International Journal of Information & Network Security (IJINS)
Vol.3, No.3, June 2014, pp. 225~237
ISSN: 2089-3299

A Cognitive Network-Based Network Security Architecture for Mission Critical Communications

Anssi Kärkkäinen
Department of Communications and Networking, Aalto University, Espoo, Finland

Article Info

Article history:

Received April 27th, 2014
Revised July 9th, 2014
Accepted June 23rd, 2014

Keyword:

Cyber security
Mission critical communications
Cognitive networks
Security architecture
Network security

ABSTRACT

The mission critical networks provide a highly deployable and reliable communication platform for authorities enhancing their ability in command and control. Emerging cybersecurity threats must be considered when new mission critical networking capabilities are designed and implemented. New threats require novel approaches when implementing network security. Cognitive networks are a promising concept to build smart and dynamic networks. This work provides an analysis how cognitive networking improves security capabilities and how new approaches of building security is required. The article describes a novel cybersecurity architecture with cognitive capabilities. The architectural model is proved by a scenario-based evaluation. A cognitive layer provides several advantages for security controls and management, but some implementation challenges still remain.

Corresponding Author:

Anssi Kärkkäinen,
Department of Communications and Networking, Aalto University,
Otakaari 2, Espoo, Finland
Email: anssi.p.karkkainen@gmail.com

1. INTRODUCTION

Mission critical communication networks are typically deployed to support governmental authorities in a case of emergency situations. These situations vary from natural disasters to military operations. Because of the rough environment the requirements for the networks are high. The networks must be robust, reliable and secure so that the authorities such as police, rescue and military are able to share information in order to establish situational awareness and command and control capabilities. Simultaneously, dependence on information technology and cyber environment is growing strongly. Global cybersecurity threats also concern the mission critical communications as it relies more and more on commercial technologies and standards. Cyber attacks may disrupt the cyber environment causing significant impact on the mission critical communication networks' ability to operate effectively. Although risks in cyberspace can be managed in several ways, they do not often match this complex and dynamic environment of the mission critical communications [1]. Security controls, protocols and management models are challenging to implement, maintain and operate in a system requiring dynamic distributed behaviour. New approaches and models are required to manage emerging threats and to build security features in networking systems.

From a mission critical communication point of view, cognitive networks (CN) [2] seems to be an interesting paradigm for providing manageable security capabilities in a complex networking environment. A cognitive network has an ability to adapt networking parameters according to the changes in the environment, service level requirements or/and security scenarios. In a cognitive network system, all network resources (e.g. spectrum, link capacity) are managed dynamically and effectively. Network administration and configuration would no longer rely on human operators. Adaptation to cyber threats may occur automatically without manual execution and reconfiguration.

The main contributions of this work are an analysis of how cognitive networking enhances security of a mission critical network, and a novel cybersecurity architecture. The analysis considers benefits and drawbacks of cognitive behaviour of network security. This work also introduces a novel cybersecurity architecture for mission critical communications. The architecture is based on cognitive capabilities providing more dynamic and stronger security features required to protect against the new cyber threats. The architecture is verified by using a scenario-based evaluation.

The structure of this paper is as follows. Section 2 reviews the communication requirements and cyber threats from the mission critical networking point of view. The section also present the main security challenges with legacy networking systems. Section 3 explains the idea behind cognitive networks and presents the basic characteristics. The analysis of cognitive capabilities is provided in Section 4. Section 5 introduces a novel cyber security architecture with cognitive capabilities, and in Section 6 the architecture model is evaluated. Finally, conclusions are drawn in Section 7.

2. CYBER SECURITY CHALLENGES ON MISSION CRITICAL NETWORKING

Implementing networking capabilities in a mission critical communications environment differs significantly from the traditional network deployment. The specific requirements create new cybersecurity threats that are not considered in legacy networking systems. In this section, we discuss on cyber threats on mission critical networking, and present the main security challenges with the current communication networks.

According to the desired effect, cyber attacks can be categorized into three basic forms from which all others derive [3]. *Confidentiality attacks* include any unauthorized acquisition of information. Global network connectivity enables attackers to access data worldwide. *Integrity attacks* include the unauthorized modification of information. Attacks can contain the disruption of data for criminal, political, or military purposes. Confidentiality and integrity attacks are typically penetration attacks that involve breaking into a system using known or unknown security vulnerabilities. The goal of *availability attacks* is to prevent authorized users from accessing into the systems or data that are required to conduct operations. Attacks are commonly described as Denial-of-Service (DoS) attacks, and they cover a wide range of malware, network traffic, or physical attacks on computers, databases and the networks connecting them. The purpose is to affect the system through diminishing the system's ability to function.

Table 1. Main security challenges in legacy mission critical communications networks.

Challenge	Description
Manual and Static Configuration	○ Configuration files are once loaded into a system, and no modifications are made until the service requirements are changed. Thus, network is static in nature, which makes it easier to be discovered and attacked. ○ Reconfiguration is provided manually by a network operator which may appear to be slow or complex as the threat environment changes rapidly and continuously.
Lack of Light-Weight Security Protocols	○ Security services consume system resources such as bandwidth, memory, processing power and also battery power in mobile devices (e.g. radios and end user terminals). Implementation of security services in mission critical networks should be resource-efficient [4]. Typically, security protocols are not designed for the mission critical networking, and thus they may cause some performance reduction [5]. ○ A good example of a security protocol providing a significant overhead is the Internet Protocol Security (IPsec) standard. The IPsec decreases a maximum throughput especially at smaller frame sizes. For example, with 64-byte packet frames the performance was approximately 27% of the maximum theoretical throughput. [6]
Centralized Security Services	○ Legacy mission critical communications networks include centralized security services such as authentication and authorization. For example, a network may be governed by a trusted third party - a central entity providing security certificates which is trusted network wide [7]. The centralized security service structure weakens reliability of the mission critical network (a single point of failure). ○ For example, in a case of advanced Distributed Denial-of-Service attack, the reconfiguration of system parameters and restoring the centralized services may take a moment [8].
Lack of Overall Security Management	○ Security management of the mission critical networks is a both technical and administrative security process including a set of security policies and controls. Security management including all relevant functions from security policies to a single security component through the entire network remains very complex [9]. ○ Applications have separated access-granting and restricting policies and methods. The criteria, on which access decisions are based, may vary vastly among different services or systems or even between different instances inside the same application [9].
Traffic Flow Confidentiality	○ The existing networks lack of traffic flow confidentiality that is even more critical in the networks where communication links are wireless, and thus easier to eavesdrop. ○ Traffic flow refers to the information that can be observed by looking at the traffic flow rather than the information content within the payload of the transferred packets. Traffic flow can expose that there is data communications, the volume of communications, and the traffic sources and destinations [8].

In mission critical networking, the access to critical data of the network system can be achieved roughly by using two different approaches. The first is a physical network node capture which means that a network node is captured by an attacker to discover critical data. Also, a captured node may be used for accessing a communications network. The second approach includes communication links and especially wireless ones. An attacker may access to network nodes by wiretapping wireless links. Cyber attacks are attractive because they can be launched from remote locations, offering the hostile attackers a degree of anonymity and safety. Advanced attackers can hide their tracks and make it challenging to identify not only who the attacker is, but also from where the attack was launched.

Legacy mission critical communications systems (e.g. some military C2 systems) were designed even decades ago. Thus, network security was not implemented to protect networks against today's latest cyber threats. There are several security gaps in the current systems, and we present five of these most challenging security gaps in Table 1.

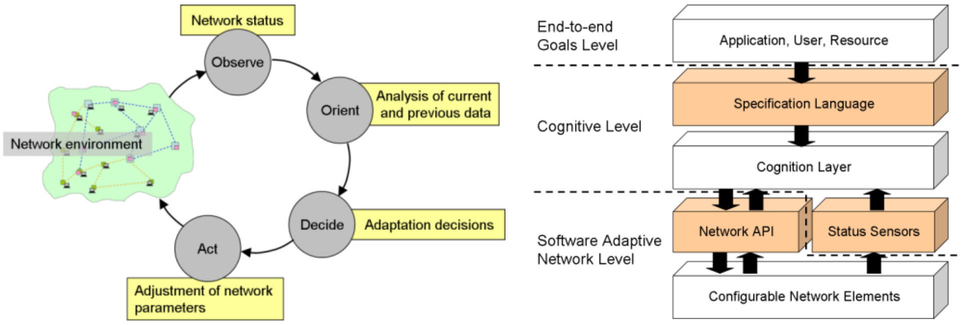
3. COGNITIVE NETWORKS

In recent years, terms cognitive and smart have been strongly linked to communication networks, but the terms are often defined inaccurately from a communication networks perspective. However, it is generally understood the above terms describe the network's ability to adapt according to environmental changes [2]. A definition described by Thomas, DaSilva and MacKenzie [2] refers cognition as consciousness and its content as a whole. Consciousness is associated with the ability to observe and analyze the environment, think, reason and solve problems. Thomas et al. [10] describe cognitive networks as:

"A cognitive network is a network with a cognitive process that can perceive current network conditions, and then plan, decide, and act on those conditions. The network can learn from these adaptations and use them to make future decisions, all while taking into account end-to-end goals."

A cognitive network tries to exactly perceive the current network situation and plan and decide how to meet the end-to-end goals in an entire network aspect. The network learns through adaptation and uses information of the previous actions for future decisions. A key element of the cognitive approach is an end-to-end goal. Without the end-to-end goal, which could be set by a user or service, the system may only perform as a cognitive device or network layer, but not as an entire cognitive network. Cognitive network means that all the layers and elements of a communications system behave in a cognitive manner.

A cognitive process could be understood as the commonly known OODA loop [11] with the observation, orientation, decision and acting phases. Figure 1 (a) illustrates the phases of cognitive networking. The observation phase is critical because data collected in the observation phase significantly affects the decision made by the network. If a cognitive network has knowledge of the entire network's state, cognitive decisions should be more "correct" than those made in ignorance. In the orientation phase, all observed status information and previous knowledge (history data) are combined and analyzed. Filters and weighting are examples of methods used in the orientation phase. In the decision phase, the best decision for the required end-to-end goal is made. Learning is an important part of the orientation phase because it can prevent the recurrence of past mistakes in future decisions. Finally, a network adjustment is provided in the acting phase. The adjustment includes parameter modifications and reconfiguration of cognitive network elements.



(a) (b)

Figure 1. The cognitive process (a) and framework (b) in a communication network.

Cognitive networks have three basic characteristics; situational awareness (SA), learning and decision-making abilities, and fully controlled network parameters and settings [12]. Situational awareness is provided through the network's ability to observe the operational environment and the internal state of the network, and thus to form "understanding" of external and internal conditions. For network optimization, it is important that the network nodes share their status information with other nodes. Learning and decision-making consists of the network's capability to use historical data and past decisions. New decisions are based on previous decision-making processes and current situational awareness. The fully controlled network means that all the network performance parameters are adjustable by software.

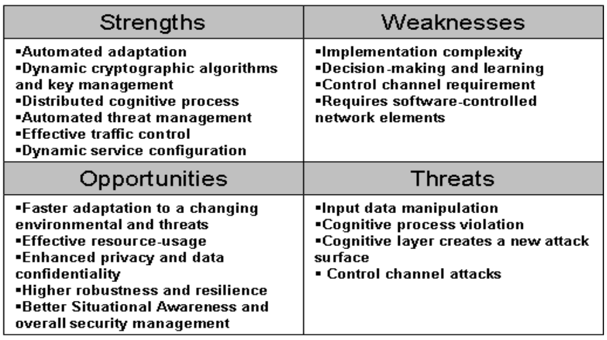
Figure 1 (b) illustrates a cognitive system framework [13] which consists of three functional levels. The end-to-end level includes applications, users and resources which form the end-to-end goals to be achieved at an appropriate service level. The cognitive level includes a specification language layer, a cognition layer, and network status sensors. The language layer communicates the goals to the cognitive layer. The status sensors provide SA information to the cognitive process. The software adaptive network layer consists of the network application programming interface (API) and configurable network elements.

4. ANALYSIS OF COGNITIVE NETWORK-BASED NETWORK SECURITY

In this section, we provide a SWOT analysis (strengths, weaknesses, opportunities and threats) [14] to perceive how cognitive capabilities bring benefits and drawbacks for security of the mission critical communications, and what opportunities and threats the cognitive system will face. In theory, the cognitive process provides many benefits when compared to legacy security management and configuration models and processes, but it may also create new challenges when the cognitive security features are implemented in practice. Figure 2 illustrates the results of the analysis.

4.1. Strengths and Opportunities

The cognitive process allows a holistic and dynamic approach when managing security parameters and building situational awareness and cyber protection for mission critical networking. Through automated adaptation all the security parameters and controls are adjusted according to the cognitive decision-making process. Adaptation cycle runs rapidly and the optimization of security parameters is provided through the entire network and all the layers. In a networking system, data privacy must be ensured at all layers and entities. There are many methods [15], such as packet level authentication or data encryption to build privacy and confidentiality, but guaranteeing the privacy requirements through all layers and network elements demands a common process such as a cognitive process. The cognitive layer also provides secure data processing in and between different security domains (e.g. confidential, secret, and restricted) as new efficient security controls such as flow control (domain access, information sharing between different domains), risk level feedback and trust-based routing are implemented within a cognitive system [16].



Strengths	Weaknesses
▪Automated adaptation ▪Dynamic cryptographic algorithms and key management ▪Distributed cognitive process ▪Automated threat management ▪Effective traffic control ▪Dynamic service configuration	▪Implementation complexity ▪Decision-making and learning ▪Control channel requirement ▪Requires software-controlled network elements
Opportunities	**Threats**
▪Faster adaptation to a changing environmental and threats ▪Effective resource-usage ▪Enhanced privacy and data confidentiality ▪Higher robustness and resilience ▪Better Situational Awareness and overall security management	▪Input data manipulation ▪Cognitive process violation ▪Cognitive layer creates a new attack surface ▪ Control channel attacks

Figure 2. SWOT analysis of cognitive network-based network security

A cognitive system also provides robustness and resilience. In mission critical networking, the environmental conditions vary a lot. Network nodes may lose their connectivity. The cognitive process brings advantages when delay-tolerant [17] and distributed operational capabilities are required. Situational awareness is a key functionality to make correct decisions, for example, during a cyber attack. With incomplete decisions the situation may lead to the conditions where the network is not operational anymore. SA could be established using several methods, for example self-organizing maps [18].

Instead of having a static network configuration, dynamic service configuration makes a mission critical network as a moving target for a potential adversary [19]. The cognitive network may change its information service configuration randomly or with a certain rule so that the attacker’s intelligence information expires before the attack will influence. The cognitive process also enables an automated cyber threat management. Reference [20] introduces a layered framework of cyber threat management for cognitive networking. The framework provides functionalities to identify threats, and to run a risk assessment process automatically. Through the previous strengths, the opportunities of the cognitive security management include faster adaptation to a changing environmental and threats, effective resource-usage, enhanced privacy and data confidentiality, higher robustness and resilience, and better situational awareness and overall security management.

4.2. Weaknesses and Threats

The complexity of a large cognitive system increases enormously. Every single security element is software-controlled which causes a lot of new software code to be run. Managing software defined security elements requires another software-based management layer at each network node. A complex, software defined system requires a lot of computational capacity. That consumes electric power and requires powerful microprocessors. The nodes are connected to each other through links that include separated control channels to build a solid, network-scale management plane. Even tough the CN provides automated and dynamic management for network operators, and thus simplifies an operator's configuration environment; the practical implementation may appear far too complex and reliable.

Ensuring security of information sharing between cognitive nodes is vital for network optimization. For optimal functioning the nodes of cognitive network must exchange a huge amount of control information. The corruption of control data causes a reduced capability to optimize network behaviour within all the other nodes in the network. A single node may still be able to make optimal decisions, but cognitive behaviour is limited to the single node. In that case, cognitive networking no more exists.

It is obvious that a new architectural design with a cognitive process and software controlled security controls may create emerging and unknown cybersecurity threats. Security challenges of the cognitive process are researched and discussed in several sources [21], [22], [23]. Cognitive networks face some unique security threats not appearing in conventional wireless or wired networks. The cognitive process itself may appear vulnerable. For instance, incomplete situation awareness or a disturbed decision-making process may lead to the decision not to use any security controls. An attacker is able to change the information environment by violating sensor data, information sharing and history data (databases). By manipulating the receiving information the attacker can feed faulty statistics data to be stored in the knowledge database of a network node. Further decisions based on the current situation and information in the knowledge database may not be optimal as the stored information is not valid.

Network level optimizing of security parameters is based on reliable information sharing between network nodes. In a mission critical environment, communication channels may be bandwidth limited and unreliable which means that the requirements for the control channel between the nodes are high. It may turn challenging when designing and implementing narrow bandwidth and reliable control that is secured and isolated from a payload channel.

4.3. Conclusions

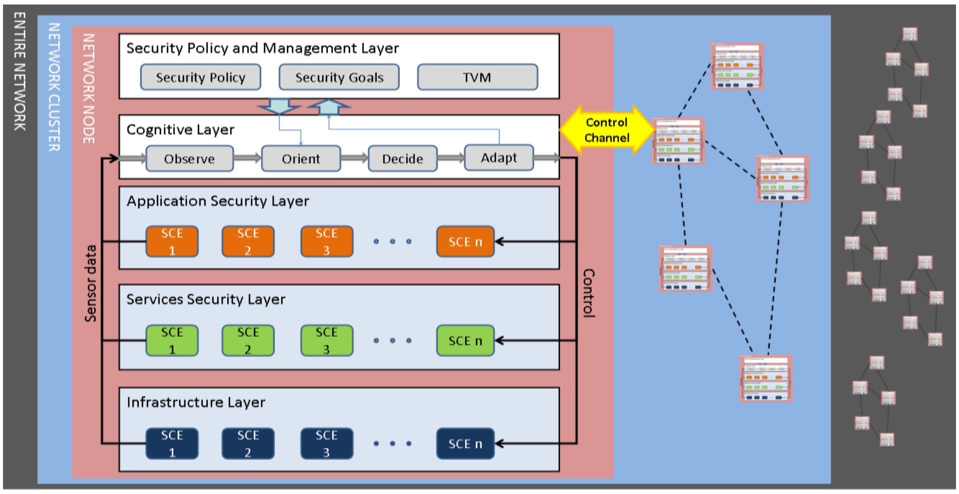
Cognitive network-based security capabilities are potential for improving network security and its management. The cognitive layer enables dynamic, automated and self-learning features to maintain desired security level through the entire network system. However, implementing is challenging. The cognitive layer increases complexity and creates new threats. Cognitive network-based security requires new design from an architectural view down to protocol descriptions. In the following sections, we propose a novel, cognitive network-based architecture model of cybersecurity capabilities for mission critical networks, and evaluate it.

5. NETWORK SECURITY ARCHITECTURE WITH COGNITIVE NETWORKING FEATURES

Existing security or enterprise architectures do not include or take into account the cognitive features when addressing security controls design in a communications network [24]. Also, different architecture frameworks have been developed for enterprise and business security [24], but none of them scope on overall communications security with cognitive approach. For the reasons above, the following security architecture is not based on any existing security architecture frameworks, but it rather complies with the layer structure of the ITU-T X.805 recommendation [25].

5.1. Architecture Overview

Figure 3 presents the overview of the network security architecture for the cognitive military networks. The architectural design is based on a block diagram that describes functional element at five functional layers. The functional layers of the architecture are the Security Policy and Management Layer, Cognitive Layer, Application Security Layer, Service Security Layer, and Infrastructure Security Layer. The layers are implemented in each network node throughout the entire network. At the top of the architecture, security policies and goals are set and executed at the Security Policy and Management Layer controls the Cognitive Layer. In addition to the Security Policy and Security Goals element, the Security Management Layer also includes the Threat and Vulnerability Management (TVM) element that provides cybersecurity threat and vulnerability information to the Cognitive Layer. A main task of the Cognitive Layer is to provide a cognitive process for decision making and to execute the security adaptations in a network node. The process is based on the previously introduced OODA presented in Figure 1 (a). The layer is connected to the Application Security Layer, Service Security Layer, and Infrastructure Security Layer in two ways. Firstly, the Cognitive Layer controls and adjusts Security Control Elements (SCE) of these three layers according to the adjustment orders (based on the decisions), and secondly, the Cognitive layer monitors all the Security Control Elements and receives status data from them.



SCE = Security Control Element   TVM = Threat and Vulnerability Management

Figure 3. Overview of the cyber security architecture.

The security controls are implemented at three separated layers in accordance with the ITU-T X.805 recommendation [25]. The Infrastructure Security Layer includes the security controls of network transmission facilities, and individual networking elements. The infrastructure layer represents the most vital base when building blocks of networks, services and applications [25]. The Services Security Layer addresses security of services that a network provides to the end-users. These services range from basic transport and connectivity to service enablers like those that are essential for providing service and network access (e.g. authentication/authorization services, dynamic host configuration services, domain name services, etc.). The Applications Security Layer focuses on security of the network-based applications accessed by end-users. The end-user applications are enabled by network services and infrastructure, and they consist of basic Command and Control (C2) applications, file transport/storage applications, voice messaging and email, video collaboration, etc.

The security control elements provide appropriate security controls at each of these three layers. The controls can be classified into three categories according to the timescale of an incident. Before the incident occurs, preventive controls are intended to prevent an incident from occurring by e.g. blocking unauthorized user access. Detective controls are designed to act during the event, and they are planned to identify and characterize an incident in progress, and to alert other security controls (in automated systems) or network security personnel (manual incident handling). After the event, corrective controls are used to limit any damages caused by the incident e.g. by separating damaged network segments, filtering traffic, or recovering damaged services.

5.2. Infrastructure Security Layer

The Infrastructure Security Layer architecture describes the security controls to prevent cyber attacks causing damages to data transition, communication links, and their supporting control capabilities such as routing, and network access. Network elements at the layer include individual routers, switches, servers, and the communication links (wireless and fixed) between them.

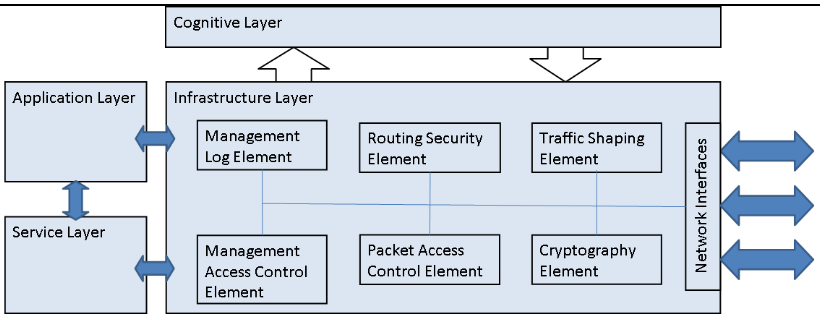


Figure 4. Infrastructure Security Layer.

In a context of the mission critical communications, the Infrastructure Security Layer mainly consists of the deployable network nodes that provide both networking and information service capabilities to the end-users. The layer protects user data packets as they are transported through the network nodes, as well as, they are being transported across wireless and fixed communication links. Securing the infrastructure layer also includes the protection of the control or signalling information (e.g. routing information) that resides in the network nodes as well as securing the receiving and transmission of control or signalling information by a network node. Figure 4 presents the architecture of the Infrastructure Security Layer that consists of six separated security elements. The infrastructure layer is connected to the other layers as depicted in the overall architecture (Figure 3). The features of each element are described in Table 2.

Table 2. The security elements of the Infrastructure Security Layer.

Control	Task(s)	Purpose
Cryptography Element (CE)	○ Encryption/decryption of the control and address data ○ Controlled by the cognitive layer (defines cryptographic algorithms and valid keys)	○ Provision of cryptographic services ○ Protection of data packets against discovering control information.
Routing Security Element (RSE)	○ Filtering of adverse or fake routing information ○ Authentication and authorization of routing information packets and their sources.	○ Ensuring routing is secured and operational
Packet Access Control Element (PACE)	○ Provision of authentication and authorization services for data packets, and blocking invalid packets to enter into a network node	○ Prevention of malicious packets arriving at a node
Traffic Shaping Element (TSE)	○ Padding of data so that the links are always fully utilized regardless of the end-user traffic volumes ○ Generation of bulk traffic to communication links so that the traffic rate of a link is constant.	○ Modification of data traffic on each link so that traffic flow do not disclose communication behaviour
Management Access Control Element (MACE)	○ Authentication and authorization of incoming management data	○ Prevention of unauthorized configuration of a network node
Management Log Element (MLE)	○ Saving of management sessions into a log file	○ Provision of the management audit trail for a network

5.3. Services Security Layer

Building security controls at the Service Security Layer may be complicated because network services are often built-upon one another. For instance, in order to provide a secure email service, a cognitive military network has to provide a simple IP service that relies on enabling services such as DHCP, DNS, and authentication [25]. The network should also provide cryptography and QoS services to meet end-user's quality and security requirements for the secure email service.

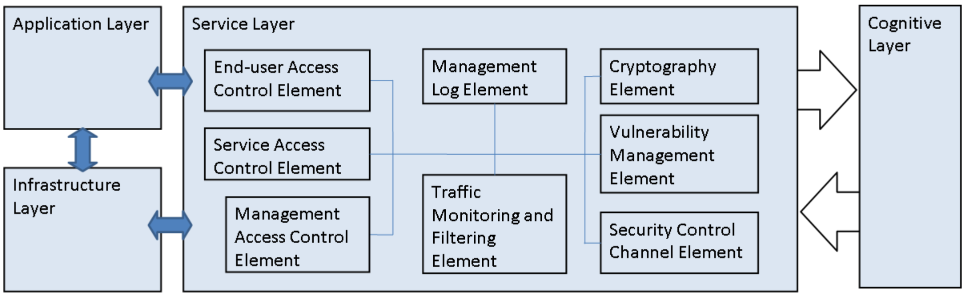

Application Layer
Service Layer
End-user Access Control Element
Management Log Element
Cryptography Element
Cognitive Layer
Service Access Control Element
Vulnerability Management Element
Infrastructure Layer
Management Access Control Element
Traffic Monitoring and Filtering Element
Security Control Channel Element

Figure 5. Services Security Layer.

Table 3. The security elements of the Services Security Layer.

Control	Task(s)	Purpose
Service Access Control Element (SACE)	○ Provision of authentication and authorization to service access messages	○ Prevention of unauthorized access to network services
Traffic Monitoring and Filtering Element (TMFE)	○ Monitoring of incoming and outgoing data traffic to prevent, detect and remove malware in all descriptions ○ Controlling of the incoming and outgoing network traffic by analyzing the data packets and determining whether it should be allowed through or not	○ Prevention of anomalous or hostile traffic flows accessing to a network node or service
Vulnerability Management Element (VME)	○ Collection and sharing of information about system vulnerabilities, and execution of patching ○ Provision of a black box testing called fuzzing [26] in which services or components are provided with invalid, unexpected, or random input data	○ Provision of up-to-date information about vulnerabilities throughout the network nodes as soon as possible

The Services Security Layer includes the security controls that protect data used by network services. Figure 5 presents the architecture of the Service Security Layer including six separated security elements. The layer has input and output connections to the cognitive layer allowing the cognitive layer to control the security elements, and to collect status data from the elements. The Cryptography Element, Management Log Element, and Management Access Control Element provide the same functionalities as those at the infrastructure layer (Figure 3). The features of the rest of the element are described in Table 3.

5.4. Application Security Layer

Securing the applications layer includes securing data generated by end-user applications. The applications may be locally installed or they may be network-based (server-client solutions). In the mission critical environment, the applications have high requirements for processing, sharing and storing classified information to ensure operational security. Securing the applications layer also includes the protection of the control or signalling information used by the network-based applications.

Figure 6 depicts the architecture of the Service Security Layer with five separated security elements. The Cryptography Element, Management Log Element and Management Access Control Element provide the same functionalities as those at the infrastructure layer (see Figure 4). The features of the rest of the element (Node Access Control Element and Application Access Control Element) are described in Table 4.

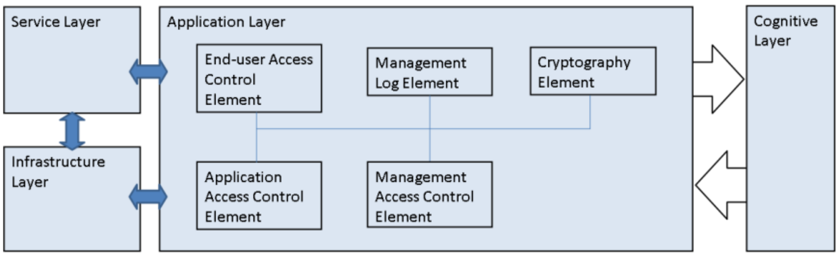


Figure 6. Application Security Layer.

Table 4. The security elements of the Application Security Layer.

Control	Task(s)	Purpose
Node Access Control Element (NACE)	○ Provision of authentication and authorization services for end-users accessing to a network node ○ Receives authentication and authorization information (keys, certificates, access lists, etc.) with the cognitive layer and sends data of user status and rejected access requests to the cognitive layer	○ Protection of illegitimate users to access and connect to a network node
Application Access Control Element (AACE)	○ Provision of authentication and authorization services for end-users accessing the applications of a local or remote node ○ Shares information with the cognitive layer as the NACE	○ Protection of illegitimate users to access the applications in a node ○ Rejection of hostile or unknown end-users

5.5. Cognitive Layer

The cognitive layer functions as “brains” for the network, and it implements the cognitive process. The layer receives status information from all the security elements at the infrastructure, service and application security layers. At the same time, the cognitive layer controls the security elements according to the decisions made during the cognitive process. The cognitive layer obtains the end-to-end security goals from the Security Policy and Management Layer.

The cognitive layer is distributed over the entire network through the control channel. The control channel is critical when network parameters are optimized over the network. Several algorithms can be applied for optimizing and decision-making [12]. In a sense of parameter optimizing, the network is divided into three areas. The first area includes a single node in which optimizing is conducted. This requires no control channel as the optimization is based on information collected from the node. The second optimizing area consists of a cluster of nodes. The network is divided in sub networks to which the specific end-to-end targets are set. Optimizing is provided among the nodes inside the cluster. The third optimizing area involves all the nodes of the network, and optimizing is performed within the whole network.

The network performance depends on the amount of available network state information at the cognitive layer. In order to make beneficial and optimal decisions, the cognitive layer must receive and have the newest status information from all software controlled network security elements. Obviously, decisions made by the cognitive layer are better than those made in ignorance. However, in complex systems such as the mission critical networks, it is unlikely that the cognitive layer would know the complete system state [13]. Weak links, connectivity problems, and scarcity of bandwidth may disturb the control channel so that the cognitive layer has to work with less than a full picture of the network and security status.

5.6. Security Policy and Management Layer

A security policy is a basis for all information security planning, design, and deployment. The policy sets limitations how networks are operated and how information is processed in the networks. The policy is a plan or course of action that conveys instructions from an organization's security management to those who make decisions, take actions, and perform other duties [8]. It is important to ensure that the security policy is enforced by mechanisms that are strong enough. In a cognitive network, the policy enforcement is provided by an automated process without any manual enforcement creating fewer possibilities that the policy is not followed. The security policy typically includes access control, configuration rules and processing of classified information.

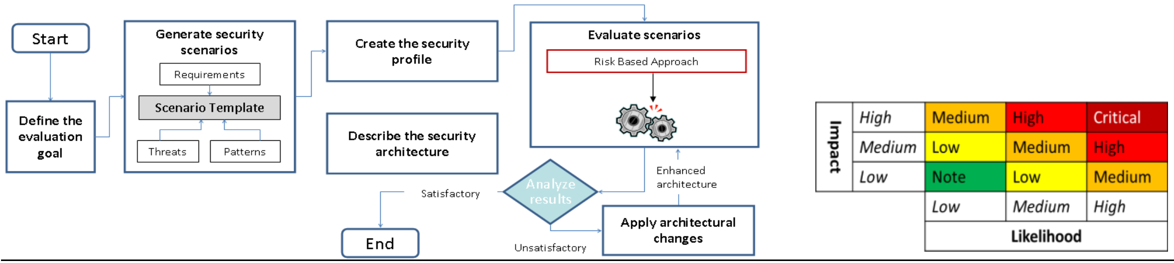
The main task of the security goals management is to describe the end-to-end security goals for the network performance. The security goals include for example approved encryption algorithms, key lengths, access protocols and controls, overall security controls in each node, etc. The Threat and Vulnerability Management (TVM) has an important role in today's cyber environment. By using TVM, the network is able to adjust its parameters to defend against current threats. The element also provides threat and vulnerability information for the risk assessment implemented at the cognitive layer.

6. EVALUATION OF THE ARCHITECTURE MODEL

Evaluation is a key element to prove compliance of the proposed cybersecurity architecture. However, measuring a security architecture is a general problem. As there is always a possibility of vulnerable, it is very difficult to develop security evaluation methods which provide reliable feedback about a system, and an architecture model behind it [27]. Also, the well-known evaluation criteria such as ITSEC [28] and CC [29] are basically designed for security products, not for architecture models. Thus, the proposed architecture is evaluated using a scenario-based evaluation model [30].

6.1. Scenario-Based Evaluation

Although the scenario-based evaluation framework is not originally developed for network security architecture, it is a promising approach to evaluate a high-level network security architecture [30]. The evaluation process leans on a scenario-based architecture review. A key goal of conducting an architecture review is to evaluate an architect's ability to deliver a system that fulfils the security quality requirements and to identify potential security risks. Using scenarios is maturing process and has proven to be a successful practice [31]. The framework includes six phases that are illustrated in Figure 7 (a).



Impact	High	Medium	High	Critical
	Medium	Low	Medium	High
	Low	Note	Low	Medium
		Low	Medium	High
		Likelihood		

(a) (b)

Figure 7. The scenario-based security evaluation framework (a) and risk severity levels (b).

The first phase is to determine an evaluation goal. This includes the declaration of the expected outcomes of this evaluation. Typically, the assessment process may have three types of goals; quantitative, qualitative or trade-off. The second phase of the process is to create the security scenarios. A coherent and logical security scenario is a key for the relevant evaluation results. To generate a reasonable scenario, threat modelling and security requirements must be considered closely. Threats can be well defined and classified using several threat models [32]. In the third phase, all identified scenarios are combined into the security profile. The fourth phase is evaluation in which the selected security profile is analyzed using a risk-based approach. The process of associating risk values with each scenario in the profile is described using the standard risk model [33]. The risk R_i of each scenario i is calculated by:

$$R_i = L_i * I_i \, , \qquad (1)$$

where L_i is the likelihood and I_i is the impact of the scenario i. The OWASP Risk Rating Methodology [33] uses the simple numerical values (0 - 9) for likelihood and impact to simplify the analysis process. The overall risk severity level is achieved as a combination of the levels of impact and likelihood as shown in Figure 7(b). Focusing on severity levels to complete the risk evaluation may take a purer meaning and draw greater attention than numerical values. Thus, it is recommended using the severity levels in the scenario-based evaluation [9]. The likelihood of the scenario i is calculated by:

$$L_i = VF_i * LR_i \, , \qquad (2)$$

where VF_i is the average of the vulnerability factors for each scenario. LR_i is the lack of security element resistance that is achieved by:

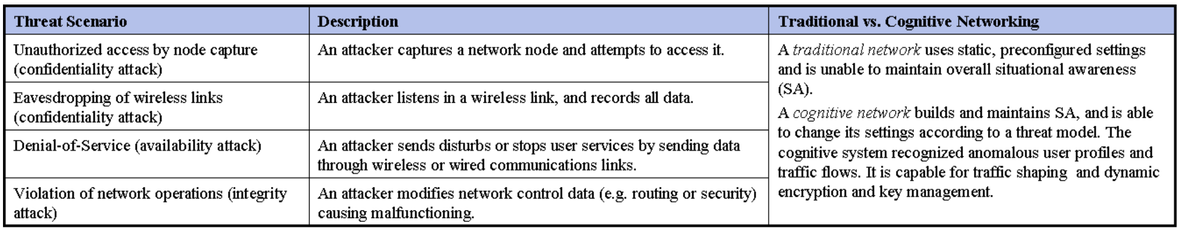
$$LR_i = 1 - Min(\alpha_j) \, . \qquad (3)$$

Each security element has the improvement effect α_j (from 0 to 1) that increases security resistance. If multiple elements are applied to a single scenario, the smallest improvement effect α_j is chosen. The overall impact I_i is achieved as the average of the impacts I on corresponding security objectives for each threat scenario.

6.2. Evaluation Results

To evaluate the proposed architecture, four most-likely threat scenarios for the mission critical communications are described in Table 5. The table also defines how cognitive networking has advantages over traditional networking. The vulnerability and impact factors are based on the OWASP Risk Rating Methodology [33], and they are presented in Tables 6 and 7.

Table 5. Threat scenarios.



Threat Scenario	Description	Traditional vs. Cognitive Networking
Unauthorized access by node capture (confidentiality attack)	An attacker captures a network node and attempts to access it.	A *traditional network* uses static, preconfigured settings and is unable to maintain overall situational awareness (SA). A *cognitive network* builds and maintains SA, and is able to change its settings according to a threat model. The cognitive system recognized anomalous user profiles and traffic flows. It is capable for traffic shaping and dynamic encryption and key management.
Eavesdropping of wireless links (confidentiality attack)	An attacker listens in a wireless link, and records all data.	
Denial-of-Service (availability attack)	An attacker sends disturbs or stops user services by sending data through wireless or wired communications links.	
Violation of network operations (integrity attack)	An attacker modifies network control data (e.g. routing or security) causing malfunctioning.	

Table 6. Technical Impact Factors.

Impact Factor	Definition	Rating
Loss of Confidentiality (LC)	How much data could be disclosed and how sensitive it is.	2 = Minimal non-sensitive data disclosed, 6 = Minimal critical data disclosed, 6 = Extensive non-sensitive data disclosed, 9 = Extensive critical data disclosed, all data disclosed
Loss of Integrity (LI)	How much data could be corrupted and how damaged it is.	1 = Minimal slightly corrupt data, 3 = Minimal seriously corrupt data, 5 = Extensive slightly corrupt data, 7 = Extensive seriously corrupt data,

		9 = All data totally corrupt
Loss of Availability (LA)	How much service could be lost and how vital it is.	1 = Minimal secondary services interrupted, 5 = Minimal primary services interrupted, 5 = Extensive secondary services interrupted, 7 = Extensive primary services interrupted. 9 = All services completely lost
Loss of Accountability (LAC)	Actions by the attackers can be traced to an individual.	1 = Fully traceable, 7 = Possibly traceable, 9 = Completely anonymous

Table 7. Vulnerability Factors.

Impact Factor	Definition	Rating
Ease of discovery (ED)	How easy it is for attackers to discover the vulnerability.	1 = Practically impossible, 3 = Difficult, 7 = Easy, 9 = Automated tools available
Ease of exploit (EE)	How easy it is for attackers to actually exploit the vulnerability.	1= Theoretical, 3 = Difficult, 5 = Easy, 9 = Automated tools available
Awareness (AW)	How well known this vulnerability is to the attackers.	1 = Unknown, 4 = Hidden, 6 = Obvious, 9 = Public knowledge
Intrusion detection (ID)	How likely an exploit is to be detected.	1 = Active detection in application, 3 = Logged and reviewed, 8 = Logged without review, 9 = Not logged

The evaluation results are presented in Table 8. The security controls applied to each scenario are chosen from the architecture layer (Tables 2 - 4). The improvement effect α_j is estimated for each security element. For the first threat scenario, the mitigating security elements are NACE, AACE and SACE that has the improvement value of 0.75 as they partly protect against unauthorized access. As the attacker has the physical access, software-based access controls do not prevent from entering to a hard disk or other databases. The LC and LAC are high (9) in a node capture, while the LI and LA are low (1) as services are distributed and the captured node automatically released from the networking system. ED and EE are difficult (3) but still possible as the attack is well aware of capturing opportunities (AW=9). In the cognitive system, an indication of capture is provided actively (ID=1).

In Scenario 2, the protecting elements are CE and TSE. If the encryption algorithms used in communications are strong enough as expected, the improvement effect is 1.0. Similarly, it is expected that TSE provides 100% traffic flow confidentiality. The impact factors are equal to Scenario 1 as critical data is lost by eavesdropping. ED is difficult (3) but once a link is discovered recording traffic is quite trivial (EE=9). Eavesdropping is well known (AW=9) and it is almost impossible to detect (ID=9).

The security elements concerning Scenario 3 are RSE, PACE, TMFE and VME. The improvement effect of RSE is estimated to 0.75 as routing management may prevent lots of DoS attacks. PACE may drop lots of DoS packets but when the attacker hides DoS commands in a payload, PACE is unable to discover it. In theory, TMFE should detect all DoS attempts (α=1.0) as it is able to form complete situational awareness. VME shares information about potential DoS attack vectors which helps protecting against DoS attacks (α=0.5). The impact factors LC and LI are low while LA is very high (LA=9). Tracing the attacker is challenging but possible (LAC=7). ED and EE are difficult (3) as the mission critical network is hard to access and includes specific protocols. Vulnerabilities for DoS attacks are obviously known (AW=6), but not public in mission critical communications systems.

In Scenario 4, threat protection is achieved by RSE and MACE. RSE concerns routing violations, but most of the violation is conducted at the cognitive layer (α=0.25). MACE prevents most of the hostile accesses to the network management including the cognitive process (α=0.75). The impact factor LC is low (2) as data theft is not a goal. On the other hand, LI, LA and LAC are quite high (7) due to the effects on networking capabilities and trust. The vulnerability is difficult to find (ED=3). The other factors EE, AW and ID are very low (1) as the vulnerabilities at the cognitive and management layers are unknown, and the attacks are detected actively due to complete situational awareness.

Table 8. Evaluation results.

#	Threat Scenario	Security Element (α)	Impact Factors				Vulnerab. Factors				Risk Level
			LC	LI	LA	LAC	ED	EE	AW	ID	
1	Unauthorized access by node capture	NACE (0.75), AACE (0.75), SACE (0.75)	9	1	1	9	3	3	9	1	**Low** I=5, V=1
2	Eavesdropping of wireless links	CE(1.0), TSE (1.0)	9	1	1	9	3	9	9	9	**Low** I=5, V=0
3	Denial-of-Service	RSE (0.75), PACE (0.5), TMFE (1.0), VME (0.5)	2	1	9	7	3	3	6	1	**Low** I=4.75, V=1,6
4	Violation of network operations	RSE (0.25), MACE (0.75)	2	7	7	7	3	1	1	1	**Low** I=5.75, V=1,1

The numerical values of the likelihood and impact factors are calculated using Equations 1 - 3, and finally converted to the likelihood and impact levels (low 0 ≤ 3, medium 3 ≤ 6 and high 6 – 9), and the final risk value is obtained by using the risk severity levels (Figure 7(b)). The results show that the security elements of the architecture decreased the risk level to low in all the scenarios. The result indicates that improvements are still to be designed to achieve the lowest risk level (Note) for each scenario.

7. CONCLUSION

Cognitive network-based network security is a promising approach to overcome the cybersecurity capability gaps within legacy mission critical communications networks. The cognitive layer provides the dynamic and self-learning network security capabilities for better situational awareness, faster reaction, and automated adaptations. The SWOT analysis results many benefits of cognitive network-based security, although implementation and overall system complexity may be challenging.

Implementing the cognitive security requires a novel approach also in architectural design. The proposed architecture introduces a layered model with the software-defined security elements. Evaluating an architecture model is very challenging. The scenario-based evaluation shows that the architecture meets the design requirements in the chosen threat scenarios as the risk level appears low. However, the results are rough, and not absolute.

Future research includes many areas. The architecture model requires more detailed description for the functionalities and protocols of each security element. This contains element to provide capabilities. Also, the architecture needs to be evaluated against real world threat scenarios. The further research should also focus on decision-making algorithms, input and output data of the process and the control channel problematic.

REFERENCES

[1] *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world*, Cabinet Office, November 2011.

[2] R. W. Thomas, L. A. DaSilva and A. B. MacKenzie, “Cognitive Networks,” in *Proc. DySPAN*, Baltimore, 2005, pp 35-60.

[3] K. Geers, *Strategic Cyber Security*, NATO Cooperative Cyber Defence Centre of Excellence, June 2011.

[4] A. K. Agarwal and Wenye Wang, “Measuring performance impact of security protocols in wireless local area networks,” in *Proc. 2nd International Conference on Broadband Networks*, Vol. 1, 2005, pp. 581 - 590.

[5] M. Ahmad, S. Taj, T. Mustafa and M. Asri, “Performance analysis of wireless network with the impact of security mechanisms,” in *Proc. ICET*, Cairo, 2012, pp. 1 - 6.

[6] L. Troell, B. Hartpence and S. Simons, “Comparative Performance of Layer 2 and IPSec Encryption on Ethernet Networks,” *Research Report*, Security and Systems Administration Department, Rochester Institute of Technology Networking, October 2006.

[7] D. Kuptsov, O. Garcia, K. Wehrle and A. Gurtov, “On Applications of Cooperative Security in Distributed Networks,” in *Proc. IFIPTM*, Morioka, Japan, 2010.

[8] M. E. Whitman and H. J. Mattord, *Principles of Information Security*, Cengage Learning, 2011.

[9] J. M. Kizza, *Guide to Computer Network Security*, Springer, 2009.

[10] R. W. Thomas, “Cognitive Networks,” Ph.D. dissertation, Virginia Polytechnic Institute and State University, June 15, 2007.

[11] J. R. Boyd, “The Essence of Winning and Losing,” a five slide set of presentation, presented in 28 June 1995.

[12] Q. H. Mahmoud (ed.), *Cognitive Networks: Towards Self-Aware Networks*, John Wiley & Sons, Ltd, 2007.

[13] R. W. Thomas, D. H. Friend, L. A. DaSilva and A. B. MacKenzie, “Cognitive Networks: Adaptation and Learning to Achieve End-to-End Performance Objectives,” *IEEE Communication Magazine*, vol. 44, pp. 51-57, Dec. 2006.

[14] N. Pahl and A. Richter, *SWOT Analysis - Idea, Methodology and a Practical Approach*, GRIN Verlag, 2009.

[15] A. P. Karkkainen and C. Candolin, “Ensuring Privacy in a Network Centric Environment,” in *Proc. ECIW 2008*, 2008, pp. 111-118.

[16] A. P. Karkkainen and C. Candolin, “Multilevel Security in a Network-Centric Environment,” in *Proc. ECIW 2009*, 2009, pp. 134-141.

[17] A. P. Karkkainen, “Ensuring Communication Security in Delay-Tolerant Networks,” in Proc. ICIW-2010, 2010, pp. 193-201.

[18] A. P. Karkkainen, “Improving Situation Awareness in Cognitive Networks Using the Self-Organizing Map,” in Proc. IEEE CogSIMA, 2011, pp. 40-47.

[19] A. P. Karkkainen, “Improving Cyber Defence of Tactical Networks by Using Cognitive Service Configuration,” in *Proc. ECCWS-2013*, 2013, pp. 135-143.

[20] A. P. Karkkainen, “Cyber Threat Management in Cognitive Networks,” *in Proc. ECIW 2012*, 2012, pp. 320-328.

[21] J. Burbank, “Security in cognitive radio networks: the required evolution in approaches to wireless network security,” in *Proc. CrownCom*, 2008, pp. 1- 7.

[22] Z. Chaczko, R. Wickramasooriya, R. Klempous, and J. Nikodem, “Security threats in cognitive radio applications,” in *Proc. INES*, Las Palmas, 2010, pp. 209 – 214.

[23] T. C. Clancy and N. Goergen, “Security in cognitive radio networks: threats and mitigation,” in *Proc. CrownCom*, 2008, pp. 1–8.

[24] *Survey of Architecture Frameworks, ISO/IEC/IEEE 42010*. [Online]. Available: http://www.iso-architecture.org/42010/afs/frameworks-table.html

[25] *Security architecture for systems providing end-to-end communications*, Series X: Data Networks and Open System Communications and Security, ITU-T Recommendation X.805, ITU-T Study Group, October 2003.

[26] N. Rathaus and G. Evron, *Open Source Fuzzing Tools*, Syngress, 2011.

[27] M. Muter, “Model-Based Security Evaluation of Vehicular Networking Architectures,” in *Proc. ICN*, Menuires, France, 2010, pp. 185-193.

[28] *Information Technology Security Evaluation Criteria (ITSEC)*, Provisional Harmonised Criteria, ECSC-EEC-EAEC, Brussels, June 1991.

[29] *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model*, Version 3.1, Revision 3, July 2009.

[30] A. Alkussayer and W. H. Allen, “A scenario-based framework for the security evaluation of software architecture,” in *Proc. IEEE ICCSIT*, 2010, pp. 687-695.

[31] P. Clements, R. Kazman and M. Klein, *Evaluating Software Architectures: Methods and Case Studies*, Addison-Wesley, 2002.

[32] F. Swiderski and W. Snyder, *Threat Modeling*, Microsoft Press, 2004.

[33] *OWASP Testing Guide*, The Open Web Application Security Project (OWASP) Foundation, Version 3.0, 2008.

BIBLIOGRAPHY OF AUTHORS

Major, M.Sc. (Eng.) Anssi Kärkkäinen graduated from the Finnish National Defence University in 2000. He also graduated a Master of Science (Engineering) degree from Helsinki University of Technology in 2005. Currently he is carrying out his doctoral studies at the Department of Communications and Networking of Aalto University. His current assignment is a Staff Engineer for J6 Cyber Defence at the Defence Command Finland.