# Telecommunication Networks

**Rasmus L. Olsen, Kartheepan Balachandran, Sara Hald, Jose Gutierrez Lopez, Jens Myrup Pedersen and Matija Stevanovic**

**Abstract** In this chapter, we look into the role of telecommunication networks and their capability of supporting critical infrastructure systems and applications. The focus is on smart grids as the key driving example, bearing in mind that other such systems do exist, e.g., water management, traffic control, etc. First, the role of basic communication is examined with a focus on critical infrastructures. We look at heterogenic networks and standards for smart grids, to give some insight into what has been done to ensure inter-operability in this direction. We then go to the physical network, and look at the deployment of the physical layout of the communication network and the related costs. This is an important aspect as one option to use existing networks is to deploy dedicated networks. Following this, we look at some generic models that describe reliability for accessing dynamic information. This part illustrates how protocols can be reconfigured to fulfil reliability requirements, as an important part of providing reliable data access to the critical applications running over the network. Thereafter, we take a look at the security of the network, by looking at a framework that describes the digital threats to the critical infrastructure. Finally, before our conclusions and outlook, we give a brief overview of some key activities in the field and what research directions are currently investigated.

**Keywords** Communication networks · Smart grid · Inter-operability · Dynamic information access · Reliability · Availability · Cyber security

R.L. Olsen (✉) · K. Balachandran · S. Hald · J.G. Lopez · J.M. Pedersen · M. Stevanovic
The Faculty of Engineering and Science, Department of Electronic Systems,
Aalborg University, Fredrik Bajers Vej 7, Room A4-212, 9220 Aalborg, Denmark
e-mail: rlo@es.aau.dk



E. Kyriakides and M. Polycarpou (eds.), *Intelligent Monitoring, Control, and Security of Critical Infrastructure Systems*, Studies in Computational Intelligence 565,
DOI 10.1007/978-3-662-44160-2_3

## 1 Introduction

Communication networks have become an essential part of our everyday lives and currently, our society is highly dependent on the proper functioning of communication networks. In connection with our private lives, the number of services that are being delivered over these networks is progressively increasing, and probably in the future, new services will appear, all converging over the same infrastructure [1].

Regarding professional aspects, communication networks play a key role in efficiently developing economical activities in a fast, secure, and reliable way. In addition, it is possible to find very powerful companies in the world having Internet services and applications as their main activity, such as Google or Facebook, and they are continuously expanding. In relation to critical applications, the question is whether the existing communication infrastructure can provide the necessary reliability, or whether new networks that allow the harsh requirements of such applications will be needed?

## 2 The Role of Telecommunication

In the early days of telecommunication, communication between two entities was ensured through a physical communication channel between the two entities by so-called circuit switched networks [2]. This type of network ensures a guaranteed bandwidth between the entities, since once setup there are no interferences, and is kept available during the communication. However, setup time is required to ensure the connection is established. Besides the setup time, it should also be fairly easy to imagine the great limitations of these types of networks when considering millions and millions of connected end devices that need communication.

The introduction of packet switched networks allowed the sharing of the limited physical medium among several communicating entities [2], and allowed for a much more flexible communication. The road from the first initial baby steps of a few machines connected over some copper wires done in the late 1960s as a response to the cold war, up to today's full scale hyper complex networks of networks is a study worth in itself [3]. Today, end users have grown accustomed to have access to communication networks more or less everywhere and whenever needed, leaving them with a perception that the Internet is something that just is. This impression has not only been driven by the fact that wired communication offers very high speeds to the individual, but also mobile communication today offers a high data rate due to the technological development [4]. Now, the next step has come, that we want to use the existing communication infrastructure to mission critical applications. One thing is to say "my Internet works nicely at home, and at work it also works nice", but another thing is to put so much trust into the network that we allow critical systems such as water, electricity management, or eHealth applications to run on top of these networks of networks.

## 2.1 Basic Communication Between Two Entities

Critical infrastructures are to a large extent also distributed by nature. In such setting, communication is often required to be able to have elements in the system interact in a synchronized and organized matter. Subsystem A may need to react upon events that happen in subsystem B or vice versa. At the same time, critical infrastructures are often characterized by deadlines due to their connection to the physical world and the properties of the physical world which a critical infrastructure interacts with. Figure 1 shows the example of two communicating physical devices located at different geographical and network locations. These two entities could for example be a water management system that has to interact with remote control units located at strategic points along water pipes.

The data that is required to be passed from A to B and vice versa has to undergo a long way through several routers due to the packet switched approach we have today. At each passing point (router), the received data needs inspection to decide which router the packet should go to next. This may not always be the same for all packets even though their sources and destinations are the same as clever traffic load balance algorithms may be applied to avoid congestions among routers. A data packet route example is illustrated in Fig. 1 as data going up and down in the different levels of the OSI model [2]. In some parts, packets need to be addressed at a network level, while in others only a link level is required. But it is clear that each hop takes some time for the routers to process packets. This leads to an end-to-end delay even though we experience the communication as a direct communication between A and B. The end-to-end delay depends on many factors, such as the quality of each link between routers, network traffic conditions (there may be bottlenecks between some routers), the route through which the data packets are

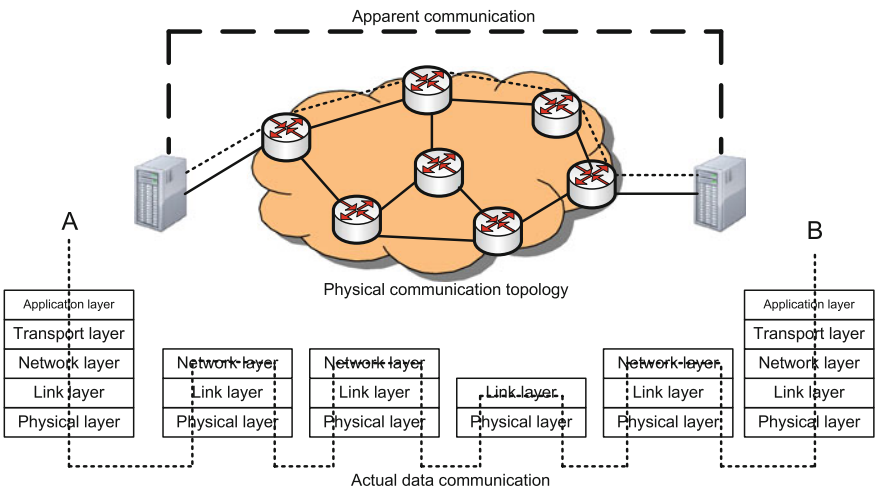


**Fig. 1** Communication between two entities [5]

being sent (this is not controlled by the application, but is impacted by the decisions made by the network). These factors also mean that the end-to-end delay usually shows a highly stochastic behaviour, rather than a desirable deterministic behaviour, and even changes over time, e.g., in some parts of the network there is more traffic during work hours than in night time or weekends.

This complexity of intercommunication needed to transport data from A to B illustrates some key problems that critical applications have when dealing with communication over networks today. There is no or very little control of the data streams going between A and B. When routers receive a significant amount of traffic, they may start to drop incoming packets. Some transport protocols, as TCP aim at providing reliable transport by ensuring retransmission of missing packets, but at the cost of end-to-end delay because it first needs to detect missing packets, and then ask for retransmission. Others such as UDP offer to send data with crossed fingers that it appears at the receiving side. In that case, the application must be able to tolerate packet losses.

Therefore, some of the key challenges that communication systems face, and even considering only two entities communicating, to support critical applications are not necessarily only classical data throughput, but definitely also latency and reliable communication. These key requirements are often assumed, because they are to a large extent hidden to the everyday user, but as communication developers we need to take these issues seriously if critical infrastructures shall be supported by (existing) communication technologies.

## *2.2 Communication over Heterogeneous Networks*

As a further complication, networks are heterogeneous and full of new and legacy systems. Figure 2 shows a conceptual example of how different devices and applications may be connected via a large set of networks of networks. The heterogeneity covers some challenges that may limit some use cases as the following example illustrates:

In order to communicate between two entities an addressing scheme is required (a basic requirement for any type of communication). The most prominent addressing scheme today is IP addressing. In principle, all addresses should be uniquely defined, in order for packets to be sent to the right destination at all times. When the Internet Protocol version 4 was designed and implemented, the space allocated for the address in the protocol allowed for 'only' approximately 4.29 billion unique devices. At the time of development, that was enough, but with the current development this amount has shown to be too small, since all sorts of sensors, mobile devices, multiple interface devices, etc., has ultimately led to an address starvation. This has not been acceptable, so several solutions have been invented to overcome this address starvation, such as Network Address Translation, use of private network addresses, tighter control of Internet registries, network renumbering of existing networks, etc. Even a new IP version 6 has been developed

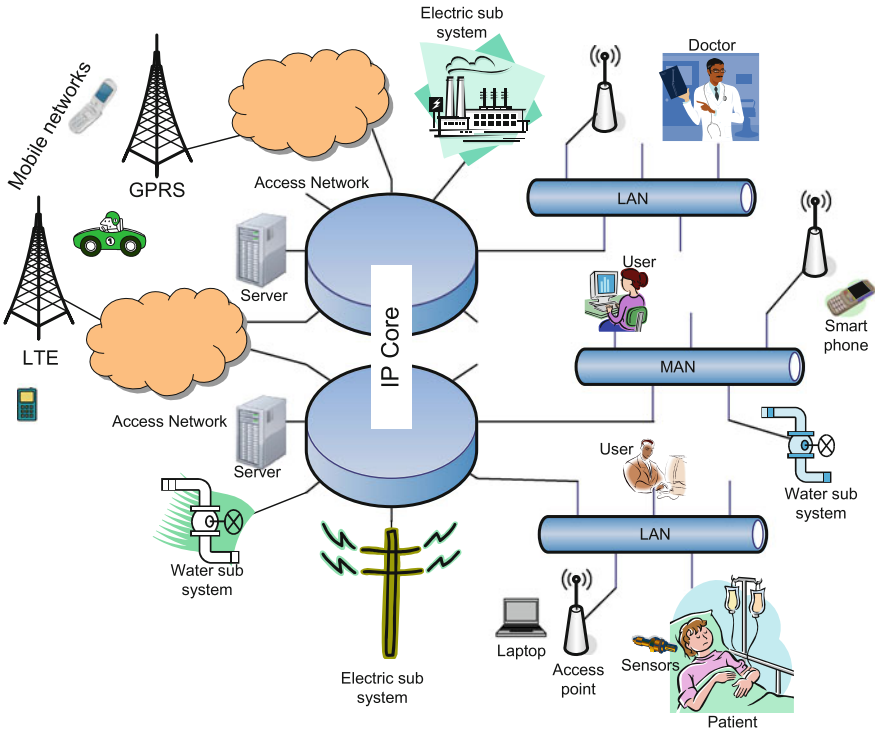


**Fig. 2** Simplified example of networks and connected applications

with a much larger address capacity, but still the earlier IP is being used, since so many devices depend on the stability of this protocol's address space, that in fact no one knows exactly what happens if suddenly software started to use IPv6 [6].

The IP address issue is just one of many examples of the complexity of networks of networks shown in Fig. 2 and how networks even today are challenged by more or less invisible problems. Therefore, once again, one could ask the following question: do we trust these networks to serve as communication media for mission critical applications? Do we dare to let this patchwork of networks, software patches, numerous of standards, protocols and configurations be the bearing part of critical, life depending elements such as electricity, water and health in our everyday life?

Referring to Fig. 2, the vision of several critical applications which interact with the network is shown:

- Doctors who have online meetings with patients, eHealth [7]
- Water detection and control, [8]
- Electric power control, smart grids [9].

On top of this, there will surely be other applications using the network, such as web browsing, video streams, emails, online games, etc. The question is, why should these critical applications use the same network? For example, cars and air planes have several dedicated internal communication networks so as not to mix the application traffic with real time critical data traffic. However, for simplification and cost reduction reasons, research is ongoing on how merge the different data traffic [10].

The time, effort and cost of deploying the Internet as it is today is immense. Deploying a separate network for each of the applications that is envisioned does not appear to be a very attractive solution if we somehow are able to ensure the existing infrastructure can support the requirements of the critical applications. A major key to the solution is the flexibility of the network as it is today. As a corner stone design idea of the early Internet (from ARPANET [3]), the idea of robustness to link failures has been eminent, which is a key feature for critical infrastructure as well as not having to deploy net networks from scratch. However the complexity and heterogenic nature of communication due to legacy systems requires interoperability and standards. In the following we take a closer look at how this is being addressed in the smart grid as an example.

## *2.3 Communication Standards for Smart Grids*

In smart grids, data from consumers and potentially also from the power grid infrastructure is required to be collected for control purposes. This not only means communication over heterogeneous networks, but also with a wide range of communicating entities, smart meters for example, produced by different vendors. Today, the core purpose of the meters already developed is to monitor power usage for e.g., electricity bills [11]. However, the data also have value for the utility company.

In smart grid terminology, being able to remotely read the meter is called automatic meter reading (AMR) and is a part of the automatic metering infrastructure (AMI), i.e., the network between the smart meter and the utility company [12]. With an AMI network the monitored data from a household can be sent to the utility company, which can use it to optimise their production of power and thereby avoiding over/underproduction.

AMI has been addressed in various projects like Power Matching City [13] and others [14, 15] and it has been shown, that using the data from monitoring systems can lead to optimisation of the demand and response (DR) [16, 17]. However, it is not clear what are the requirements for the communication network. For example, the authors in [13] have made a living lab to demonstrate a smart grid. In the chosen setup, dedicated ADSL communication lines are used for AMI in order to avoid human interference. The purpose of this is to make sure that they have enough bandwidth for the communication. Nevertheless, the requirements for the networks are not mentioned. Implementing dedicated communication lines only

for the smart grid communication is very expensive and not a feasible solution for all cases of AMI.

Furthermore, the data can be used by the utility company to act as an energy consultant, to advice the customers how to save money based on their power usage data and additionally offer free or cheaper electricity during overproduction periods to encourage their customers to use power consuming devices, for example heat pumps, or allow the utility company to perform Direct Load Control (DLC) by controlling the customers devices and Distributed Energy Resources (DER) [18]. Being able to control e.g., heat pumps, electric cars and other DER's, makes it possible for the utility company to control and level the peak periods in the power grid by remotely turning on/off specific units in order to take off load or supply more power to the grid appropriately [16].

In Denmark, the Danish Ministry of Climate, Energy and Building has published a report in October (2011) about Smart Grid in Denmark [70]. In the report they encourage further research and development in smart grid and also mention communication as a vital part of the smart grid.

## *2.4 Standards for Smart Grids*

Mapping requirements for critical infrastructures is a challenging task, because the smart grid is a large complex infrastructure with different layers of networks, which gives a diversified communication performance expectation [18]. IEEE and IEC have already proposed a number of standards regarding the communication in smart grid in different layers. One of the most commonly used standard is IEC 61850, which focuses on the substation automated control and is used in the Danish smart grid project in Bornholm called ECOGRID [71] and for the AMI there is IEC 62056 [19, 20]. In the following some communication standards are mentioned which are proposed for different parts of the smart grid.

*IEC 61968-9 and 61970*: Defines the common information model for data exchange between devices and networks in the power distribution domain and the power transmission domain respectively. They are used in: Energy management system [21].

*IEC 60870-6*: Defines the data exchange model between the control center and power pools. It is used in: Inter-control center communication [21].

*IEC 61850*: Defines the communication between devices in transmission, distribution and substation automation system. It is used in: Substation automation [21].

*IEEE P2030*: Defines the inter-operability of energy devices and IT operation with electric power systems. It is used in: Customer side application [21].

*IEEE 1646*: Defines the communication delivery times to substation. It discusses the requirements of the system to deliver real-time support, message priority, data criticality and system interfaces. It is used in: Substation automation [21].

**Challenges for the smart grid network:** Other challenges in the communication network in smart grids, relates to delay, availability and security [12, 15, 18].

If the utility company is expected to control the distributed energy resources (DER), delay becomes a critical metric in the network performance. The delay in the network will have a high impact on the grid if the DERs are not activated or shutdown on time; thus, some sort of message priority scheme in the communication protocol will be required [18, 22]. Availability and reliability of the network are of importance to ensure the grid operation and also plays a vital role in the demand response [23, 24]. Security is crucial to the smart grid. When extracting information from the user, the privacy of the user has to be secured. The grid can also be vulnerable to terrorist attacks if the control messages to control various electric devices are hijacked [25]. Adding security can have an impact on the delay, as the messages have to be encrypted. Another way to add security is by not letting the hacker know where these control messages come from or go to. For this, an anonymous packet routing with minimum latency has been proposed [26].

There are a number of challenges in the communication network for smart grid. The standards proposed still have to be implemented and tested in many scenarios, in order to examine the network performance. There is still a need for research in protocols that can deliver messages safely according to the time constraints specified by the different standards.

## 3 Design of Critical Optical Transport Infrastructure

Communication networks have become an essential part of our everyday lives and our society is highly dependent on the proper functioning of communication networks. In connection with our private lives, the number of services that are being delivered over the data networks is progressively increasing, and probably in the future new services will appear, all converging over the same infrastructure.

Regarding professional aspects, networks play a key role in efficiently developing economical activities in a fast, secure, and reliable way. In addition, it is possible to find very powerful companies in the world having Internet services and applications as their main activity, such as Google or Facebook, and they are continuously expanding.

Telecommunication systems have been evolving for the past 10 years, towards the unification of services and applications over the same infrastructure [27]. Currently, it is possible to identify how this initiative is partially followed by operators providing voice, data and video transmissions over the same access connection, known as Triple Play. However, the distribution networks of these services are not unified physically. For example, the TV and telephony infrastructures are traditionally separated. The unification of these infrastructures implies ambitious requirements to be supported by the network, for example due to the heterogeneity of the traffic flowing through, or the significant profit losses, or the number of affected users when loss of connectivity occurs [28]. Examples of recent cable cuts in optical networks are:

- In the beginning of 2008, the cable connecting Europe and Middle East suffered four single cuts, affecting millions of users [29].
- In April 2009 AT&T suffered cable cuts, perhaps due to vandalism, in the area of San Jose and Santa Clara, California, leaving many of Silicon Valley businesses and customers without phone and data services [30].
- In July 2011 35,000 broadband customers were affected for several hours by a cable cut caused by a truck in Washington State, USA [31].

Looking back it is possible to realize how fast the world of communications has evolved. For example, in 2009 the 40th anniversary of the first ever data transmission over ARPANET was celebrated. This fast evolution of communication technologies and services is causing a gradual increment of the bandwidth and reliability requirements to be fulfilled by the network infrastructure [32].

In addition, the traffic supported by the Internet has significantly grown over the last few years, shaping up the requirements that future networks need to handle. In order to be able to support all the traffic and quality of service demands, there is a need for high performance transport systems, and focusing on the specific field of this work, **a highly reliable optical backbone infrastructure** [33].

The interest is especially increasing regarding optical transport networks, where huge amounts of traffic are continuously traversing their links. Inefficiencies or disruptions on delivering the information become critical at this level, due to the number of simultaneously affected users. All these huge flows of information must be efficiently distributed using reliable high capacity transport networks. Bandwidth requirements clearly indicate that the optical network technology based on wavelength division multiplexing (WDM) will play a key role regarding this issue [34].

## 4 Planning the Physical Infrastructure

The deployment of optical networks is a long and expensive process, due to the trenching tasks involved, especially for large geographical areas such as national or continental territories. It can take 10–15 years to deploy such networks under the cost of millions of euros [35]. Moreover, the lifetime of the physical infrastructure is rather long, between 30–50 years [36, 37]. These features make such a network deployment a long term investment project, which should be carefully planned. In addition, when this high investment is combined with a **reliable**, **preventive** and **green** planning, a better outcome can be achieved [35].

Optical network systems are very complex; each of the network layers can have great impact on the overall performance, going from physical to application layers. In relation to backbone networks, the infrastructure can be limiting the global performance of a network just by the fact that the physical interconnection scheme has not been carefully planned [28]. In fact, when the network requires some kind of physical upgrade, the solution's costs in economic terms might be much more significant, due to trenching and deployment tasks, than at higher layers where software updates might be enough to solve the problem [38].

Hence, networks should be planned and designed to provide high performance and high availability in transmissions. As the economic relevance of these networks is increasing, it is also feasible to increase the investment for their deployment. This capital increment opens up a whole new space of possibilities when designing the network's interconnection. Planning is crucial and even small improvements may have high economic impact. However, no well documented methods exist for the whole interconnection planning process leaving room for the development of this work.

The main overall challenge can be described as the physical interconnection decision problem of a set of nodes. This interconnection can be configured in many different ways, and several of these might be "optimal", depending on the objective function and constraints of the optimization. In this case, two of the most relevant objective functions are: *Deployment cost minimization* and *average connection availability maximization*.

The main problem is how to cover these two aspects in the same optimization process, as they are contradictory. Usually, the minimization of deployment costs would imply a negative effect on the availability of the designed networks. The number of deployed links to interconnect the nodes is compromised, in order to achieve the minimization goal. This can be avoided by conveniently selecting the proper constraints in the search process. The feasible solutions spectrum can be reduced to graphs that a priori will provide good solutions in terms of availability and not be extremely costly. Three-connected graphs are a good possibility to implement such transport networks. This type of graphs is discussed below, but first the models regarding deployment costs and availability should be introduced.

**Definition 1** *A graph is k-connected when any* $k-1$ *elements, nodes or links, can be removed from the network and still maintain a connected graph.*

## 4.1 Deployment Cost

There are three main contributing elements regarding the economic costs for deploying optical transport networks using WDM technology: trenching, nodes, and fiber spans. These are considered to define the following deployment cost model used in this work but new elements may be included at a later stage. Some of these concepts can be found in [39] and a complete review on the architecture of optical networks can be found in [34].

Let $I_{NT} = I_{links} + I_{nodes}$ be the total cost of deploying a network. $I_{links}$ is the cost of deploying the links and $I_{nodes}$ is the cost of deploying the nodes. Each existing link is characterized by its length, $Lm_{ij}$, and the traffic traversing it, $Ld_{ij}$. Not all pairs $i-j$ have an existing link. Basically, three cost parameters can be defined to calculate $I_{links}$: $I_{trench}$, $I_{fix}$, and $I_{span}$.

$I_{trench}$ corresponds to the price for the trenching tasks per km and its value can significantly vary, depending on the region or landscape. $I_{fix}$ corresponds to the fiber terminating equipment, and $I_{span}$ is the cost related to each fiber span where ducts, fiber and amplifier costs are included. The length of each span $L_{span}$ can vary from 50 to 100 km [36].

Therefore, $CW$ being the wavelength ($\lambda$) capacity and $W$ being the number of $\lambda's$ per fiber, the number of fibers $nf_{ij}$ for the link between nodes $i$ and $j$ is defined in Eq. (1). The number of amplifiers, $nla_{ij}$ in a link is defined in Eq. (2). Consequently, the economic costs for deploying the links of a network $Top$, $I_{links}$, is formally defined in Eq. (3).

$$nf_{ij} = \left\lceil \frac{Ld_{ij}}{CW \cdot W} \right\rceil \tag{1}$$

$$nla_{ij} = \left\lfloor \frac{Lm_{ij}}{L_{span}} \right\rfloor \tag{2}$$

$$I_{links} = \sum_{\forall\, i,j \,\in\, S_N} \left( I_{trench} \cdot Lm_{ij} + 2 \cdot nf_{ij} \cdot I_{fix} + \left( \left\lfloor \frac{TRF_{ij}}{L_{span}} \right\rfloor + 1 \right) \cdot I_{span} \right) \tag{3}$$

Regarding the nodes, $I_{nodes}$ can be divided in two parts; the facility cost, $I_{fal}$, and the switching cost, $I_{swch}$, related to each switch size. The switch size is given by the number of incoming and outgoing fibers to each node and the number of wavelengths per fiber. Usually standard switch sizes are given by $2^m x 2^m$ for $0 < m \leq 5$, and $I_{swch}$ is not linearly proportional to $m$ [40]. Concluding, $I_{nodes}$ is formally defined as Eq. (4).

$$I_{nodes} = N \cdot I_{fal} \sum_{\forall\, i \,\in\, S_N} I_{swch}(i) \cdot W \tag{4}$$

## 4.2 Availability

Availability is a convenient parameter for measuring the efficiency of the network infrastructure regarding failure support. Availability is defined in [36] as follows: "*Availability is the probability of the system being found in the operating state at some time t in the future, given that the system started in the operating state at time t = 0. Failures and down states occur, but maintenance or repair actions always return the system to an operating state*".

Availability in optical networks has been widely studied. For example, [41] presents an interesting availability review of Wavelength-Division Multiplexing (WDM) network components and systems. In terms of connection availability analysis, [42] compares the availability results between simulation and analytical environments for a shared protection scenario. Also, in [43] an interesting approach

is followed to evaluate the availability in optical transport networks. It is measured in expected traffic losses when failures occur.

Availability is mathematically defined as the *working time/total time* ratio. Let *MTTF* be the Mean Time To Fail of any element or system and *MFT* be the Mean Failure Time. Availability *Av* is presented in Eq. (5), resulting in a numerical value of $0 \leq Av \leq 1$.

$$Av = \frac{MTTF}{MTTF + MFT} \tag{5}$$

The availability in relation to an $s - d$ pair connection is given by the availability calculation of sets of elements in series and in parallel. For each provided disjoint path to be available, all of its elements must be available. For a connection to be available, at least one path must be available.

Let $Av_{pj(s,d)}$ be the availability of each $j$ of the provided $k$ disjoint paths between $s$ and $d$. $m_j$ is the number of elements of path $p_j(s,d)$, each of these characterized by an availability $Av_i$. Equation (6) presents the calculation of the availability for each path. The connection availability for an $s - d$ pair, $Av_{C(s,d)}$, is presented in Eq. (7).

$$Av_{pj(s,d)} = \prod_{i=1}^{m_j} Av_i \tag{6}$$

$$Av_{C(s,d)} = 1 - \prod_{j=1}^{k} (1 - Av_{pj}) \tag{7}$$

### 4.3 The Graphs

The decision of how to deploy optical links to interconnect network nodes is a complex problem. Its combinatorial nature makes it impractical to make the interconnection decision using exhaustive search methods. Heuristics may provide a good approximation to optimal results while Integer Linear Programming would be the ultimate approach.

In relation to the distribution of the links, currently it is widely accepted that these ring interconnections are reliable enough for the demands of the users. However, if the current evolution of telecommunication demands keeps heading towards a more IT dependent society, higher degree physical networks (>2) can significantly contribute to the improvement of failure support, congestion control, or delay propagation aspects due to multipath options. For example, in the long term, it might be cheaper to build more reliable networks than less reliable networks that require higher maintenance investment to keep similar availability levels. Therefore, 3-connected graphs could be the natural evolution for this type of networks [44].

Consequently, networks formed by 3-connected graphs are capable of supporting two simultaneous failures, links or nodes, and still maintain connectivity between any pair of nodes.

### *4.4 Illustrative Example*

The **main goal** of this example is to identify the deployment cost versus availability consequences of using 3-regular, 2- and 3-connected graphs to interconnect several sets of nodes. The number of links in all options is the same but their different distribution of the links implies different performance characteristics. In order to obtain concrete numerical results, three scenarios are presented. These consist of sets of 16 nodes in Europe, US, and Asia to be interconnected.

This experiment consists of designing the interconnection for these sets of nodes following these topologies: Single Ring, *SR*; 3-regular 2-connected, $D3_{2C}$; and 3-regular 3-connected, $D3_{3C}$. The *SR* is the shortest 2-connected topology and it is used as a lower bound reference.

Downtime and capacity allocation are determined considering two disjoint paths (1:1 protection) in the *SR* case. In the $D3_{2C}$, three disjoint paths (1:1:1 protection) are provided between pairs of nodes, if possible; for the rest, two disjoint paths are used. In the $D3_{3C}$ case, three disjoint paths are provided between each pair of nodes. The interconnections are optimized in terms of deployment costs, and the cost and availability models presented above are used. Details about this experiment, and Figs. 3 and 4 can be found in [45].

Figure 3 presents the comparison of deployment cost vs. downtime in the three scenarios. The pattern followed by the results in the three cases is similar, and it can be noticed how the improvement of moving from the $D3_{2C}$ to the $D3_{3C}$ is more significant than moving from the *SR* to the $D3_{2C}$. The slope of the lines between points can be interpreted as the availability benefit of increasing the deployment costs, the steeper the better. Figure 4 illustrates the resulting $D3_{3C}$ graphs for the three scenarios.

In summary, to deploy $D3_{3C}$ graphs is slightly more costly (between 2 and 11 % higher) than the $D3_{2C}$ option, but the improvement on availability pays off the extra investment by reducing the yearly downtime between 230–400 times.

## 5 Reliable Access to Dynamic Information in Critical Infrastructures

As a part of dependability, reliability of the system and information being accessed is critical. In many situations in critical systems, events are happening and require reporting to a server that will take action upon the event. In this matter, it is critical

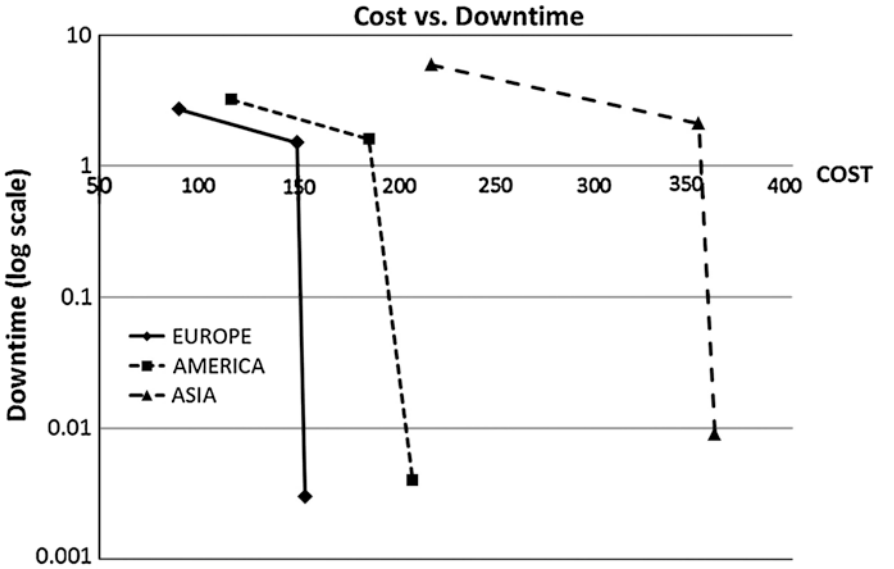


**Fig. 3** Cost versus downtime

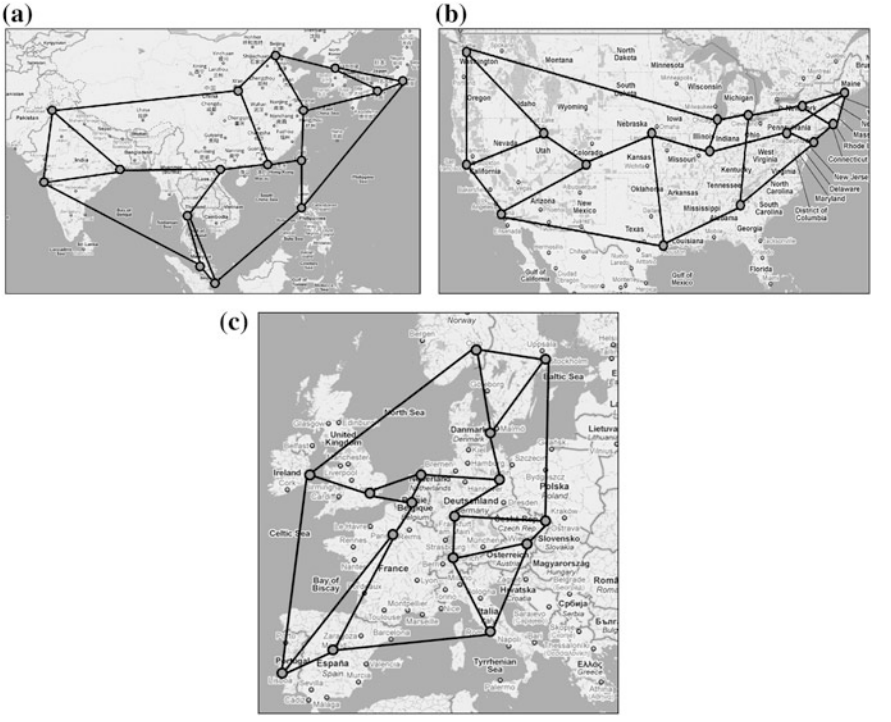


**Fig. 4** 3-connected solutions. **a** Asia, **b** America, **c** Europe

that the server reacts upon the situation as it is, and not how it was moments ago. In the following we consider the communication between two entities A and B, at different geographical and network locations, with A having a need to obtain information from B which happens to be dynamic, and this access needs to happen over a (complex) network with a stochastic end-to-end delay (see e.g., Fig. 1).

In [46] we evaluated the impact on different access strategies to dynamic information elements over a network. The access scheme models are generic meaning that they do not model any particular protocol, but rather the behaviour of one. The delays involved are described statistically such that any stochastic models based on MAC, IP or Application layer can be incorporated. The models consist of the following three basic schemes: reactive access, proactive event driven and proactive periodic.

Then, for the following we consider the stochastic processes

- An Event process $\mathcal{E}$, if Poisson with rate $\lambda_e$. $E = \{E_i, i \in \mathbb{Z}\}$, where $i$ the $i$th event number.
- An upstream (A–B) and downstream (B–A) delay $\mathcal{D}$, if Poisson with rate $v$, and indices $u$ and $d$ for upstream and downstream, respectively. $D = \{D_j, j \in \mathbb{Z}\}$, where $j$ the $j$th delay.
- An Access Request process $\mathcal{R}$, if Poisson with rate $\mu_r$. $R = \{(R_k, k \in \mathbb{Z})\}$, where $k$ indicates the $k$th request.

The definition of an event may not be unique, but by event we here mean a *significant* change in the value of some attribute or information element of interest. Significant can for example be if a signal exceeds some threshold or simply takes another enumerated value.

## 5.1 Reactive Access

The reactive access is characterized by A sending a request for information to B. Once B receives the request, it sends back the response to A containing the information and A will use this information for some purpose, for example as input for a smart grid control. Then we can calculate the probability of A using outdated and mismatching information as [46],

$$mmPr_{rea} = 1 - \int \overline{B}_E(t) F_D(dt) \tag{8}$$

where $\bar{B}_E(t)$ is the CDF of the backwards recurrence time (see [46] for details) of the event process, and $F_D(t)$ the CDF of the delay (with the bar indicating the reliability function, i.e. $\bar{F}_X = 1 - F_X$). Here traffic is only generated whenever needed. The average waiting time is entirely defined by the sum of the upstream and downstream delay. The result obtained from B may also be cached at A, on which for some time period any requests are fetched from the local cache rather

than sending requests to B. The mismatch probability model for that case is rather complex (see [47]) for details. Applying a cache means also that network traffic is in average reduced, as well as the average waiting time.

## 5.2 Proactive: Event Driven Update

Another option is that B, which collects the data, sends an update to A if it detects an event has occurred. In this way, network traffic is only generated whenever events occur, however, if the event process is rather fast this can become a rather large amount of traffic. The mismatch probability for this approach can be calculated by considering two types of updates: (1) if each update contains full information, i.e., each update completely overwrites existing value at A, or (2) if each update only provides the incremental value since the previous update. For case (1), the mismatch probability becomes exactly the same as for the reactive strategy, but for (2), the mmPr can be modelled by considering the probability of finding a $G/G/\infty$ queue being busy, with queue elements modelling updates in transit. If just one is in transit, then there will be a mismatch (see [46] for further details).

$$\mathrm{mmPr}_{pro,evn}^{(inc)} = \mathbb{P}(E/D/\infty \quad queue \quad is \quad busy) \tag{9}$$

## 5.3 Proactive: Periodic Update

This approach relies on B sending the current value or state of the information to A with a time period specified in one way or another. The traffic generated by this approach is entirely determined by the update rate. The mismatch probability for this approach is based on a thinned Poisson update process. This also means that the update process is stochastic, while it normally is deterministic. However, due to clock and scheduling drift in operating systems, and the fact that a deterministic update process (via simulation studies) shows to provide better reliability, this assumption serves as a worst case scenario. Thus, the model becomes

$$\mathrm{mmPr}_{pro,per} = \int_0^\infty \exp\left(-\int_0^t \tau F_D(s)ds\right) A_E(dt), \tag{10}$$

with $\tau$ the update rate, $F_D$ the delay distribution and $A_E$ the backward recurrence time, [46].

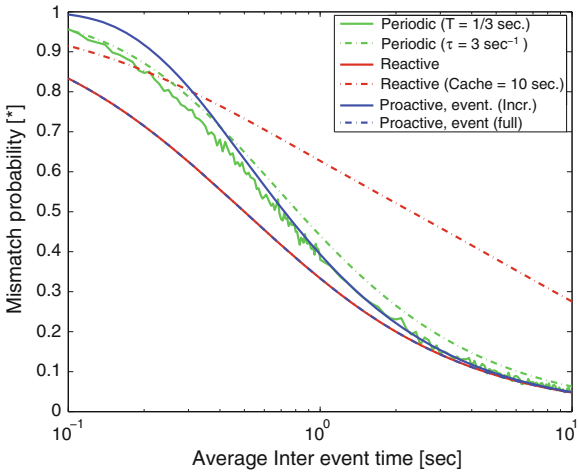


**Fig. 5** Mismatch probability as a function of the event rate for different access strategies, for a symmetric delay of 500 ms and request rate of avg. 0.1 req/s

## 5.4 Impact of Access Strategy on Reliability

Figure 5 shows the mismatch probabilities for the different access strategies with varying event process rate, under the assumption that the involved processes are all exponentially distributed (for simplicity). The effect is clear for this situation: there is not only a significant impact, but also a very different impact on the different strategies, which makes it less clear which approach is actually the best.

Although it appears as if the pure reactive and event driven (using full update) appears to perform best, one also has to consider that the traffic generated is different (reactive in this case is 0.2 messages/s, event driven in the range of 0.1–10 messages/s compared with the periodic one which is 1/3 message/s). Thus, in case of scalable systems such as smart grids where several thousands of customers provide data regularly, the solution of which strategy to take is not necessarily clear.

## 5.5 Impact of Event and Delay Processes

It is also not just the event rate that has an impact on the reliability. If there are restrictions to which values an information source can attain, e.g., a lamp is either on or off, and that is the information needed for e.g., a smart grid solution, then this additional information on restriction has an additional effect on the reliability. Figure 6 shows an example of a case where information can only be in one of two states (ON or OFF), with the ratio of time spent in one or the other state ($\zeta = \lambda/\mu$, with $\lambda$ and $\mu$ as the rates at which the information changes states in a two state Markov Chain).

The figure shows that there is a maximum mismatch probability at the ratio of 1, i.e., when there is equal probability of finding the information in one of the two states. Any other ratio gives a lower mismatch probability due to the biased time

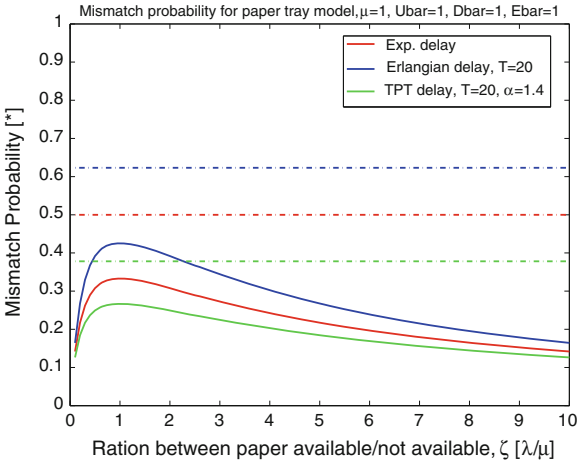


**Fig. 6** Mismatch probability for an ON/OFF type of information model

spent in one or the other state. In comparison, the same process modelled as a Markov jump process instead, shows not only the obvious that the ratio does not have an impact, but that the resulting mismatch probability is higher than the two state model at any point.

Another important aspect which is shown in Fig. 6 is that the delay process is important too (in fact the following observation is equally valid for the event process too—that is as long it is not a recurrent process). The figure shows three results of the same plot, coming from three different distribution types: (1) an exponential distribution, (2) an Erlang distribution with 20 phases, and (3) a Truncated Power Tail (TPT) with 20 phases, all with the same mean value. The results, which are consistent with other results shown in [46], show that the deterministic process (modelled by the Erlang distribution) is far the worst case, i.e., resulting in the highest mismatch probability. The best case is the highly stochastic type of information modelled by the TPT distribution.

This is indeed good news for example for smart grid solutions, where the most stochastic elements are those which will need to be observed, while the deterministic elements are often those which will need or can be controlled, and thus do not need much other observation than perhaps a feedback whether the element has been activated or not. Take the example of a lamp, TV, or other similar device such as a household device which has a level of stochastic behaviour which may be modelled e.g., as an ON/OFF model as shown in Fig. 6.

## *5.6 Network Adaptive Access Strategies*

One example of how the models can be useful is the selection of the update rate of the periodic strategy. Figure 7 shows how an appropriate choice of update rate ($\tau$) in the periodic scheme can lead to a consistent reliability, set here to 0.3. However,

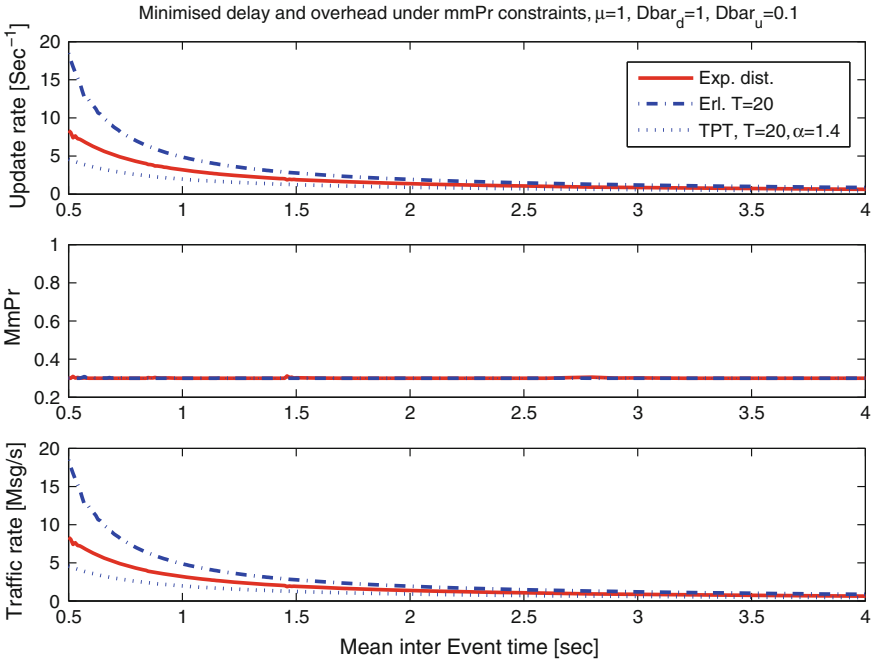


**Fig. 7** Mismatch probability for an ON/OFF type of information model

this comes at a cost of an increased network overhead which in theory can rise to an infinitely fast update rate (this is of course unrealistic).

Similarly, an appropriate caching period can be selected to keep reliability (see [47]). Therefore, these models offer a large range of possibilities for reconfiguration of protocols which have the above mentioned type of interaction for dynamic information. However, as already discussed, networks are not static, and end-to-end delays are not necessarily similar over the days, weekdays or months. Therefore, these processes should be monitored and estimated, which is not trivial and requires software components, [67–69]. But, if done properly, algorithms via observations of information access request rates, data sizes of requests, and knowledge of the delays and event processes can be provided for proper selection and configuration of access to dynamic information for reliable operation. Then, the selection of metrics becomes a matter of how much traffic a system is allowed to create and how high requirements to the reliability of the information one has. A proposal for such an algorithm that utilizes the mentioned aspects has been described and evaluated in [48].

### 5.7 Summary

From this section we learned that the information access, the dynamics of the information, and the delay are closely related to reliability. Mismatch probability is a probabilistic notion on how certain dynamic information accessed remotely is, when being used for whichever purpose. The more likely it is that the information is correct, the more likely a correct system behaviour will occur. Unless dedicated networks are set up where data can be reliably scheduled, future critical infrastructure will have to face such challenges thus only probabilities for success can be given, and the cost of deploying networks is not to be underestimated as we will look into later in this chapter.

## 6 Security and Threats to Critical Infrastructure

Networks are controlled by software, and as such they are vulnerable to flawed designs in protocols, implementation bugs, exploits and so forth, and every opened communication channel generates principally for a possible attack opportunity. In today's world where for example terrorism is in focus, securing networks when used in critical infrastructures is more important than ever. Securing networks is a continuous battle against an invisible and sometimes unknown enemy, and in war, one of the most fundamental elements for a successful defense is to know and understand the enemy. Therefore, in this section we propose a framework for analyzing digital hacker threats to critical infrastructures [49, 50].

As the digital aspect of society and our lives in general becomes ever more important, the defence hereof becomes an increasingly higher priority. Billions of dollars are spent each year to protect the systems that form the basis for our everyday lives against malicious attackers who would steal our data or sabotage our critical infrastructures. It is an uneven battle—attackers need to be successful only once, while the defenders must be successful every time. Therefore it is imperative that we know as much as possible about the potential attackers and their methods to be able to prioritize the defence efforts. If we know the potential attackers, we are able to predict, detect and manage possible attacks.

To do this, it is necessary to make a threat assessment for the systems in question [51]. Threats can be divided into three categories: natural disasters, accidents, and attacks. Traditionally, attackers are considered to be the same attackers who would attack the installation/system in the physical world (e.g., criminals and terrorists), with an added category of "hackers" [52, 53]. However, "hackers" is such a loose term that by grouping all attackers into this one category, it is very difficult to say anything specific about important threat properties.

For an assessment of the hacker threat to critical infrastructures to be useful, it should have a greater granularity with respect to the attacker identification. By dividing the "hacker" category into a number of subcategories, for which we can

determine specific threat properties, it is possible to give a much more precise picture of the threat. We divide the hackers into eight categories:

- Script kiddies
- Insiders
- Gray hats
- Hacktivists
- Cyber punks
- Petty thieves
- Professional criminals
- Nation states.

The motivations behind each of the categories of hackers can be represented by a circumplex, as illustrated in Fig. 8. Each of these categories will be evaluated separately, whether or not they represent a sabotage threat against critical infrastructures. In this context, the sabotage is considered as reducing or removing the availability of the service provided by the critical infrastructure. In terms of cyberattacks, this can be achieved for instance, by a malicious use of controls, (Distributed) Denial of Service (DDOS) attacks, or worms [54]. These are the vectors that will be considered. The threat assessment is performed by comparing hacker motives (intent) and capabilities (competencies and available resources) [51], with the profile of the targeted critical infrastructure. This profile is described widely in the literature, e.g., in [55] and [56], and will be summarized in the following section. Obviously, the first step is to generally protect the infrastructure, by making sure that it is not vulnerable to common security threats. Therefore, in

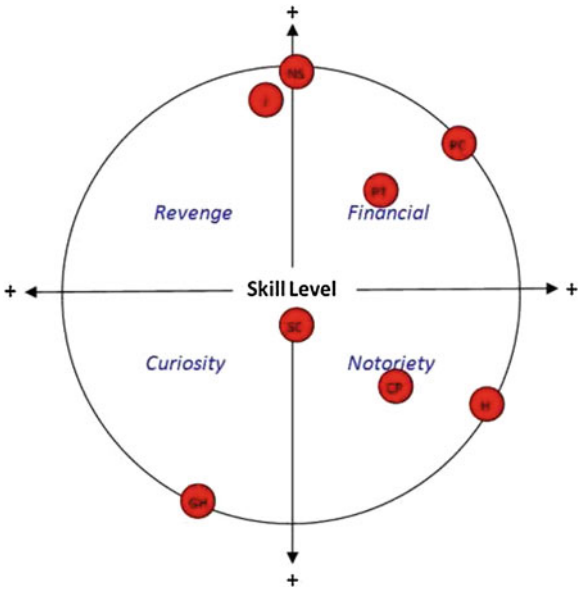


**Fig. 8** Circumplex illustrating motivations behind each of the categories of hackers

the rest of the section we will assume that appropriate action has been taken to ensure this, and we will focus on more advanced/severe kind of attacks.

**Intent**: Critical infrastructure is a high-profile target that provides critical services to the area it is located in, indicating that attackers with Notoriety or Revenge motives would find critical infrastructure tempting targets. The return on investment on sabotaging critical infrastructure for money is very low because of the high security and the lack of monetary gain, so Financial motives are not likely to drive a hacker to this type of attack. And while Curiosity might cause an attacker to try and break into critical infrastructure, it is unlikely that it would spur the hacker to perform sabotage [57].

**Triggers**: Critical infrastructures, being high-profile targets, do not need any special triggers to be attacked. However, since critical infrastructures are often state-run and a necessity for a state to run, attackers with revenge motives could be triggered to attack at a perceived threat or insult from the government of the state in question.

**Capabilities—skills**: Critical infrastructures should be and usually are assumed to be protected against common vulnerabilities; the systems are updated and protected by security solutions. Therefore it takes either a significant amount of very specialized skills to break the defences and/or considerable resources [58].

**Capabilities—resources**: For sabotage of critical infrastructures to be really effective, several facilities need to be hit for prolonged periods. This requires either huge amounts of resources to be able to hit several systems in parallel and sustain attacks, or very specialized skills and insider knowledge to create cascading effects between networked systems.

**Methods**: While critical infrastructures are generally well protected, no system is completely secure. Critical infrastructures are vulnerable to all considered attack vectors (malicious use of controls, DDoS attacks, and worms) if the attackers utilize them with enough resources and/or skills.

**Trends**: The increased focus on cyber security in the society in general also has a positive effect on the security awareness of critical infrastructures. One example is that industrial control systems are generally better protected after the Stuxnet incident made everyone aware that they are a potential target [59].

In the following we will use these threat properties to discuss to which extent the different hacker categories have the will and the capabilities to execute successful attacks specifically against critical infrastructures.

## *6.1 Script Kiddies*

Attackers of the Script kiddies category are novices with low hacking skills and limited understanding of technical consequences, who use tools or scripts downloaded from the internet.

**Intent**: Primary motivations for Script kiddies are notoriety and curiosity, and as such critical infrastructure being a high-profile target would be attractive, but

the tools used by Script kiddies often choose targets at random (for example, The Honeynet Project (2004)).

**Triggers**: The only trigger Script kiddies need to attack is the opportunity. If they find a vulnerability in their random, automated search, they will exploit it.

**Capabilities—skills**: Low technical competencies makes it highly improbable that a Script kiddie could execute a successful attack against a target with a minimum of up-to-date defences. This is expected to exclude critical infrastructures from their targets.

**Capabilities—resources**: Having very little resources available and operating solo further decreases the probability of a successful attack.

**Threat assessment**: Have the will but lack the capabilities.

## *6.2 Cyber Punks*

Members of the Cyber punks category are medium-skilled but mostly solitary hackers and virus writers.

**Intent**: As primary motivations of Cyber punks are notoriety and curiosity, they might target critical infrastructures.

**Triggers**: Cyber punks need no trigger to attack.

**Capabilities—skills**: Cyber punks have some technical skills and understanding, and they will be able to use and even improve tools available on the Internet. A Cyber punk might write their own malware exploiting well-known vulnerabilities, but they are not likely to develop their own 0-days or perform very advanced attacks. However, some virus writers also fall under this category, and a novel virus might compromise one or more critical infrastructure systems [60]. It is not likely that systems could be compromised in such a manner as to cause cascading failures without being specifically designed to do so, but if a worm spreads aggressively enough to infect a large number of critical infrastructure systems, then it could cause widespread denial of service.

**Capabilities—resources**: Cyber punks have limited resources since they are mostly solitary, or in small groups. They are likely to able to perpetrate simple, isolated attacks, although nothing sustained or large-scale.

**Threat assessment**: Have the will and the capabilities.

## *6.3 Insiders*

Insiders are malicious but trusted people with privileged access and knowledge of the systems in question.

**Intent**: Insiders are motivated by revenge and to some degree notoriety, and the former part makes them likely to try to conduct sabotage.

**Triggers**: A malicious Insider mostly needs to be triggered to attack, however since the trigger can be any perceived insult or slight at the workplace, it can be very hard to determine whether or not a potential attacker has been triggered—especially considering that the potential attacker is typically a trusted employee.

**Capabilities—skills**: An Insider can have extensive knowledge of the systems, including vulnerabilities, as well as privileged access to controls. An Insider might even have the skills to perpetrate an effective cascading attack.

**Capabilities—resources**: While insiders very often work alone, they usually have the resources needed to make an effective attack, namely privileged access to controls, and physical access to the systems.

**Threat assessment**: Have the will and the capabilities.

## *6.4 Petty Thieves*

Members of the Petty thieves category commit low-level fraud and theft, usually by using existing tools and scripts.

**Intent**: Petty thieves are primarily motivated by financial gain, and as such, critical infrastructures do not constitute an attractive target to members of this category.

**Triggers**: This group needs no other trigger than opportunity and a viable business case to attack.

**Capabilities—skills**: Petty thieves use a standard portfolio of tools and techniques primarily focused around phishing, scamming, and credit card fraud. They are not likely to possess the skill set nor the tools needed to attack critical infrastructures.

**Capabilities—resources**: Members of this group work alone or in small groups, and considering their focus on low-level crime, it is not likely they will have the resources needed to commit a successful attack.

**Threat assessment**: Lack the will and the capabilities.

## *6.5 Grey Hats*

Grey hats are often skilful hackers with limited criminal intent but a lack of respect for limitation on information flow and a large curiosity.

**Intent**: This category of attackers is primarily motivated by curiosity, and they are very unlikely to perpetrate any form of sabotage.

**Triggers**: Rumors of secret information or "impenetrable" defences might increase the risk of attack.

**Capabilities—skills**: Grey hat hackers have very specialized technical skill sets and an extensive exchange of information, and as such it is likely they would be able to execute an attack successfully.

**Capabilities—resources**: While there is a high degree of knowledge exchange in this group, most work alone and as such do not have the manpower to make widespread and persistent attacks. They do have the skills and equipment however, to gain insider access to the systems in question, which could enable them to execute a cascading attack.

**Threat assessment**: Lack the will but have the capabilities.

## *6.6 Professional Criminals*

Professional criminals are organised groups of hackers with a strict business approach to attacks.

**Intent**: Professional criminals are purely financially motivated. There is currently no business model that makes the reward of an infrastructure attack worth the risk, since most governments do no negotiate with terrorists, so they are unlikely to attack.

**Triggers**: Like Petty thieves, the Professional criminals need no specific trigger apart from a viable business case.

**Capabilities—skills**: Members of this group of attackers possess a wide variety of technical skills and knowledge, and they are willing to recruit or hire people with the necessary competencies to complete an operation.

**Capabilities—resources**: This group has many resources in the form of money, equipment, and manpower—enough to perpetrate a successful attack against critical infrastructures.

**Threat assessment**: Lack the will but have the capabilities.

## *6.7 Hacktivists*

Hacktivists are groups of ideologically motivated hackers with varying technical skills, but many and geographically distributed members.

**Intent**: Since Hacktivists are motivated by ideological agendas and notoriety and known for a lack of regard for consequences, they are likely to target critical infrastructures. The US Department of Defense warns that it believes one of the biggest hacktivist groups, Anonymous, have both the will and the capability to perform such an attack [61]. However, Anonymous have publicly declared [62], that they are not interested in attacking the power grid because they realize the adverse effect it would have on the general population, and as such the intent in this regard is not completely clear. There are many groups, though, and not all of them have the same moral scruples as Anonymous claims to have. On the other hand, they do not alone have the necessary resources available.

**Triggers**: Hacktivists are triggered by perceived threats or insults to their ideology.

**Capabilities—skills**: While the levels of technical skills are diverse within the Hacktivist groupings, they usually have members with high technical competencies, although they might not have the highly specialized skills needed for a cascading attack.

**Capabilities—resources**: Hacktivists have a large geographical spread and sometimes vast amounts of manpower. They may also have the attack resources in the form of botnets available to execute a widespread and sustained attack. However, only Anonymous is big enough at this point in time to conduct a sustained attack, and they have declared a lack of interest in doing so. This is subject to change though.

**Threat assessment**: Have the will or the capabilities, but not both.

## *6.8 Nation States*

Nation states or representatives hereof have been known to perpetrate everything from industrial espionage over acts of terrorism to devastating nation-wide attacks in the cyber arena.

**Intent**: In case of a conflict, any disruption of the enemy's infrastructure is desirable, and as such, critical infrastructures represent an extremely attractive target to a hostile Nation state.

**Triggers**: Nation states are almost exclusively triggered by disputes in the physical arena, most often geopolitical in nature.

**Capabilities—skills**: Many nation states have substantial presence in cyberspace and commands many highly skilled experts in the critical infrastructure field.

**Capabilities—resources**: They have vast resources in the form of money, manpower, specialized knowledge and intelligence, and equipment. They are very likely to be able to conduct a successful attack.

**Threat assessment**: Have the will and the capabilities.

## *6.9 Threat Picture*

Three of the hacker categories—Insiders, Hacktivists, and Nation states, see Table 1—can be considered a substantial sabotage threat to critical infrastructures at present time, but this is subject to change. Currently, only these three categories have both the will and the capabilities to execute a successful attack on critical infrastructures.

**Table 1** Threat matrix indicating will and capabilities of attackers

| Categories | Will | Capabilities | Threat |
|---|---|---|---|
| Script kiddies | Yes | No | No |
| Cyper punks | Yes | Yes | Yes |
| Insiders | Yes | Yes | Yes |
| Petty thieves | No | No | No |
| Gray hats | No | Yes | No |
| Professional criminals | No | Yes | No |
| Hacktivists | Yes/No | Yes/No | No |
| Nation states | Yes | Yes | Yes |

## *6.10 Defence Priorities*

Working to defend critical infrastructure in a resource-constrained environment means that limited budget funds must be applied to achieve the best effect. While the thorough "basic" security is assumed in place, there are many areas in which security officers could focus their attention.

**Cyber punks methods**: While most of the attacks performed by this category of attackers are limited in scope and sophistication, the Cyber punks do have one weapon that is a legitimate sabotage threat to critical infrastructures, namely viruses. A worm exploiting an unanticipated attack vector might plausibly infect several of critical infrastructure systems and causing widespread denial of service. Viruses such as Melissa (1999), ILOVEYOU (2000), Nimda (2001), Slammer (2003), and Conficker (2008) (most contributable to Cyber punks) show that it is certainly possible to reach a critical amount of infection in a very short while. To defend against such a worm may prove difficult; see Wiley, Brandon (circa 2002). An Intrusion Detection and Prevention System (IDPS) that uses statistical anomaly-based detection and/or stateful protocol analysis detection would have a good chance of catching such a threat, and there are different ways of hardening the network, depending on how fast the worm propagates [63, 64].

**Insider methods**: Attacks by Insiders will likely take the form of malicious use of controls. Based on the [65], 43 % of Insider attacks were executed while the attacker still had legitimate access to the systems. The majority of Insider attacks were, however, executed while the attacker should no longer have the access. The defence mechanisms that would help defend against such attacks should be based on the principle of least privilege in order to limit the amount of damage that can be done with malicious use of legitimate access. Also, having tight management of personnel access would limit the amount of damage previous employees could cause, since they would lose access as soon as they were no longer employed. More detailed advice on how to mitigate the threat of Insider attacks can be found in [66].

**Nation state methods**: The methods employed by Nation states vary, but there seems to be a prevalence towards spear-phishing and zero-day exploits combined

with worms (e.g., Night Dragon and Stuxnet attacks) as well as devastating DDoS attacks (e.g., Georgia, 66, and 10 Days of Rain). Defence priorities include educating staff and increasing awareness to avoid anyone falling victim to spear-fishing or similar social engineering attacks. It is in the nature of things quite difficult to detect the use of zero-day exploits, but good intrusion detection systems might be able to pick up the change in network behaviour. DDoS prevention should also be a priority, and the volume of the attacks can be expected to be severe, so cooperation with for instance large ISPs might be an option to consider.

### *6.11 Summary*

Based on the threat picture described in this section, defence efforts against digital sabotage of critical infrastructures should focus on dealing with malicious Insiders as well as Cyber punks, and hostile Nation states. This could be done by prioritizing access management, including implementing the principle of least privilege, as well as installing an Intrusion Detection and Prevention System, educating staff to be wary of spear-phishing and similar social engineering attacks, and protecting systems from DDoS attacks. Defence efforts should be particularly focused in times of geopolitical conflict, where the risk of a Nation state attack is high. Furthermore, an eye should be kept on the development in the Hacktivist category, since there is a risk that this group will develop into a threat in the near future. The analysis presented can also be used when designing and deploying new infrastructures such as Smart Grid, Intelligent Transportation Systems, and infrastructures supporting Tele-Health in larger scales. Knowing which groups are the most probable attackers, and knowing their capabilities in terms of skills and resources, can help identify which kinds of attacks are important to prepare for. There is a big difference between being attacked by Insiders, Nation states, or Script kiddies. For researchers in the domain of cyber security this knowledge can be used to indicate where further research and development is needed, e.g., when developing technologies for intrusion detection systems for general or specific critical infrastructures.

## 7 Previous and Ongoing Research Activities

The purpose of this section is not to provide an elaborate list of projects, but give a short overview of some of the activities that have been carried out, are running or will be running in the near future, at European level in the area of communication role in Critical infrastructures and related topics. For more details, the reader should visit the IST website: http://www.ist-world.org/ or http://www.cordis.europa.eu/ist/.

## 7.1 Brief Overview of Selected Projects and Activities

**CRUTIAL** This project, which ran from 2006–2008, has focused on key issues related to trust establishment, access control and fault diagnosis for critical infrastructures. Inspired by Intrusion tolerant system architecture, CRUTIAL is based on two facts; Critical Information Infrastructure features a lot of existing legacy systems, and two existing security solutions may jeopardize operational and functional requirements to critical infrastructure systems. Key components in their architecture are (1) configuration aspects, (2) middleware for automatic fault tolerance inclusive intrusion, (3) trustworthy monitoring mechanism, (4) security and access policy management and enforcement.

**MAFTIA** was a project running between 2000–2003, focusing on fault and intrusion tolerance network support for critical infrastructure systems. The project aimed to develop an architecture based on hybrid failure assumptions, recursive use of fault prevention and fault tolerance techniques, and the notion of trusting components to the extent of their trustworthiness. MAFTIA distinguishes between *attacks*, *vulnerabilities*, and *intrusions* as three types of interrelated faults. Selected system components were implemented and validated through a set of text scenarios with success.

**HIDENETS** The aim of HIDENETS, running from 2006 to 2008, was to develop and analyse end-to-end resilience solutions for distributed applications and mobility-aware services in ubiquitous communication scenarios. The idea has been to make use of off-the-shelf components and wireless communication links to dramatically decrease the costs of market entry and enable ubiquitous scenarios of ad hoc car-to-car communication with infrastructure service support commercially feasible. Dependability has been a keyword in this project, and many of the lessons learned here will be beneficial to critical infrastructure communication systems.

**GRIDCOMP** GridComp main goal was to design and implement a component based framework suitable to support the development of efficient grid applications. Such frameworks are important since the automation and complexity of critical infrastructures makes it necessary to have a structural way of developing software components and middleware on top of networks. The key feature of the developed framework was its level of abstraction perceived by programmers by hierarchically composable components and advanced, interactive/integrated development environments. The framework was supposed to allow a faster and more effective grid application development process by considering advanced component (self-) management features.

**NESSI-GRID** The objective of this project was to contribute to the activities of the Networked European Software and Service Initiative (NESSI) with special focus on next generation Grid technologies; Services not necessarily only for user interaction, but also for critical subsystems. The aspect regarding services in the communication infrastructure and inter operability is not trivial, and it was expected that output of this activity would be aligned with that of Service Oriented Knowledge Utilities (SOKU) as defined by the Next Generation Grid expert group.

**INTEGRIS** A project which has run since 2010 and ended in 2012, addressing a novel and flexible ICT infrastructure based on a hybrid power line communication/wireless integrated communication system for smart electricity grids. The project covers monitoring, operation, customer integration, demand side management, voltage control, quality of service control and control of distributed energy resources. On the communication side, in particular interoperability of the power line communication, wireless sensor networks and radio frequency identification are in focus.

**REALSMART** This project, running from 2010 to 2014, aims to look at smart grid solutions. From a communication point of view, the solutions sought in this project relate to measurement collection procedures for phasor measurements to allow an improved observation of the transmission grid. Among other questions that need to be addressed, is the handling of the massive amounts of real time data that are to be collected.

**EDGE** EDGE is a Danish funded project running from 2012 to 2017, which aims to develop complex control algorithms for smart grid systems based on power flexibility from consumers. The role of the communication in this project is in particular on the interaction between these advanced control algorithms and strategies and the network dynamics that exist in heterogenous networks.

**SmartC2Net** This project is a new smart grid project starting in the last part of 2012 until 2015. This project aims to provide an ICT platform that supports flexible interaction possibilities between control algorithms and strategies, and the physical entities distributed in the power grid. This entails information reliability models, flexible reconfiguration of the network, control strategy based QoS control, network monitoring and security threat analysis.

## *7.2 Summary*

A common denominator of all these projects is the focus of ICT and its role in the various aspects of critical applications that run over the network. As investigated in this part, this is necessary as networks are complex, and far from perfect. In most cases, and in particular for large scaled, general purpose networks (e.g., the Internet) only probabilistic guarantees can be given, which may or may not be sufficient for the critical applications. Projects such as CRUTIAL, MAFTIA and HIDENETS focus to a large extent on the dependability of services in the network infrastructure, which all concerns both reliability and availability in a distributed setting elements. Availability and security is strongly linked. These are key elements when supporting critical infrastructures, and surely lessons learned here will in some way find the way in future networks.

Projects such as GRIDCOMP and NESSI-GRID focus also on service interaction and interoperability as well as on how programmers can integrate software solutions. This is absolutely a key feature for reliable operation of networks, since

as also seen in many of the other projects, middleware and software components in the network will play a key role in future critical networks.

Finally, projects such as INTEGRIS, EDGE and SmartC2Net aim specifically to address the interaction between control algorithms for smart grids and the network. For the network, the running application behaviour is critical, as this sets the requirements to the network that provides the end-to-end communication. Therefore, understanding the interaction between application and network is critical, and is manifested to some degree in the need for such projects.

These examples as well as the other non-European efforts, national projects and initiatives, provides valuable insight in the challenges and solutions of using the existing network for critical applications. At the end this benefits to save costs for redeployment of dedicated networks to each critical application that exists. This makes it necessary to explore and spend funding on research to achieve a reliable communication infrastructure.

## 8 Conclusions and Outlook

Communication networks are complex and pose a challenge to distributed systems, and although these networks offers great advantages of cheap exchange of information for various purposes, it is critical not to under estimate the role communication plays in distributed applications. In particular not for critical infrastructures which require communication due to their distributed nature. The complexity and dynamics of the networks are challenged at all levels. Through this chapter, we looked at basic communication, standards for smart grids, network deployment, reliability of protocols, security and threats, and also gave a brief overview of what type of research is or has been ongoing at a European level to address the issues that need to be tackled for networks to support critical infrastructures.

## References

1. Future Internet 2020: Visions of an Industry Expert Group, DG Information Society and Media Directorate for Converged Networks and Service—"The Internet People", May 2009, European Commission, Information Society and Media. ISBN: 978-92-79-11320-8, doi:10.2759/4425
2. Tannenbaum, A.S.: Computer Networks, 4th edn. Prentice Hall, Upper Saddle River, Internation Edition, ISBN: 0-13-038488-7
3. http://www.netvalley.com/history_of_internet.html
4. Prasad, R., Mihovska, A.: New Horizons in Mobile and Wireless Communications: Reconfigurability, ISBN: 978-1-60783-971-2, New Horizons in Mobile and Wireless Communications series, Artech House (2009)
5. Wang, W., Xu, Y., Khanna, M.: A survey on the communication architectures in smart grid. Comput. Netw. **55**(15), 3604–3629
6. http://www.ipv6vsipv4.com/

7. Murray, et al.: Why is it difficult to implement ehealth initiatives? A qualitative study. Implementation Sci. **6**, 6 (2011)
8. Strobla, R.O., Robillardb, P.D.: Network design for water quality monitoring of surface freshwaters: a review. J. Environ. Manag. **87**(4), 639–648 2008. http://dx.doi.org/10.1016/j.jenvman.2007.03.001
9. Mattern, F., Staake, T., Weiss, M.: ICT for green—how computers can help us to conserve energy. In: Proceedings of the 1st International Conference on Energy-Efficient Computing and Networking (e-Energy 2010), ACM, pp. 1–10. Passau (2010)
10. Lim, H.-T., Volker, L., Herrscher, D.: Challenges in a future IP/ethernet-based in-car network for real-time applications. In: Design Automation Conference (DAC), 2011 48th ACM/EDAC/IEEE, pp. 7–12, 5–9 June 2011
11. Karjalainen, S.: Consumer preferences for feedback on household electricity consumption. Energy Build. **43**(23), 458–467 (2011). ISSN 0378-7788, doi:10.1016/j.enbuild.2010.10.010
12. Ye, Y.; Yi, Q., Sharif, H.: A secure and reliable in-network collaborative communication scheme for advanced metering infrastructure in smart grid. In: Wireless Communications and Networking Conference (WCNC), 2011 IEEE, pp. 909–914, 28–31 March 2011
13. Bliek, F., van den Noort, A., Roossien, B., Kamphuis, R., de Wit, J., van der Velde, J., Eijgelaar, M.: PowerMatching City, a living lab smart grid demonstration. In: Innovative Smart Grid Technologies Conference Europe (ISGT Europe), 2010 IEEE PES, pp. 1–8, 11–13 Oct 2010
14. Benzi, F., Anglani, N., Bassi, E., Frosini, L.: Electricity smart meters interfacing the households. IEEE Trans. Ind. Electron. **58**(10), 4487–4494 (2011)
15. Depuru, S.S.S.R., Wang, L., Devabhaktuni, V., Gudi, N.: Smart meters for power grid—challenges, issues, advantages and status. In: Power Systems Conference and Exposition (PSCE), 2011 IEEE/PES, pp. 1–7, 20–23 Mar 2011
16. Byun, J., Hong, I., Kang, B., Park, S.: A smart energy distribution and management system for renewable energy distribution and context-aware services based on user patterns and load forecasting. IEEE Trans. Consum. Electron. **57**(2), 436–444 (2011)
17. LeMay, M., Nelli, R., Gross, G., Gunter, C.A.: An integrated architecture for demand response communications and control. In: Proceedings of the 41st Annual Hawaii International Conference on System Sciences, pp. 174, 7–10 Jan 2008
18. Wang, W., Xu, Y., Khanna, M.: A survey on the communication architectures in smart grid. J. Comput. Netw. **55**(15), 3604–3629 (2011)
19. Sidhu, T.S., Yin, Y.: Modelling and simulation for performance evaluation of IEC61850-based substation communication systems. IEEE Trans. Power Delivery **22**(3), 1482–1489 (2007)
20. Kanabar, M.G., Sidhu, T.S.: Reliability and availability analysis of IEC 61850 based substation communication architectures. In: Power & Energy Society General Meeting, 2009. PES '09. IEEE, pp. 1–8, 26–30 July 2009
21. Gungor, V.C., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., Hancke, G.P.: Smart grid technologies: communication technologies and standards. IEEE Trans. Ind. Inf. **7**(4), 529–539 (2011)
22. Zaballos, A., Vallejo, A., Selga, J.M.: Heterogeneous communication architecture for the smart grid. IEEE Netw. **25**(5), 30–37 (2011)
23. Zhang, R., Zhao, Z., Chen, X.: An overall reliability and security assessment architecture for electric power communication network in smart grid. In: 2010 International Conference on Power System Technology (POWERCON), pp. 1–6, 24–28 Oct 2010
24. Moslehi, K., Kumar, R.: A reliability perspective of the smart grid. IEEE Trans. Smart Grid **1**(1), 57–64 (2010)
25. McDaniel, P., McLaughlin, S.: Security and privacy challenges in the smart grid. IEEE Secur. Priv. **7**(3), 75–77 (2009)
26. Venkitasubramaniam, P., Tong, L.: Anonymous networking with minimum latency in multihop networks. IEEE Symposium on Security and Privacy, 2008. SP 2008, pp. 18–32, 18–22 May 2008

27. Doshi, B., Harshavardhana, P.: Broadband network infrastructure of the future: roles of network design tools in technology deployment strategies. IEEE Commun. Mag. **36**, 60–71 (1998)
28. To, M., Neusy, P.: Unavailability analysis of long-haul networks. IEEE J. Sel. Areas Commun. **12**, 100–109 (1994)
29. Singel, R.: Fiber optic cable cuts isolate millions from internet, future cuts likely wired. http://www.wired.com/threatlevel/2008/01/fiber-optic-cab/ (2008). Accessed January 2008
30. Hachman, M.: Sabotage suspected in silicon valley cable cut PCMag. http://www.pcmag.com/article2/0,2817,2344762,00.asp (2009) . Accessed 9 April 2009
31. Farley, J.: Bremerton fiber optic cable cut knocks out service for wave broadband customers. http://www.kitsapsun.com/news/2011/jul/06/bremerton-fiber-optic-cable-cut-knocks-out-for/#axzz36lWFNBmE(2011).
32. Zhang-shen, R., Mckeown, N.: Designing a predictable internet backbone with valiant load-balancing. IWQoS **2005**, 178–192 (2005)
33. Raza, K., Turner, M.: CCIE Professional Development Large-Scale IP Network Solutions. Cisco Press, Indianapolis (1999)
34. Iniewski, K., McCrosky, C., Minoli, D.: Network Infrastructure and Architecture: Designing High-Availability Networks. Wiley, New York (2008)
35. Riaz, T.: SQoS based planning for network infrastructures. Ph.D. thesis (2008)
36. Grover, W.D.: Mesh-Based Survivable Networks, Options and Strategies for Optical, MPLS, SONET and ATM Network, vol. 1. Prentice Hall PTR, Upper Saddle River (2003)
37. Ecobilan: FTTH solutions for a sustainable development (2008)
38. Madsen, O.B., Knudsen, T.P., Pedersen, J.M.: SQOS as the base for next generation global infrastructure. In: Proceedings of IT&T 2003, Information Technology and Telecommunications Annual Conference 2003, pp. 127–136 (2003)
39. Caenegem, B.V., Parys, W.V., Turck, F.D., Demeester, P.: Dimensioning of survivable wdm networks. IEEE J. Sel. Areas in Commun. **16**, 1146–1157 (1998)
40. Gutierrez, J.M., Katrinis, K., Georgakilas, K., Tzanakaki, A., Madsen, O.B.: Increasing the cost-constrained availability of WDM networks with degree-3 structured topologies. In: 12th International Conference on Transparent Optical Networks (ICTON), 2010, pp. 1–4 (2010)
41. Rados, I.: Availability analysis and comparison of different wdm systems. J. Telecommun. Inf. Technol. **1**, 114–119 (2007)
42. Zhou, L., Held, M., Sennhauser, U.: Connection availability analysis of shared backup path-protected mesh networks. J. Lightwave Technol. **25**, 1111–1119 (2007)
43. Booker, G., Sprintson, A., Zechman, E., Singh, C., Guikema, S.: Efficient traffic loss evaluation for transport backbone networks. Comput. Netw. **54**, 1683–1691 (2010)
44. He, W., Somani, A.K.: Path-based protection for surviving double-link failures in mesh-restorable optical networks. In: Proceedings of IEEE Globecom 2003 (2003)
45. Gutierrez, J.M., Riaz, T., Pedersen, J.M.: Cost and availability analysis of 2- and 3-connected WDM networks physical interconnection. In: Proceedings in ICNC 2012 (2012)
46. Hansen, M.B., Olsen, R.L., Schwefel, H.-P.: Probabilistic models for access strategies to dynamic information elements. Perform. Eval. **67**(1), 43 (2010)
47. Schwefel, H.-P., Hansen, M.B., Olsen, R.L.: Adaptive Caching strategies for Context Management systems, PIMRC07, Athens, Sept 2007
48. Shawky, A., Olsen, R., Pedersen, J., Schwefel, H.: Network Aware Dynamic Context Subscription Management, Computer Networks, vol. 58, pp. 239–253. 15 January 2014, ISSN 1389-1286. http://dx.doi.org/10.1016/j.comnet.2013.10.006.
49. Hald, S.L.N., Pedersen, J.M.: The Threat of Digital Hacker Sabotage to Critical Infrastructure. Submitted for GIIS 2012 (2012)
50. Hald, S.L.N., Pedersen, J.M.: An updated taxonomy for characterizing hackers according to their threat properties. In: 14th International Conference on Advanced Communication Technology (ICACT) 2012, IEEE (2011). ISBN 978-8955191639

51. Moteff, J.: Risk Management and Critical Infra-structure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences. Congressional Research Service, Washington D.C. (2005)
52. Devost, M.G.: Current and emerging threats to information technology systems and critical infra-structures. Glob. Bus. Brief. (2000)
53. The White House: The National Strategy to Secure Cyberspace, p. 5. The White House, Washington D.C. (2003)
54. Vatis, M.A.: Cyber Attacks During the War on Terrorism: A Predictive Analysis. Institute for Security, Dartmouth College, Hanover (2001)
55. Shea, Dana A.: Critical Infrastructure: Control Systems and the Terrorist Threat. Congressional Research Service, Washington D.C. (2004).http://fas.org/irp/crs/RL31534.pdf
56. Lewis, James A.: Cybersecurity and Critical Infrastructure Protection. Center for Strategic and International Studies, Washington D.C. (2006)
57. Rogers, M.: A two-dimensional circumplex approach to the development of a hacker taxonomy. Digit. Investig. **3**(97–102), 2006 (2006)
58. Rollins, J., Wilson, C.: Terrorist Capabilities for Cyberattack: Overview and Policy Issues. Congressional Research Service, Washington D.C. (2007)
59. Hunt, J.: Stuxnet, Security, and Taking Charge, Industrial Ethernet Book Issue 62/53, IEB Media GbR, Germany (2011). ISSN 1470-5745
60. Eronen, J., Karjalainen, K., et al.: Software vulnerability vs. critical infrastructure—a case study of antivirus software. Int. J. Adv. Secur. **2**(1) (2009). ISSN 1942-2636 (International Academy, Research, and Industry Association)
61. Department of Homeland Security: National Cybersecurity and Communications Integration Center Bulletin: Assessment of Anonymous Threat to Control Systems. Department of Homeland Security, Washington D.C. (2011)
62. Anonymous, youranonnews: Available at https://twitter.com/youranonnews/status/171941104860672000 (2012)
63. Antonatos, S., Akriditis, P., et al.: Defending Against Hitlist Worms Using Network Address Space Randomization, WORM '05, ACM 1-59593-229-1/05/0011, USA (2005)
64. Lai, S.-C., Kuo, W.-C., et al.: Defending against Internet worm-like infestations. In: Proceedings of the 18th International Conference on Advanced Information Networking and Application (AINA'04), ISSN 0-7695-2051-0/04, IEEE (2004)
65. Keeney, M., Cappelli, D., et al.: Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors. United States Secret Service and Carnegie Mellon Software Engineering Institute, Washington D.C. (2005)
66. Capelli, D., Moore, A., et al.: Common Sense Guide to Prevention and Detection of Insider Threats, 3rd edn. Version 3.1, Software Engineering Institute, Carnegie Mellon University (2009)
67. Hernandez, J.A., Phillips, I.W.: Weibull mixture model to characterise end-to-end Internet delay at coarse time-scales. IEE Proc. Commun. **153**(2), 295–304 (2006). doi:10.1049/ip-com:20050335
68. Bolot, J.-C.: Characterizing end-to-end packet delay and loss in the Internet. J. High Speed Netw. IOS Press. ISSN 0926-6801 (Print), 1875-8940 (Online), Comput. Sci. Netw. Secur. **2**(3), 305–323 (1993)
69. Bovy, C.J., Mertodimedjo, H.T., Hooghiemstra, G., Uijterwaal, H., Van Mieghem, P.: Analysis of end-to-end delay measurements in Internet. In: Proceedings of the Passive and Active Measurement Workshop-PAM 2002 (2002)
70. Klima-, Energi- og Bygningsministeriet, HOVEDRAPPORT for Smart Grid Netværkets arbejde, available online at http://www.kebmin.dk/en
71. ECOGRID Bornholm: Official websitehttp://ecogridbornholm.dk/