A Dirichlet-based security belief model. The surveillance observations are categorized into three possible security events with certain probabilities. This model allows security belief updating after transactions between nodes have taken place. (iii) Security risk assessment and prediction. With distributions of possible security events, risk is computed for corresponding security measures and the time when a security incident shall happen is also forecasted. The rest of this paper is organized as follows: Section II reviews related work and points out its limitations. Section III describes a surveillance architecture and Section IV presents the game-theoretic Dirichlet-based risk assessment framework, which is then applied to a practical illustrating example in Section V. Finally, Section VI concludes the paper and discusses future works.

978-1-5090-2320-2/16/$31.00

II. Related work

The report of ENISA [7] presents an inventory of risk management/risk assessment methods and tools. The European Institute for the Protection and Security of Citizen (EC Joint Research Centre [8]) reviews twenty-one European and worldwide risk assessment methodologies and identifies their gaps. However, most of the listed/compared risk assessment methodologies in [7] and [8] are qualitative risk analysis (e.g., based on failure mode effects and criticality analysis) and some methods focus on terrorist attacks or physical attacks in critical infrastructures. [9] reviews twenty-four risk assessment methods for Supervisory Control and Data Acquisition (SCADA) systems from different aspects, outlines five research challenges and points out possible approaches to deal with those challenging issues. Here we highlight quantitative risk analysis methods that assess security risks in information networks.

Continuous-time Hidden Markov Models (HMMs) for real-time risk assessment are introduced in [4]. The risk of assets on a network is evaluated as the probability and consequence of unwanted incidents. However, the parameters of the mathematical models to calculate the probability and consequence values are highly uncertain. Based on fuzzy theory and Petri Nets, [5] assesses and forecasts network security risks based on the detection alerts and network attack information. Since extensive attack information is difficult to obtain or not totally known to the public, this approach suffers the problem of attack information incompleteness. A vulnerability-centric risk analysis approach [6] is proposed to determine security risks associated with multi-step cyber attacks in critical information infrastructures. Hosts' vulnerabilities are mapped into preconditions and effects, and rule-based reasoning is used for vulnerability chaining. Finally, attack paths in the system are identifies with a vulnerability chains augmented graph. However, it does not calculate risk levels and does not identify which attack path has the highest likelihood to compromise the whole system. A Game Theoretic Attack-Defense Model (GTADM) is proposed in [3] to quantify the threat probability in network security risk assessment. Based on a cost-benefit analysis, the payoff matrix of the attacker and the defender is formulated to analyze the equilibrium of the GTADM model. Combined with vulnerability associated to nodes, risks of the system are computed as the sum of threat value of all the nodes. In [10], in order to find secure communication paths between two entities (the sender and the receiver), game theory is used to simultaneously optimize several performance indicators of a transmission service. However, few existing literature has explicitly elaborated how the information for risk assessment is collected and interpreted, or even, how the risk levels could be forecasted. The work in [11] presents a trust model based on RSS feeds and information obtained from the Internet and takes beta distribution with two parameters as a prior belief model to assess and forecast risks. Differently, our work in this paper uses a surveillance architecture to monitor nodes' message transactions in communication networks. These surveillance observations are then interpreted as Dirichlet- distributed security incidents with certain probabilities. This work views the interactions between suspicious nodes and the security operator as a transmitting-monitoring game to inform the security operator when his surveillance configurations should be reconsidered.

III. Surveillance architecture

We assume a multiagent system architecture consisting of agents that observe message transactions among nodes in a communication network with surveillance technologies. An agent is a computer program capable of a certain degree of autonomous actions. In a multiagent system, agents are capable of communicating and cooperating among each other. In this paper, an agent is responsible for collecting and aggregating data from a set of surveillance devices. These devices can be any information-gathering program or device, including sensor nodes, closed-circuit television (CCTV), smart phones, logging systems, firewalls, intrusion detection systems, etc. They are monitoring message transactions among nodes in communication networks. Agents are capable of process surveillance observations, specifically, extracting behavior patterns of both message sender and message receiver. This paper assumes that the security operator is capable of configuring surveillance devices and changing locations of surveillance devices. It is also assumed that message transactions are received or collected in discrete time intervals. These surveillance observations can be alarms from intrusion detection/prevention systems, suspicious traffic patterns, entries in log data files, and so on. An agent will receive observation messages from more than one surveillance device and these devices may provide surveillance observations in different forms. It is to be noted that, in the application of monitoring message transactions among nodes, only those surveillance observations that are relevant to message transmissions are taken into account. This paper assumes that the multiagent system is able to classify and send standardized observations according to the security belief model, explained in the following Section IV-A.

IV. Game-theoretic Dirichlet based risk assessment

A. Dirichlet-based Security Belief Modeling

In our model, the message transactions observed from the surveillance architecture are divided into three categories: dropped messages, maliciously modified and successfully forwarded messages. These three categories correspond to three possible security events of nodes: selfish, malicious and friendly behavior. Selfish nodes and malicious nodes can impair the network availability and network integrity, respectively. Additionally, the observed message transaction is one of the predefined three categories with a certain probability. Thus, the security belief model here can be translated into having a state space of cardinality three for the Dirichlet distribution. The Dirichlet distribution is denoted as $Dir(\boldsymbol{\alpha})$, where $\boldsymbol{\alpha}$ is a vector of security event counts α_1, α_2 and α_3, which are the shape parameters for the probability distribution function of

the Dirichlet distribution. Reflected to the message transaction monitoring scenario, α_1, α_2 and α_3 are the number of messages dropped, the number of messages maliciously modified and the number of messages successfully forwarded in time period t, respectively. If surveillance observations would be divided into only two categories, then the Dirichlet distribution could be replaced by the beta distribution, which is denoted as Beta(α_1,α_2). Let observations of dropped messages, maliciously modified or successfully forwarded messages be an observed sequence of $X = (X_1, X_2, X_3) \sim Dir(\boldsymbol{\alpha})$ and $\alpha_0 = \sum_{i=1}^{3} \alpha_i$, then the expected value of each probability p_i ($\sum_{i=1}^{3} p_i = 1$) in the Dirichlet distribution is known as $E(p_i|\boldsymbol{\alpha}) = \alpha_i/\alpha_0$ ($i \in \{1, 2, 3\}$).

The approach based on Dirichlet distribution allows agents to update a node's security belief after transactions between other nodes have taken place. The aggregated ratings for a node A until time period *t* are expressed as $\boldsymbol{\alpha_t} = \{\alpha_{ti}|i \in \{1, 2, 3\}\}$. The simplest way to update a rating value as a result of a new rating is by adding the newly received rating values to the previous stored ones. It is efficient, easily understandable and verifiable, but it is not weighted towards current behavior [12]. Since nodes are changing their behaviors over time and those changes mostly depend on their current behaviors, a forgetting factor $0 \leq \lambda \leq 1$ [13] is introduced to give relative greater weight to more recent ratings. Given $\mathbf{N_t}$ ($\mathbf{N_t} = \{N_{ti}|i \in \{1, 2, 3\}\}$) as the instances of new data arriving during time period *t*, then the accumulated ratings at time period $t + 1$ can be expressed as $\boldsymbol{\alpha_{t+1}} = \boldsymbol{\phi\alpha_t} + \mathbf{N_t}$, where $\boldsymbol{\phi}$ is a vector of forgetting factors: $\phi_i = 1$ means that ratings are never forgotten; while $\phi_i = 0$ denotes ratings are completely forgotten after a single time period and only newly collected ratings are remembered.

B. Preliminary of Game Theory

This work deals with message transaction scenarios. There are suspicious nodes (either service requester or service provider) and a security operator (who configures a surveillance architecture). Hence we take suspicious nodes in the network as one player and the security operator as another player. Obviously, the two players – suspicious nodes and the security operator can not make an agreement since they do not have any motivation to cooperate, so the interactions between them can be modelled as a two-player non-cooperative game. Since observation messages are collected in discrete time periods, we assume that the same game is played repeatedly for a number T (possible infinite or finite) of periods. Such that, the game between nodes and the security operator is a repeated non-cooperative game.

A non-cooperative game γ is a triple $\gamma = (N, H, S)$, where $N = \{1, 2, \cdots, n\}$ is a set of players, $S = \{PS_1, \cdots, PS_n\}$ is a finite family of strategies (or outcomes) for each player, and $H = \{u_i : PS_i \times PS_{-i} \to \mathbb{R}; i \in N\}$ is a family of utility functions of all players. In this paper, $N = \{1, 2\}$ and the set of strategies is $S = \{PS_1, PS_2\}$. $H = \{u, -u\}$ is settled to model a zero-sum regime for nodes and the security operator.

Let a_{ij} represent the payoff from player1 to player2 if player1 chooses strategy $s_i \in PS_1$ and player2 chooses strategy $s_j \in PS_2$. The element a_{ij} corresponds to the value $u(s_i, s_j)$. Let the probabilities of player1's outcomes and player2's outcomes be: $\mathbf{p} = [p_1 \quad p_2 \quad \cdots \quad p_n]^T$ and $\mathbf{q} = [q_1 \quad q_2 \quad \cdots \quad q_n]^T$, respectively. The probability of player1 having outcome s_i and player2 having outcome s_j is therefore $p_i q_j$. Then the expected value of player1's payoff is:

$$E(\mathbf{p}, \mathbf{q}) = \sum_{i,j=1}^{n} p_i a_{ij} q_j = \mathbf{p}^T \mathbf{A} \mathbf{q}. \tag{1}$$

The model matrix $\mathbf{A}$ over the taxonomy $\mathcal{T}$ = {0,1} is denoted as $\mathbf{A}$ = $\{a_{ij}|i, j \in \{1, 2, \ldots, n\}\}$. There exist optimal strategies $\mathbf{p}^*$ for player1 and $\mathbf{q}^*$ for player2 such that, for all strategies $\mathbf{p}$ and $\mathbf{q}$:

$$\begin{aligned} &\forall(\mathbf{p}, \mathbf{q}) \in PS_1 \times PS_2, \\ &E(\mathbf{p}, \mathbf{q}^*) \leq E(\mathbf{p}^*, \mathbf{q}^*) \leq E(\mathbf{p}^*, \mathbf{q}). \end{aligned} \tag{2}$$

The strategy profile $s^* = (\mathbf{p}^*, \mathbf{q}^*)$ is a *nash-equilibrium* in a two-player zero-sum game. Let the sets S(PS_1) and S(PS_2) represent all probability distributions supported on PS_1 and PS_2, respectively. Then the entry $v(\mathbf{A})$ which is the minimum entry in its row and the maximum entry in its column:

$$v(\mathbf{A}) = (\mathbf{p}^*)^T \mathbf{A} \mathbf{q}^* = \max_{\mathbf{p} \in S(PS_1)} \min_{\mathbf{q} \in S(PS_2)} \mathbf{p}^T A \mathbf{q}, \tag{3}$$

is called the saddle-point of payoff matrix $\mathbf{A}$ [14]. There may sometimes be more than one saddle point, but they will all yield the same value for the game.

A simple example is given in the following to elaborate payoff and *nash-equibrium* of a game. Suppose there are two players: player A and player B, and each has two strategies: A_1, A_2 and B_1, B_2. The game between these two players is assumed to be non-cooperative zero-sum. If player A chooses to play A_1 and player B chooses to play B_1, player A receives no payoff ($u_{11} = 0$). But if player B chooses to play B_2 when player A plays A_1, player A receives a negative payoff ($u_{12} = -1$). If player A chooses to play A_2, player A receives a negative payoff ($u_{21} = -1$) if player B chooses to play B_1 and receives a positive payoff ($u_{22} = 2$) if player B chooses to play B_2, respectively. The payoff matrix $\mathbf{A}$ of their game is shown in (4)

		Player B	
		B_1	B_2
Player A	A_1	0	-1
	A_2	-1	2

(4)

and player A's expected payoff $u(A_1)$ as a function of the probability $p(A_1)$ of trying strategy A_1 for this game is illustrated in Fig. 1. The dashdotted line displays the expected payoff when player B chooses strategy B_1 ($p(B_1) = 1$), while the dashed line displays the expected payoff when player B chooses strategy B_2 ($p(B_2) = 1$). Hence, the outcome which

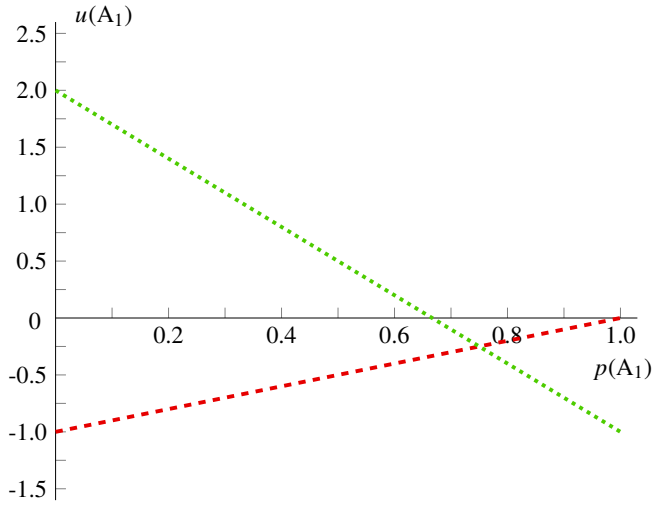

Fig. 1. The expected payoff for the game in (4).

provides the highest payoff for player A is using strategy A_1 with a probability of $p(A_1) = 0.75$. The strategy profile $([0.75, 0.25], [0.75, 0.25])$ is a *nash-equibrium* of the game in (4), as indicated in Fig. 1 and verified by the Gambit software tool [15].

C. Game-theoretic Quantitative Security Assessment

In this work, the network security is considered from two different points of view: network availability and network integrity. The network availability is influenced by whether nodes in the network behave selfish or not. Any degree of freedom in configuring surveillance devices (always on or on-demand basis, different frequencies to check communication links, different locations to monitor nodes, etc) when monitoring a node, can constitute a different entry in the set of PS_1. For a pair of sender and receiver of a message, let these two have identified several ways of communicating (e.g., the choices of cryptographic protocols, the selection of routing paths), which are collected in a set PS_2. For each combination $(s_i, s_j) \in PS_1 \times PS_2$, the network operator receives surveillance observations, which can denote whether a message is dropped, maliciously modified or successfully forwarded. Let $\mathbf{A} \in \mathcal{T}^{n \times m}$ ($\mathcal{T}$ = {0,1} is taken in this work) be the model matrix set up by the security operator. Suppose an honest service requester is requesting services from different service providers. Surveillance devices are assumed to have $n = |PS_1|$ pure strategies (see Section V) for monitoring transactions between the service requester and service providers. Service providers (act as either original senders or intermediate nodes and perhaps are under control of an adversary) have $m = |PS_2|$ pure strategies for transmitting service messages to the service requester. The entry in matrix $\mathbf{A}$ could be a function of the expected probability of dropped messages or modified messages till time period $t+1$. The risk level $\rho(\mathbf{A})$ is then defined as [11]:

$$\rho(\mathbf{A}) := max(\mathcal{T}) - v(\mathbf{A}), \tag{5}$$

where $v(\mathbf{A})$ is the saddle-point value of the zero-sum game. The outcome $a_{ij} = u(s_i, s_j) = 0$ indicates the network is totally unavailable or the transmitted messages are totally modified; while the outcome of $a_{ij} = 1$ indicates the messages are successfully forwarded. $\rho(\mathbf{A})$ is the maximum probability of a message being dropped or modified.

In this paper, probabilities from the aforementioned security belief model (in Section IV-A) are used as prior beliefs and are taken as the parameter of interest that will be updated repeatedly. The combination of prior belief of security events with newly collected data can be represented as a posterior distribution. Each surveillance observation has a probability to be any one of three possible security events, as described in Section IV-A. For a node H_1, suppose his transactions with other nodes will be dropped with probability p_1. Then, the estimated probability (i.e., node H_1's security belief value) that he/she will drop a message updated from the security belief model can be denoted as $\pi(p_1|\alpha_1, \alpha_2, \alpha_3) = Beta(\alpha_1, \alpha_2 + \alpha_3)$, where α_1, α_2 and α_3 are total number of message counts that are dropped, maliciously modified and successfully forwarded, respectively. In this paper, a node's security belief (e.g., aforementioned $\pi(p_1|\alpha_1, \alpha_2, \alpha_3)$) of possible security events will be taken as a prior belief to construct and update the model matrix $\mathbf{A}$ as time goes by.

D. Prediction of Security Incidents

Once the model parameters (e.g, $a_{ij} \in \mathbf{A}$) have been updated, it is easy to calculate the risk level according to equation (5) and its predecessors. However, predicting the point in time where the risk impairing network availability and network integrity will exceed a certain threshold can help informing the security operator when surveillance configurations need to be reconsidered. The accumulated rating for each possible security event can be updated with the model described in Section IV-A. A risk threshold can be fixed and the number of observation messages can be asked for until the risk level exceeds the corresponding fixed threshold. In this way, the evolution of nodes' behaviors can be predicted and the security operator can know how long the underlying network is "secure" (i.e., no message is dropped or maliciously modified). In order to show how network availability evolves, we can simulate dropped message updates and count the number of steps until a chosen threshold ρ_0 is exceeded. If the security operator is more interested in whether messages will be modified, he can simply simulate modified message updates and see the evolution of network integrity. The prediction of security incidents, in the sense of finding the expected time until surveillance configurations need reconsideration, can be done as follows:

1) Pick an unacceptably high risk threshold ρ_0.
2) Determine

$$p_n = \mathbb{E}\pi(p_1|\alpha_1 + n, \alpha_2, \alpha_3) = \frac{\phi_1\alpha_1 + n}{\alpha_0}, \tag{6}$$

where $\alpha_0 = \phi_1\alpha_1 + \phi_2\alpha_2 + \phi_3\alpha_3 + n$ (ϕ_1, ϕ_2 and ϕ_3 are forgetting factors). The expectation (i.e., the security belief) is taken as the probability that a node works as expected.

3) Establish the model matrix $\mathbf{A}$, such that $r_0 = \min_n\{\rho(\mathbf{A}(p_n)) > \rho_0)\}$ is the minimum number of updates to attain the maximum acceptable risk level ρ_0 (see [11] for deep discussion of the optimization).

4) Depending on the time interval in which we receive such updates, the time when a security incident would happen is trivially found.

The number provided is pessimistic. Since only dropped message (or maliciously modified message, when considering network integrity) updates are counted from the security belief model until the risk increases above the acceptable limit. However, successful forwarded message updates can decrease the risk eventually, thus the time when the risk impairing network security exceeds the predefined threshold will be prolonged.

V. Practical Example

Considering an advanced metering infrastructure in which a gateway administrator is supposed to install (or update) a piece of software at a smart meter. The required patches can be obtained from several servers on the Internet. Suppose four different patch servers have such a patch needed by the smart meter. For security reasons, a gateway administrator chooses two of them for querying and verifying the patch (by verifying MD5 checksum). Putting this scenario into our game theoretic risk assessment framework (which can be taken as a transmitting-monitoring game), there are a total of six possibilities for the administrator to monitor message transactions. To make it easy to illustrate, an adversary is assumed to be capable of compromising at most two servers at the same time. In this example, there are six possibilities for the attacker to compromise requested patch servers. Likewisely, this work assumes that there are also six possibilities to monitor message transactions. This example shows how the risk of network availability is analyzed. Assuming all servers in our system drop messages independently with a probability p. The parameter p is updated from the security belief model with the count of dropped messages from new surveillance observations.

After repeating the analysis of transmitting-and-monitoring game, Table I can be derived.

TABLE I
Payoff matrix $\mathbf{A}(p)$ of transmitting-monitoring game

Payoff matrix $\mathbf{A}(p)$		Suspicious requested servers					
		S_1S_2	S_1S_3	S_1S_4	S_2S_3	S_2S_4	S_3S_4
Servers with configured surveillance	S_1S_2	$1-p^2$	$1-p$	$1-p$	$1-p$	$1-p$	1
	S_1S_3	$1-p$	$1-p^2$	$1-p$	$1-p$	1	$1-p$
	S_1S_4	$1-p$	$1-p$	$1-p^2$	1	$1-p$	$1-p$
	S_2S_3	$1-p$	$1-p$	1	$1-p^2$	$1-p$	$1-p$
	S_2S_4	$1-p$	1	$1-p$	$1-p$	$1-p^2$	$1-p$
	S_3S_4	1	$1-p$	$1-p$	$1-p$	$1-p$	$1-p^2$

Starting with parameters $\alpha_1 = 3$, $\alpha_2 = \alpha_3 = 200$, giving the forgetting factors $\phi_1 = \phi_2 = \phi_3 = 0.4$ (these parameters are arbitrarily chosen for illustration), Fig. 2 shows the risk of network availability impairment as a function of vulnerabilities in the light of dropped message updates, by setting the forgetting factor of successful forwarded messages to be $\phi_3 = 0.5$. Fig. 2 shows that forgetting factors have a very big impact on the risk of network availability impairment. With the increase of forgetting factor (from $\phi_1 = 0.1$ to 0.5) for dropped updates count, the risk increases correspondingly. The minimum number of updates (approximately 9, as shown in Fig. 2) that makes the risk level exceed the predefined risk threshold is firstly obtained by the largest forgetting factor. While with the increase of forgetting factor (from $\phi_2 = 0.2$ to 0.7) for maliciously modified updates count, the risk of network availability decreases. From Fig. 2, it can be seen that risks of some curves are firstly higher, however, later lower than the threshold and higher than the threshold again after a certain number of updates. This is because of the *nash-equilibria* computation. These forgetting factors make the game a dynamic one and thus results in big risk value with yet little number of updates.

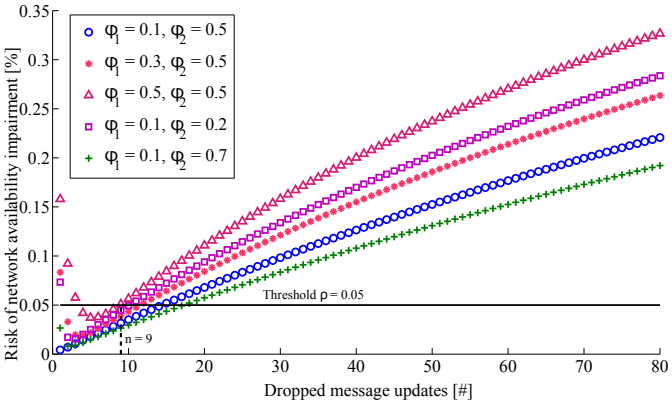

Fig. 2. Risk of network availability impairment in the light of dropped message updates.

VI. Conclusion

This paper presents a simple and light-weight approach for risk assessment and risk prediction in communication networks. It establishes a surveillance architecture to collect the required data for risk assessment. These surveillance observations are interpreted as Dirichlet-distributed security events. This work takes interactions between suspicious nodes and the security operator as a transmitting-monitoring game. Such that, the risk level with certain surveillance configurations is computed and the time point when a security incident would happen is predicted. The results of a simple example demonstrate the effectiveness of the risk prediction system in predicting how long the communication network is "secure" until its security risk exceeds a predefined threshold. The risk assessment framework can execute on an isolated machine and has no impact on the communication network under surveillance. Future works include investigating the impact of uncertainty in surveillance observations on risk levels and

adapting forgetting factors in this framework to the current state of the environment.

ACKNOWLEDGMENT

The research leading to the results presented in this paper was supported by the European Commission's Project No. 608090, HyRiM (Hybrid Risk Management for Utility Networks) under the 7th Framework Pro- gramme (FP7-SEC-2013-1). The authors acknowledge Stefan Rass from Alpen-Adria-Universität Klagenfurt for his valuable discussions and comments.

REFERENCES

[1] G. Ericsson, "Cyber securtiy and power system communication — essential part of a smart grid infrastructure," *IEEE Transactions on Power Delivery*, vol. 25, no. 3, pp. 1501–1507, 2010.

[2] W. Wang and Z. Lu, "Survey cyber security in the smart grid: survey and challenges," *Computer Networks*, vol. 57, no. 5, pp. 1344–1371, 2013.

[3] H. Wei, C. Xia, H. Wang, C. Zhang, and Y. Ji, "A game theoretical attack-defense model oriented to network security risk assessment," in *International Conference on Computer Science and Software Engineering*, 2008.

[4] K. Haslum and A. Årnes, *Computational Intelligence and Security*. Springer Berlin Heidelberg, 2007, ch. Multisensor real-time risk assessment using continous-time hidden Markov models, pp. 694–703.

[5] N. Liao, F. Li, and Y. Song, "Research on real-time network security risk assessment and forecast," in *International Conference on Intelligent Computation Technology and Automation*, 2010.

[6] Z. Ma and P. Smith, *Critical Information Infrastructures Security*. Springer International Publishing, 2013, ch. Determining risks from advanced multi-step attacks to critical information infrastructures, pp. 142–154.

[7] E. T. Department, "Risk management: implementation principles and inventories for risk management/risk assessment methods and tools," European Network and Information Security Agency, Tech. Rep., 2006.

[8] G. Giannopoulos, R. Filippini, and M. Schimmer, "Risk assessment methodologies for critical infrastructure protection. part i: a state of the art," European Commission, Insttitute for the Protection and Security of the Citizen, Tech. Rep., 2012.

[9] P. B. Y. Cherdantseva, A. Blyth, P. Eden, K. Jones, H. Soulsby, and K. Stoddart, "A review of cyber securiry risk assessment methods for scada systems," *Computer & Security*, pp. 1–27, 2016.

[10] S. Rass, B. Raner, M. Vavti, H. Göllner, A. Peer, and S. Schauer, *Mobile Networks and Applications*. Springer US, 2015, ch. Secure communication over software-defined networks, pp. 105–110.

[11] S. Rass, "Towards a rapid-alert system for security incidents," in *Sixth International Conference on IT Security Incident Management and IT Forensics*, 2011.

[12] M. E. Moe, B. Helvik, and S. Knapskog, *Trust Managment III*. Springer Berlin Heidelberg, 2009, ch. Comparison of the bata and the hidden Markov models of trust in dynamic environments, pp. 283–297.

[13] A. Jøsang and R. Ismail, "The beta reputation system," in *Proceesdings of the 15th Bled Conference on Electronic Commerce*, 2002.

[14] S. Rass, S. König, and S. Schauer, *Decision and Game Theory for Security*. Springer International Publishing, 2015, ch. Uncertainty in games: using probability-distributions as payoffs, pp. 346–357.

[15] R. Mckelvey, A. McLennan, and T. Turocy, *Gambit: software tools for game theory, Version 14.1.0. http://www.gambit-project.org*, 2014.