Journal of Telecommunications System & Management

Oakes et al., J Telecommun Syst Manage 2018, 7:2
DOI: 10.4172/2167-0919.1000171

Research Article Open Access

A Dynamic Operational Model for Improving the Resilience of Wireless Networks against Jamming

Oakes BD[1]*, Mattsson L-G[2], Näsman P[3] and Bäckström M[4]

[1]ABB, HVDC, SE-77131 Ludvika, Sweden
[2]Department of Civil and Architectural Engineering, KTH Royal Institute of Technology, SE-10044 Stockholm, Sweden
[3]Center for Safety Research, KTH Royal Institute of Technology, SE-10044 Stockholm, Sweden
[4]Saab Aeronautics, SE-58188 Linköping, Sweden

Abstract

A dynamic operational model for improving operational resilience of wireless net-works using dynamic routing against jamming attacks is presented. The model highlights the consideration of the time dimension, a determining factor of infrastructure resilience. The operation of a wireless network is optimised so as to minimise the additional operational cost, or more generally resilience loss, when the network is subjected to a coordinated jamming attack. The model first minimises the total amount of blocked data traffic using dynamic routing, i.e. routing the traffic c depending on the signal to noise ratios at the wireless access points. Assuming the operator is able to discern and sound out jamming signals, the jammers are located and neutralised by search teams prioritizing jammers that have the highest potential impact on the resilience loss. The searches for the jammers have finite time durations, which are captured in the model. The cost per unit of time is presented as a function of time for a hypothetical Wireless Local Area Network (WLAN) attacked at two locations by jammers.

Keywords: Jamming attacks; Resilience; Critical infrastructure; Wireless networks; Intentional electromagnetic interference (IEMI)

Introduction

Resilience engineering has in recent years been a highly discussed topic [1,2] largely due to the following reasons: (1) modern society is becoming increasingly dependent on various infrastructures; e.g. electric power, transportation, telecommunications, (2) infrastructures are becoming more interdependent and (3) with the vast technological advancements, infrastructures are more complex and can be more vulnerable to a broader variety of hazards. The increased concern of intentional attacks on critical infrastructure has urged the development of operational models to protect infrastructure systems [3]. At the same time, it has become apparent that modern societal infrastructure is heavily dependent on electrical and electronic components and systems, e.g. the electric power grid, wireless and cellular networks, and even water distribution networks [4]. The advancing connected transportation system of the near future with more and more autonomous vehicles will provide another such infrastructure. Models for analysing the vulnerability of electric power grids and other electromagnetically susceptible infrastructures are seen in literature [5-7]. More recently, attention has been drawn to the particular hazard of intentional electromagnetic interference (IEMI) [8,9] and on cost-effectively managing risks that can be caused by electromagnetic interference [10]. IEMI generally includes low-level interference, High Power Microwaves (HPM), High Altitude Electromagnetic Pulse (HEMP) and other kinds of High Power Electromagnetic (HPEM) environments such as current injection (IEC 2003). IEMI is most commonly comprised of low-level interference, which includes jamming (or front-door interference) where energy is coupled through antennas distorting the received signal, and so called back-door interference [11], i.e. interference in electronic circuits caused by coupling of electromagnetic energy to cables and leads. In more extreme cases permanent damage of receivers and electronic equipment can also be achieved. Typically, permanent damage is caused by junction burnouts in semiconductors [12], resulting from insufficient heat dissipation upon an instantaneous high surge of current across the junction. Permanent damage however, is more difficult to accomplish than interference, typically requiring much higher power and energy levels demanding a greater level of skill, resources and precision (e.g. access to military HPM weapons or even a (HEMP). Mainly due to the low requirement on power levels, we consider jamming, i.e. interference with radio (and radar) receivers at their operating frequency, to be the most likely form of IEMI in the context of disturbing the transmission of wireless networks. High voltage transformers and circuit breakers have been known to become damaged in the presence of rare and extreme geomagnetic storms or lightning strikes [13,14]. In such events, permanent damage occurs practically instantaneously. Conversely, jamming is limited to causing temporary communication interruption only during the time the jammer is turned on. Jammers generally have a finite battery lifetime, setting an upper limit on the duration of interference and thereby the magnitude of impact on the attacked system. It is a well-known fact that the severity of a disruption increases with its duration, e.g. transportation delays or power outages [15], and that a key parameter for fast infrastructure recovery is time management [16]. Undeniably, the same typically applies for jamming attacks, too. The open nature of wireless communication leaves it vulnerable to jamming attacks [17]. Wireless networks come in many different variations. Major features that classify wireless networks are coverage range and if the network is an infrastructure or ad hoc network [18]. While wireless infrastructure networks rely on pre-existing infrastructure in the form of routers and switches to relay traffic between users, devices can connect directly to each other in wireless ad hoc networks. Wireless ad hoc networks have in the past been applied primarily for military or emergency situations

***Corresponding author:** Oakes BD, ABB, HVDC, SE-77131 Ludvika, Sweden, Tel: +46730491112; E-mail: boakes@kth.se

Received October 03, 2018; **Accepted** October 05, 2018; **Published** October 12, 2018

Citation: Oakes BD, Mattsson L-G, Näsman P, Bäckström M (2018) A Dynamic Operational Model for Improving the Resilience of Wireless Networks against Jamming. J Telecommun Syst Manage 7: 171. doi: 10.4172/2167-0919.1000171

[19], however, due to the high demand on connectivity today, they are becoming more common commercially, e.g. often applied to smart homes, smart grids, automatic meter reading, lighting controls, building automation systems (sometimes called wireless sensor networks), tank monitoring, medical devices and fleet applications e.g. ZigBee [20] or communication within businesses [21]. There is an increasing concern over coordinated intentional attacks [22]. Recent studies have proposed models to analyse the risk of IEMI [23] and even applied operational models to the IEMI threat [24]. Random graph theoretical models and percolation theory have also been proposed to assess the threat of IEMI on wireless networks [25]. Linear programing models have been applied to optimise the traffic flow in a wireless network under a coordinated jamming attack [26]. The vast majority of existing such models and operational models are static, meaning they involve the analysis of infrastructure vulnerability without consideration of the time dimension [27]. This simplication is a critical one, and in many cases does not render useful advice since the impact on the cost on society due to the duration of a disruption and the recovery time of the affected system are not taken into account. Dynamic operational models as opposed to static ones, model infrastructure performance and restoration over time and are recently becoming more applied [28]. To the best knowledge of the authors, no studies have yet applied dynamic operational models to the threat of IEMI explicitly, or more relevantly, to jamming. In this article, we provide a foundation for establishing a dynamic operational model in the form of a stepwise linear program that will help a system operator make decisions to guide the operation of a wireless network so as to minimise the total operational cost resulting from a coordinated jamming attack. The operator is presumed to have a number of search teams at her disposal that try to locate and neutralise hidden jammers with a finite battery time. The search for the jammers takes time and the longer the jammers are turned on, the longer the network remains congested and the higher the operator penalty cost. The proposed model is kept general in the sense that it can be applied to both infrastructure and ad hoc wireless networks. By default, the model presented here is adapted for wireless infrastructure networks. However, it can be easily modified to model wireless ad hoc networks, too. These modifications are pointed out in the paper when relevant. Also, we do not attempt to detail any specific data transmission or routing protocols between devices, due to the multiplex of existing wireless network technologies [29]. We assume that communication between devices is one-way and that no master or authentication signal is required from a device to receive messages from another. Data is simply sent from one device to another and it is assumed that the necessary routing is managed by the network in a centralised or decentralised manner. This simplification leaves room for adjusting the model to a specific type of wireless network, whether it be infrastructure or ad hoc networks. In practice, the applied operational model should be tailored to model a specific type of scenario.

Assumptions and Delimitations

The operational model is delimited to analyse a single wireless network with the purpose of providing network users with the means to transmit and receive information to each other, i.e. the information has an origin and a destination. A user could be a computer, cell phone or another smart device. Network vertices represent wireless access points (WAPs). Users must connect to at least one WAP to communicate with each other[1]. For this study, the traffic demand from one vertex to another is assumed constant in time. Also, we assume the network is not connected to the Internet or a central database and that data does not have to be sent to a central vertex before it reaches the destination vertex. Direct paths between vertices on which information can be sent are henceforth called edges. Each edge has a specified channel data rate capacity. It may not be possible or not preferable to send information directly from origin to destination vertex. If so, information may be sent from the origin vertex via the term wireless access point (WAP) is generally used for wireless infrastructure networks (not ad hoc) and refers to the terminal from the user to the router. In wireless ad hoc networks, vertices represent user devices which can connect directly without a WAP if within range. Other connecting vertices until it reach the destination vertex. The received desired signal impinging on a vertex can be distorted by noise, effectively reducing the channel data rate capacity of the sending edge.

The network is coordinated by the operator - a decision making entity comprised of humans and computers, whose objective is to manage the network operation so as to reduce the operational cost as much as possible, even (especially) in the event of disruptions. The operator is issued a transmission cost to send information between two connecting vertices. The total operational cost per unit of time does not directly include any user costs, only transmission costs [30] and, if the operator fails to meet user demand, i.e. traffic is blocked between users, she is issued a penalty cost. The penalty cost is the operator's monetary loss per unit of time which increases with the extent of affected users. Typically, the penalty cost is composed of compensation for user lost revenue, operator reputational damage and lost business opportunities [31]. If the network is used within an organisation or company which is also responsible for operating the network i.e. the operator, the penalty costs are issued on that company. However, if the network is used by several companies or individuals, the penalty cost is internalised, i.e. the operator must compensate the users for their loss. Penalty costs are generally many times greater than transmission costs [32]. The operator is therefore, in the event of a disruption, highly inclined to make comprehensive efforts by means of dynamically rerouting data and working to eliminate the source of disruption as swiftly as possible to avoid long periods of user unmet demand.

The longer the duration of a disruption, the greater the monetary loss for the operator. An often-applied metric in resilience engineering used to measure how well a society or an organisation copes with a disruption, is the performance loss or loss of resilience. The resilience loss is generally defined as being equal to, or proportional to the additional total cost on society or the organisation during and after a disruption [33,34]. Resilience loss is conceptualised in Figure 1 and is typically identified by the area between the level of full functionality and the actual system functionality over time. We will apply the metric of resilience loss to define the additional operational cost resulting

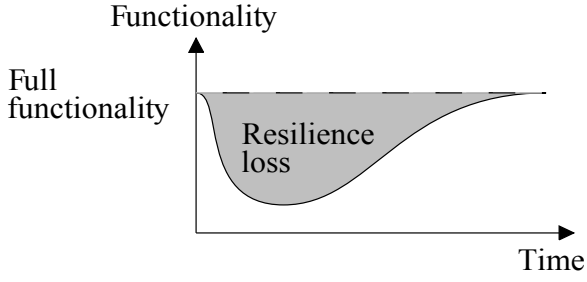

Figure 1: Functionality curve illustrating the concept of resilience loss.

[1]The term wireless access point (WAP) is generally used for wireless infrastructure networks (not ad hoc) and refers to the terminal from the user to the router. In wireless ad hoc networks, vertices represent user devices which can connect directly without a WAP if within range.

from a disruption. However, we do not use the notion of functionality as seen in Figure 1. Instead, we define the resilience loss as the area between the operational cost per unit of time when the network is fully functional (network is operated at minimal operational cost per unit of time) and the actual operational cost per unit of time. Resilience loss here, is defined based on monetary loss since cost per unit of time is a commonly applied performance metric in operational models [27].

We presume the existence of an attacker; a malicious individual or group of individuals who intend to disturb the network operation so as to render the operator a high resilience loss. Since the context of this article is jamming attacks on wireless networks, the attacker is conned to only using jammers as means to achieve his objective, even if other means of attack may be a more rational choice for the attacker. Here, we consider scenarios where the attacker deploys a finite number of jammers at publicly accessible locations and abandons them there. For modelling simplicity, we assume that the attacker turns all jammers on at the same time. During the time the jammers are turned on, vertices will experience interference, potentially reducing the capacity of certain edges. Jammers are assumed to remain at these same locations and are not turned off until their batteries completely discharge or they are located and neutralised by the operator. We consider this an adequate assumption since IEMI attacks are typically recognised as covert and anonymous in the literature, where jammers may be hidden at various locations and difficult to detect [35]. For simplicity, jammers are assumed isotropic radiators; their radiation pattern can spread across a geographical area and interfere with network vertices (Figure 2). For further reading, the impact on different types of networks caused by disturbances spreading out over geographical regions has been presented in multiple studies [36-38]. Moreover, jammers can produce different waveforms. However, for simplicity of calculation, we only account for jammers which produce (band-limited) white Gaussian noise and not coloured or frequency dependent noise. The operator is assumed to be able to measure the level of jamming noise at each vertex, and on observing these levels, tries to reduce the resilience loss as much as possible by rerouting data traffic in the network provided this can be done at a feasible price and also assigns search teams to locate and neutralise the jammers [39]. In practice, an operator does not continuously make decisions, but naturally at discrete points in time, to be called the decision times. In the model, it is assumed the operator uses a myopic approach to make her decisions since she is only able to know the present state of network functionality and cannot predict how the network will be disrupted in the future. At each decision time, the operator chooses her decision variables including which jammers to search for so as to reduce the additional operational cost between the current decision time and the next as much as possible based on her assumption that the jamming signal strengths will remain the same until the jammers are neutralised. A jammer may suddenly run out of battery, which will immediately change the course of operation. However, jammer battery times cannot be known by the operator and therefore cannot be anticipated in her decision making. For the sake of brevity, we assume that jammer noise only in influences the channel capacity and not the transmission costs. However, in practice, transmission costs can increase due to noise (e.g. if the transmission power on an edge is increased to compensate for the jamming signal [40]. In this article, we do not attempt to model the behaviour of an attacker and where he decides to deploy the jammers, as in the wireless network jamming problem [41-43]. Therefore, we do not model the optimum decisions of both a rational attacker and the operator assuming they have perfect information about their adversaries as in a Stackel berggame. In a real scenario however, the attacker will try to place jammers near WAPs so that a large portion of the jamming signal power is received by the WAPs, thus reducing the channel data rate capacity of the sending edges. The main focus here is how the operator makes decisions over time so as to minimise the resilience loss resulting from a coordinated jamming attack.

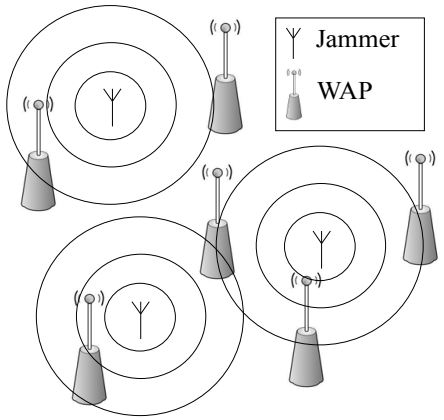

Figure 2: The figure illustrates a coordinated attack on a network of wireless access points (WAP) which is irradiated by three jammers; contours represent the radiated noise generated by the jammers. The net signal power at a given point is the superposition of all contributions.

Model Formulation

The network

The wireless network is represented by the graph $\mathcal{G}=(\mathcal{V},\mathcal{E})$ where $v \in \mathcal{V}=\{1, 2,\ldots V\}$ denotes the set of vertices and $[u, v] \in \mathcal{E}$ the set of edges, i.e. connected pairs of vertices $u,v \in \mathcal{V}$, $u \neq v$ in the network. Information in the network has an origin and a destination vertex. The traffic intensity from vertex u to vertex v is defined as the average packet arrival rate times the average packet transmission time and has the dimensionless unit of Erlang (ITU2005)[2]. The traffic intensity demand from node u to node v is denoted d_{uv}, where $d_{uv} \geq 0 \; \forall \; u, v \in \mathcal{V}$, $u \neq v$. Notice that users near vertex $v \in \mathcal{V}$ may send traffic to other users at the same vertex v and thus we denote this demand as $d_v \geq 0$ ($d_v=0$ for ad hoc networks). Each edge $[u, v] \in \mathcal{E}$ has a capacity D[u,v]-the maximum allowed traffic intensity across edge [u,v] per unit of time. Traffic is sent across paths (with no cycles) $p \in \mathcal{P}$, where $\mathcal{P}$ is defined as the set of all sets of connected vertices and edges $p=\{v_1, [v_1, v_2], v_2, [v_2, v_3],\ldots, v_{M-1}, [v_{M-1}, v_M]\}$, such that all of the vertices and edges are distinct, i.e. for all $m \neq n$ such that $v_m, v_n \in p$, $v_m \neq v_n$ and for all $m \in \{1,2,\ldots M-1\}$, $[v_m, v_{m+1}] \in \mathcal{E}$. Each path p has a transmission cost c_p-the cost per unit of time per Erlang across path p, defined as [44]:

$$c_p = \sum_{[u,v] \in p} c_{[u,v]} \tag{1}$$

Here, we assume the transmission cost of an edge $[u, v] \in \mathcal{E}$ is independent of the level of traffic on that edge as opposed to what is the case in e.g. transportation systems, and denote these costs c[u,v]. The cost per unit of time per Erlang of sending data locally between users at vertex v is denoted c^0_v and is also considered a constant. Moreover, the local capacity of vertex v is denoted D_v.

The channel capacity in Erlang of edge [u, v] is dependent on the interference noise power levels on the edge and is given by the Shannon channel capacity equation [45]:

[2]Erlang may alternatively be conceived as the average number of concurrent packets sent across an edge or a path at a given point in time (and is dimensionless).

$$D_{[u,v]}\left(N_{[u,v]}\right)=\frac{B_{[u,v]}}{G_{[u,v]}}\log 2\left(1+\frac{S_{[u,v]}}{N_{[u,v]}}\right) \quad (2)$$

where B[u,v] is the channel bandwidth in Hertz of edge [u, v], S[u, v] is the average incoming signal power in Watts at vertex v from edge [u, v], N[u, v] is the average noise power level in Watts on edge [u, v] and G[u, v] is the average packet data rate in bitsper second on edge [u, v]. The same equation holds for vertex capacities D_v, only that B[u, v], S[u, v], N[u,v] and G[u, v] are replaced by B_v, S_v, N_v and G_v, respectively, where B_v is the bandwidth of the channel receiving data from local computers at vertex v, S_v is the average signal power of this channel, N_v is the noise on the channel and G_v is the average packet data rate sent between local computers at vertex v.

The attacker

The attacker possesses a set of identical jammers $j \in \mathcal{J}=\{1, 2,\ldots J\}$ which he deploys in the two-dimensional topographic map at locations $l_j \in \mathbb{R}^2$. The jammers are omni-directional, band-limited Gaussian white noise jammers. All jammers $j \in \mathcal{J}$ are turned on at time τ=0. Let $g_v \in \mathbb{R}^2$ denote the position of vertex v. Assuming both receivers and transmitters are isotropic, i.e. have a zero gain, the average noise power impingingat vertex v generated by jammer j is estimated using Friis transmission equation as [46]:

$$N_{vj}\left(l_j,g_v,z_j(\tau)\right)=\left(1-z_j(\tau)\right)\frac{c^2P_j}{\left(4\pi f_j\right)^2\left\|l_j-g_v\right\|^2} \quad (3)$$

where $\left\|l_j-g_v\right\|$ is the Euclidean distance in metres betw.een jammer j and vertex v,f_j is the centre frequency in Hertz of jammer j, c ≈ 3.108 m/s is the speed of light in vacuum, P_j is the radiated power (rms) in Watts of jammer $j, \overline{\tau}_j > 0$ is the battery time in hours of jammer j and zj(τ)=0 if $0 \le \tau \le \overline{\tau}_j$ 0 and $z_j(\tau)$=1 otherwise. As linear superposition of fields applies in vacuum [47], we assume this is an acceptable approximation also in our case. The total noise power (rms) in Wattsat each edge [u, v] ∈ $\mathcal{E}$ at time is then the sum of all jammer contributions at the receiving vertex v:

$$N_{[u,v]}\left(z(\tau)\right)=N_0B_{[u,v]}+\sum_{j=1}^{J}N_{vj}\left(l_j,g_v,z_j(\tau)\right) \quad (4)$$

where $z(\tau)=(z_1(\tau), z_2(\tau),\ldots,z_J(\tau))$ is the vector indicating which jammers have run out of battery, and the constant $N_0=\kappa T$ is the thermal noise power spectral density, where is Boltzmann's constant and T the ambient temperature in Kelvin. It is worthwhile noting that when a jamming signal is present, the N_0B[u, v]term can be neglected since it is typically many orders of magnitude smaller than the jamming noise N_{vj}.

The operator

Recall that the operator's objective is to maintain network operation at the lowest feasible cost, even in the event of disruptions. When a disruption occurs, the operator tries to minimise the resilience loss by rerouting traffic flow in the network and by using available search teams to locate and neutralise jammers. In the following, three different operator models are presented. The first is the most basic - the operator does not attempt to locate and neutralise jammers, only reroutes flows at the decision times so as to minimise the operational cost per unit of time. In the second model, we expand the first model by allowing the operator to locate and neutralise jammers assuming a negligible search time and in then al model, the second model formulation is made more realistic by introducing a finite search time [2,3,48].

Instantaneous operational model without search teams: This establishes the basis of our operator model. Here, the operator is not concerned about the jammers locations, but only how she can reroute the traffic flow so as to minimise the operational cost per unit of time given the edge capacities and the traffic intensity demand.

The penalty cost is defined as the cost per blocked Erlang per unit of time from vertex u to vertex v and is denoted π_{uv}, and the local penalty cost at a vertex v is denoted π_v.

Decision times are the time points kΔτ, where the time step Δτ is the time between decision times and k ∈ {0, 1,….,K} is the time step number. Here, K is the minimum integer such that $K\Delta\tau \ge max\left[\overline{\tau}_1,\overline{\tau}_2,\ldots,\overline{\tau}_j\right]$. Different decisions may be taken by the operator as long as k > K. When k > K, the operator will not alter her decision since all jammer batteries are at time max $\left[\overline{\tau}_1,\overline{\tau}_2,\ldots,\overline{\tau}_j\right]$ and thus, from this point, the noise power at all edges is simply the thermal noise level N_0B[u, v] and operation will return to normal. For simplicity, we use the notation $z^k_j=z_j(k\Delta\tau)$ and thereby dene the vectors $z_k=(z^k_1, z^k_2,\ldots,z^k_J)$. As seen in eqn. (2), the edge capacities and vertex capacities depend on the noise levels at the vertices. They are bounded from above by the corresponding levels for an undisrupted, fully functional network [49,50]:

$$D[u,v](N[u,v](z^k))\le D[u,v](N[u,v](zK))=DK[u,v],\forall[u,v]\in\mathcal{E} \quad (5)$$

where for an undisrupted, fully functional network, edge capacities and vertex capacities acquire their maximum levels $D^K_{[u,v]}$ and D^K_v, respectively. Notice that z^K is the unit vector of size J, and thereby all $N_{[u,v]}(z^K)$ and $N_v(z^K)$ are equal to $N_0B_{[u,v]}$ andN_0B_v, respectively, as a result of eqn. (4).

Operator decision variables at each decision time k are the traffic intensities on the paths, denoted by Y kp representing the traffic intensity in Erlang on path p. The instantaneous operator problem at decision time k ∈ {0,1,…..K} is formulated as a linear program [27] (the fundamental difference being that here the time dimension is included):

$$\begin{aligned}
&\hat{C}^k=\min_{Y^k_p}\sum_{p\in\mathcal{P}}cpY^k_p+\sum_{u\in\nu,u\neq\nu\nu\in\nu}\sum\pi_{uv}\left(d_{uv}-\sum_{p\in\mathcal{P}_{uv}}Y^k_p\right)\\
&+\sum_{u\in\nu}c^0_v\min\left[D_v\left(N_v\left(z^k\right)\right),d_v\right]+\\
&+\sum_{u\in\nu}\pi_v\left(d_v-\min\left[D_v\left(N_v\left(z^k\right)\right),d_v\right]\right)\\
&s.t\sum_{p\in P_{uv}}Y^k_p\le d_{uv}\forall u,v\in\mathcal{V},u\neq v,\\
&\sum_{p\in P}\delta_{p[u,v]}Y^k_p\le D_{[u,v]}\left(N_{[u,v]}\left(z^k\right)\right)\forall[u,v]\in\mathcal{E},\\
&Y^k_p\ge 0\forall p\in\mathcal{P},
\end{aligned} \quad (P.1)$$

where $\hat{C}^k$ denotes the minimum operational cost per unit of time at decision time $k, P_{uv}\subset P$ denotes the set of all paths from vertex u to vertex v, and δ_p[u,v]=1 if[u, v] ∈ p and p[u,v]=0 otherwise. Notice that ˆ is the operational cost per unit of time when the network is not under attack, i.e. fully functional.

The problem formulation (P.1) involves solving K+1 linear programs [51].

Instantaneous operational model with search teams and negligible search time: We now enable the operator to search for and neutralise jammers assuming searches take no time at all. In order to decide which jammers to neutralise at each decision time, the operator must know how much the removal of each jammer will improve the operational cost per unit of time. As in the previous problem formulation, the operator can measure the noise level at each vertex.

However, now, we also assume that she is able to accurately discern the noise signal contributions from each jammer. The instantaneous operational model is expanded by adding the new binary decision variables X^k_j, equal to 1 if the operator decides to neutralise jammer j and 0 if not. Hereby we also define the vector $X^k=(X^k_1,X^k_2,\ldots,X^k_J)$. In addition, the operator has a limited number of available search teams A (a positive integer), and can only neutralise A jammers at each decision time. At each decision time k, the operator thus decides not only the path flows, but also which jammers to neutralise in a manner that minimises the operational cost per unit of time at decision time k [1,52].

The noise contribution from jammer j at vertex v at decision time $k \geq 0$ will depend on whether the jammer has been neutralised or not and if the battery is still powered. Letting the vector be the value of the vector X^k which reduces the operational cost per unit of time the most at decision time k, we recursively define the binary variable indicating the number of active jammers at time points k>0 as:

$$x_j^k = \begin{cases} 1, \left(x_j^{k-1}=1\right) \vee \left(z_j^k=1\right) \vee \left(\hat{X}_j^k=1\right), \\ 0, otherwise \end{cases} \tag{6}$$

and since all jammers are initially active, $x^0_j=0$.

The operator's expanded optimisation problem with negligible search times at decision time $k \in \{0,1,\ldots K\}$ is:

$$\begin{aligned} &\hat{C}^k = \min_{Y_p^k} \sum_{p\in\mathcal{P}} c_p Y_p^k + \sum_{u\in\mathcal{V},u\neq v v\in\mathcal{V}} \sum \pi_{uv}\left(d_{uv} - \sum_{p\in\mathcal{P}_{uv}} Y_p^k\right)+ \\ &+\sum_{u\in\nu} c_v^0 \min\left[D_v\left(N_v\left(X^k\right)\right),d_v\right]+ \\ &+\sum_{u\in\nu} \pi_v\left(d_v - \min\left[D_v\left(N_v\left(X^k\right)\right),d_v\right]\right) \\ &s.t \sum_{p\in P_{uv}} Y_p^k \leq d_{uv} \forall u,v\in\mathcal{V},u\neq v, \\ &\sum_{p\in P} \delta_{p[u,v]} Y_p^k \leq D_{[u,v]}\left(N_{[u,v]}\left(X^k\right)\right) \forall [u,v]\in\mathcal{E}, \\ &Y_p^k \geq 0 \forall p\in\mathcal{P}, \\ &X_j^k \in \{0,1\} \forall j\in\mathcal{J}, \\ &X_j^k \geq x_j^k \forall j\in\mathcal{J}, \\ &\sum_{j\in\mathcal{J}} X_j^k \leq \sum_{j\in\mathcal{J}} x_j^k + A \end{aligned} \tag{P.2}$$

Here too, $\hat{C}^K$ is the operational cost per unit of time when the network is fully functional. This problem formulation (P.2) also involves solving K+1 optimisation problems which are now of the mixed integer linear programming type [53].

Recall that we dene the resilience loss as the area between the operational cost per unit of time for the disrupted network and the operational cost per unit of time when the network is fully functional, i.e. $\hat{C}^K$. In practice, the operational cost per unit of time may change during the periods between the decision points k and k+1 when optimal decisions are taken, since the noise at the vertices may change during these periods. Defining the vectors $q(\tau)=(q_1(\tau), q_2(\tau),\ldots. q_J(\tau))$ and $q^k=(q^k_1, q^k_2,\ldots,q^k_J)$, we define the continuous operational cost per unit of time as:

$$\begin{aligned} &\hat{C}(\tau) = \hat{C}^k + +\sum_{u\in\nu} c_v^0 \min\left[D_v\left(N_v\left(q(\tau)\right)\right),d_v\right] \\ &-\sum_{u\in\nu} c_v^0 \min\left[D_v\left(N_v\left(q^k\right)\right),d_v\right] \\ &+\sum_{u\in\nu} \pi_v\left(d_v - \min\left[D_v\left(N_v\left(q(\tau)\right)\right),d_v\right]\right) \\ &-\sum_{u\in\nu} \pi_v\left(d_v - \min\left[D_v\left(N_v\left(q^k\right)\right),d_v\right]\right) \end{aligned} \tag{7}$$

for $k\Delta\tau \leq \tau < (k+1)$, $\forall\ k \in \{0,1,\ldots., K\}$ with $q(\tau)=z(\tau)$ and $q^k=z^k$ for optimisation problem (P.1) and with $q(\tau)=\max\left[z(\tau),\hat{X}^k\right]$ and $q^k=\hat{X}^k$ for (P.2), and where the maximisation of the vectors is component-wise. The resilience loss caused by a disruption given optimal counteractions, can then be expressed as (we can let the upper bound of the integral be infinity since $\hat{C}(\tau)=\hat{C}^K$, for $\tau \geq K\Delta\tau$):

$$\wedge = \int_0^\infty \left(\hat{C}(\tau) - \hat{C}^K\right) d\tau \tag{8}$$

Notice that in practice, however, it is difficult to generally specify $\hat{C}(\tau)$ since domain specific relations are required to evaluate edge flows and unmet demand at vertices between the operator decision times. If $\hat{C}(\tau)$ cannot accurately be estimated, one may assume it remains constant between decision times which more accurately holds for small.

The function $\hat{C}(\tau)$ and resilience loss $\wedge$ may be conceptualised as in Figure 3. Notice that an infinite resilience loss cannot occur since all jammers have a finite battery lifetime and the operator is able to neutralise up to A jammers at each decision time.

Instantaneous operational model with search teams and finite search times equal to one time step: The negligible search time assumption in the previous model suffices solely as a starting point to further develop a more realistic operational model. In practice, search times may be long and cannot be omitted when evaluating resilience loss. For this reason, we now combine the previous two models to formulate a more realistic model with a finite search time. For simplicity, we let the search time be equal to one time step, $\Delta\tau$, assuming all jammers take the same amount of time to locate and neutralise. Like (P.2), this problem is recursive. However, the operational cost per unit of time and optimal flow decisions at the present decision time will depend on which jammers she chose to neutralise at the previous decision time and not at the present time. The operator does not only minimise the

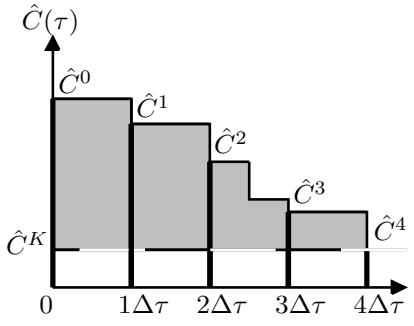

Figure 3: Example of the operational cost per unit of time as a function of time when the operator is able to reroute edge traffic flows, regulate unmet demand and search for jammers at the decision times indicated by bold vertical lines (K=4). The grey area represents the resilience loss. Notice that between decision times $2\Delta\tau$ and $3\Delta\tau$ one of the jammer batteries goes at and the operational cost per unit time drops.

operational cost per unit of time at the present decision time k (as in the previous two models), but also choses which jammers to neutralise so as to minimise the optimal operational cost per unit of time at then next decision time k+1. In order to know which jammers to neutralise at decision time k, the operator must predict the noise level at the vertices at decision time k+1. Since the operator has no information about the duration of the jamming signals, i.e. the jammer battery times, a natural assumption about the myopic operator is that's he behaves as if she assumes the noise levels at the vertices remain at their present values throughout the whole time period, i.e. that $x^{k+1}=x^k$. Hence the operator solves two sub problems at each decision time k:first, (P.3) the instantaneous operator problem taking into consideration the present state of path transmission costs and edge and vertex capacities, and then (P.2) deciding which jammers to search for between decision time k and k+1 such that the operational cost per unit time is minimised when solving (P.3) at decision time k+1. The information required by the operator in (P.3) is the same as in (P.1) where the operator only requires the noise levels at the vertices to minimise the operational cost per unit of time. Hence, at each decision time, the operator decides the path flows and which jammers to neutralise.

The optimisation problem at decision time $k \in \{0, 1,\ldots,K\}$ is a modified version of (P.1) followed by (P.2). In the first subproblem at decision time k, we solve (P.1) replacing z^k by $x^k=(x^k_1, x^k_2,\ldots x^k_J)$. The first subproblem is:

$$\begin{aligned}
&\hat{C}^K = \min_{y_p^k} \sum_{p\in\mathcal{P}} c_p Y_p^k + \sum_{u\in\mathcal{V},v\in\mathcal{V}} \sum \pi_{uv}\left(d_{uv} - \sum_{p\in\mathcal{P}_{uv}} Y_p^k\right) + \\
&-\sum_{u\in v} c_v^0 \min\left[D_v\left(N_v\left(x^k\right)\right), d_v\right] + \\
&+\sum_{u\in v} \pi_v\left(d_v - \min\left[D_v\left(N_v\left(x^k\right)\right), d_v\right]\right) \\
&-\sum_{u\in v} \pi_v\left(d_v - \min\left[D_v\left(N_v\left(x^k\right)\right), d_v\right]\right) \qquad \text{(P.3)} \\
&s.t \sum_{p\in P_{uv}} Y_p^k \le d_{uv} \forall u,v\in\mathcal{V}, u\ne v, \\
&\sum_{p\in P} \delta_{p[u,v]} Y_p^k \le D[u,v]\left(N_{[u,v]}\left(x^k\right)\right) \forall [u,v]\in\mathcal{E}, \\
&Y_p^k \ge 0 \forall p\in\mathcal{P},
\end{aligned}$$

and in the second subproblem at the same decision time k, we solve (P.2) to obtain $\hat{X}^K$ to be used to solve (P.3) at the next decision time k+1. The continuous operational cost per unit of time is for problem (P.3) defined as in eqn. (7) except $q(\tau)=\max[z(\tau), x^k]$ and $q^k=x^k$.

Application of the model on a hypothetical Wireless Local Area Network (WLAN)

Now we illustrate the effect on the resilience loss of searching for the jammers by applying and comparing operational models (P.1) and (P.3) on a hypothetical WLAN attacked by two jammers. In addition, the continuous operational cost per unit of time $\hat{C}(\tau)$ is calculated at different values of Δτ in the model (P.3), in order to learn how the time step duration, i.e. the search time, affects the resilience loss.

All network data, attacker data and operator data used for this case study are exemplary and are presented in (Table 1). The network comprises three WAPs (vertices) and six wireless channels (edges) connecting these, as illustrated in Figure 4. Each WAP services a number of computers, sending and receiving data to and from each other via the WAPs in the network. The network operates on the 2.4 GHz band and the channel bandwidth is assumed to be 20 MHz as commonly used in Wi-Fi and WLAN applications [54]. Moreover, the maximal edge capacities are set to100 Erlang for simplicity and therefore, the average receive power at each vertex is assumed to be 1 mW and the packet data rate 6.7 Mbit/s. For calculation simplicity, jammer centre frequencies are assumed 3 GHz and that the noise generated by the jammers is uniformly distributed over all the channels used by the network.

Network data		**Unit**
Local demand at all vertices	d_v=0	(Erlang)
Traffic demand from vertex 1 to 2	d_{12}=100	(Erlang)
Traffic demand from vertex 2 to 1	d_{21}=150	(Erlang)
Traffic demand from vertex 1 to 3	d_{13}=100	(Erlang)
Traffic demand from vertex 3 to 1	d_{31}=50	(Erlang)
Traffic demand from vertex 2 to 3	d_{23}=50	(Erlang)
Traffic demand from vertex 3 to 2	d_{32}=100	(Erlang)
Fully functional capacity of all edges [u,v]	$D^K_{[u,v]}$=100	(Erlang)
Position of WAP 1	g_1=(0,0)	[m]
Position of WAP 2	g_2=(50,100)	[m]
Position of WAP 3	g_3=(100,0)	[m]
Attacker data		
Number of jammers 1	J=2	
Position of jammer 1	l_1=(30,100)	[m]
Position of jammer 2	l_2=(1,100)	[m]
Battery time of jammer 1	$\bar{\tau}_1$ =9	[h]
Battery time of jammer 2	$\bar{\tau}_2$ =6	[h]
Jammer radiated power	P_1,P_2=10	[W]
Jammer centre frequency	f_1,f_2=3	[GHz]
Operator data		
Transmission cost of all edges	c[u,v]=0.1	[€/h]
Penalty cost on all vertex pairs	π_{uv}=1	[€/h]
Maximum number of searches per time step	A=1	
Channel bandwidth of all edges and vertices	$B_{[u,v]},B_v$=20	[MHz]
Signal power at all edges and vertices	$S_{[u,v]},S_v$=1	[mW]
Average packet data rate of all edges and vertices	$G_{[u,v]},G_v$=6.7	[Ms^{-1}]

Table 1: Simulation data.

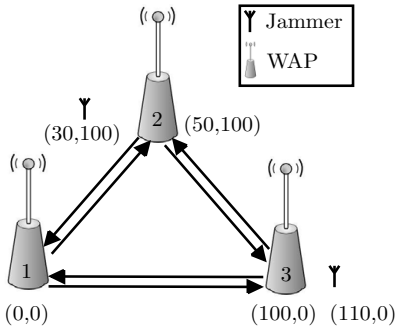

Figure 4: Hypothetical wireless local area network (WLAN) attacked by two jammers. The vertices are wireless access points (WAP), each pair of them has a specified taffic intensity demand. The coordinates mark vertex and jammer positions.

Results

The operational cost per unit time is presented over a 12 h period starting from when jammers are turned on by the attacker. The operational cost per unit of time is evaluated for operational models

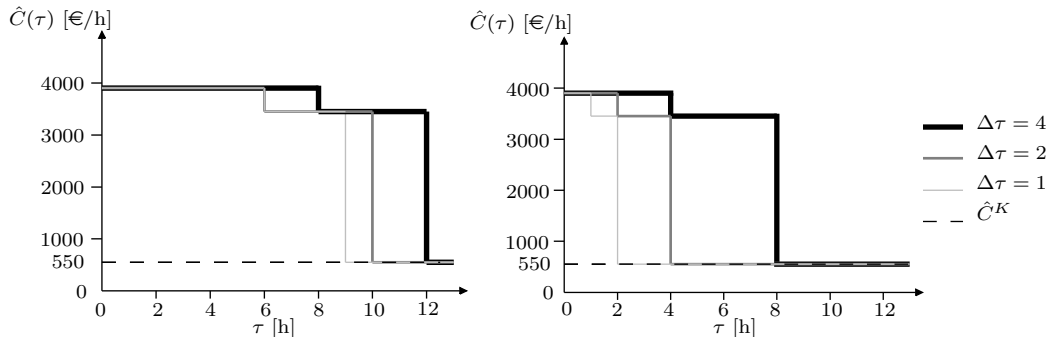

Figure 5: Operational cost per unit of time $\hat{C}(\tau)$ for problems (P.1) without search teams on the left and on the right (P.3) with finite search times equal to one time step using Δτ=4 h, 2 h, 1 h and A=1.

(P.1) and (P.3) for three different time step lengths of Δτ=4 h, Δτ=2 h and Δτ=1 h, depicted in Figure 5. As expected, the resilience loss is maximal when the operator is not allowed to search for the jammers, i.e. (P.1). In this case, the fully functional operational cost per unit of time $\hat{C}^K$ is only reattained once all jammer batteries have run out of power and the operator has no other choice than to suffer the penalty costs of unmet demand before then. As expected, the resilience loss increases with Δτ, illustrated by the larger area under the curves in Figure 5. The resilience loss is for (P.1) calculated to be €3852, €3181 and €2889 with Δτ=4 h, Δτ=2 h and Δτ=1 h, respectively, and for (P.3) €2510, €1255 and €627 with Δτ=4 h, Δτ=2 h and Δτ=1 h, respectively [55].

Discussion and Conclusions

This paper presents three different operational models for wireless networks in the presence of a coordinated jamming attack. We model the decision-making of a network operator that tries to optimise the network operation so as to minimise the resilience loss in the event of such a disruption. Optimisation results are presented for a hypothetical wireless network where results from models (P.1) and (P.3) are compared. In the former model, the operator only regulates the traffic flow in the network and in the latter, she regulates the traffic flow and is also allowed to search for and neutralise a finite number of jammers from one decision time to the next. Comparing results from these models, we observe that searching for the jammers naturally yields a lower resilience loss than without searches. Next, we analyse the effect of the search time on the resilience loss in the operational model with search teams and a finite search time, (P.3), where search times are equal to one time step. We observe that the resilience loss increases with the time step duration, i.e. search time. These estimates may prove useful when deciding how to tune the time step duration. If the time step is too large, the resilience loss may be unacceptable and if the time step is too small, the operator has to optimise the network operation more frequently which may be expensive in a real scenario.

Since the operator does not know the jammer battery times, she makes decisions myopically and neutralises the jammer which increases the operational cost per unit of time the most (and not the resilience loss). In the example, jammer 2 increases the operational cost per unit of time the most and she therefore neutralises it first. However, jammer 1 has a longer battery time and may inflict a higher resilience loss than jammer 2, particularly for longer time steps. This illustrates how the operator's lack of perfect information can lead to poor decision-making.

A limitation of the present type of model is that it requires a large amount of data. Data on the jammer parameters, estimating search times and how the jammer interference a effects the maximum receivable data rate at the WAPs are examples of uncertain parameters in a realistic scenario which may have to be, in many cases, roughly estimated.

One simplification of the present model is that searches do not cost anything. In practice, costs may also be inflicted on the operator when changing the mode of operation due to additional labour, delays, etc. These costs may be added straight forwardly to the objective function in the operator model. Another possibility would be to enforce a budget constraint on the search of jammers, W. The constraint on the maximum number of jammers that can be found at each time step k would then be replaced by:

$$\sum_{j\in J} w_j\left(X_j^k - x_j^k\right) \leq W, \tag{9}$$

where w_j is the cost of finding jammer j.

Another generalisation of the model would be to allow the search time to be a multiple of the time step length. Furthermore, conditions affecting the operational cost per unit of time may change between decision times, e.g. penalty costs of blocked traffic increase as the time of unmet demand increases. Therefore, the objective function could be modified such that penalty costs are increasing functions of the amount of blocked per time unit instead of insufficient traffic capacity. A further expansion of the model is to allow the vertices to be mobile as in a Mobile ad hoc network (MANET) or a vehicular ad hoc network (VANET), which are becoming more on demand and are important for autonomous vehicles [56,57].

In this article, the focus has been on the choices of the operator. The objective of an attacker is generally to deploy his jammers at locations so as to cause the highest possible resilience loss. Therefore, the attacker's problem, also generally known as the wireless network jamming problem, may be included in the model to solve the Nash equilibrium for different attacker and defender resource budget limitations.

To further develop and increase the realism of the attacker model, one could allow the attacker to turn the jammers on and o at different times so as to deceive the operator and further maximise the total resilience loss. In addition, jammers in this study were assumed isotropic. Jammer directivity may be added straightforwardly as a parameter and the beam angle added as an attacker decision variable.

References

1. Woods DD (2006) Resilience Engineering: Redefining the Culture of Safety and Risk Management. Human Factors and Ergonomics Society 49.
2. Dekker S, Hollnagel E, Woods D, Cook R (2008) Resilience Engineering: New directions for measuring and maintaining safety in complex systems. Lundy University School of Aviation.
3. Brown GG, Carlyle WM, Salmeron J, Wood K (2005) Analyzing the Vulnerability of Critical Infrastructure to Attack and Planning Defenses. Informs, Tutorials in Operations Research.
4. Taormina R, Galelli S, Tippenhauer NO, Salomons E, Ostfeld A (2017) Characterizing Cyber-Physical Attacks on Water Distribution Systems. J Water Res Plan Man 143.
5. Salmeron J, Wood K, Baldick R (2004) Analysis of Electric Grid Security Under Terrorist Threat. IEEE Transactions on Power Systems 19: 905-912.
6. Donde V, Lopez V, Lesieutre B, Pinar A, Yang C, et al. (2005) Identification of Severe Multiple Contingencies in Electric Power Networks. Proceedings of the 37th Annual North American Power Symposium.
7. Holmgren AJ, Jenelius E, Westin J (2006) Optimal Defense of Electric Power Networks against Antagonistic Attacks. IEEE Transactions on Power Systems. International Electro technical Commission, EC. Electromagnetic compatibility (EMC)-Part 2-13: Environment - High-power electromagnetic (HPEM) environments -radiated and conducted, 2003.
8. Radasky W, Savage E (2010) Intentional Electromagnetic Interference (IEMI) and Its Impact on theU.S. Power Grid. Metatech Corporation pp: 1-53.
9. Gummadi R, Wetherall D, Greenstein B, Seshan S (2007) Understanding and Mitigating the Impact of RF Interference on 802.11 Networks 37: 385-396.
10. Armstrong K (2013) Cost-effectively managing Functional Safety and other risks which could be caused by electromagnetic disturbances. IEEE International Symposium on Electromagnetic Compatibility (EMC).
11. Backstrom MG, Lovstrand KG (2004) Susceptibility of Electronic Systems to High-Power Microwaves: Summary of Test Experience. IEEE Transactions on Electromagnetic Compatibility 46: 396-403.
12. Metzger F (2011) Failure Modes of Electronics. The English Press.
13. Kappenman J (2010) Geomagnetic Storms and Their Impacts on the U.S. Power Grid Metatech.
14. Systems Control Inc. Impact Assessment of the 1977 New York Blackout. Energy Systems Division, 1978.
15. Eaton (2013) National Centre of Excellence for Aviation Operations Research 2010.
16. Collier ZA, Lambert JH (2018) Time Management of Infrastructure Recovery Schedules by Anticipation and Valuation of Disruptions. Journal of Risk and Uncertainty in Engineering Systems, Part A: Civil Engineering 4.
17. Anderson R (2001) Security Engineering-A Guide to Building Dependable Distributed Systems. Wiley.
18. Goldsmith A (2005) Wireless Communications. Cambridge University Press.
19. Suwart J (2008) Wireless Ad Hoc Networks: Limitations, Applications and Challenges. Project Thesisat Technische Universitat at Braunschweig, Institute of Operating Systems and ComputerNetworks (IBR).
20. ZigBee (2007) Standards Organization. ZigBee Specification. ZigBee Alliance Board of Directors.
21. Frodigh M, Johansson P, Larsson P (2000) Wireless ad hoc networking-The art of networking without a network. Ericsson Review No. 4 pp: 1-16.
22. Gorenc B (2016) Understanding the Attack Surface for Critical Infrastructure.
23. Genender E, Garbe H, Sabath F (2014) Probabilistic Risk Analysis Technique of Intentional Electromagnetic Interference at System Level. IEEE, Transactions on electromagnetic compatibility 56: 200-207.
24. Oakes BD, Mattsson L, Nasman P, Glazunov AA (2018) A Systems-Based Risk Assessment Framework for Intentional Electromagnetic Interference (IEMI) on Critical Infrastructures. Risk Analysis 38: 1279-1305.
25. Kohlberg I (2005) Random Graphs and Percolation Theory Applied to Survivability of Ad-Hoc Wireless Communication and Sensor Networks. EMC Aspects Dealing with Safety, Reliability,and Security in the Domains of Transportation and Data Communications, 14-15, Paris, France, 2007.
26. Tague P, Slater D, Poovendran R, Noubir G (2008) Linear Programming Models for Jamming Attackson Network Traffic Flows. Mobile, Ad Hoc and Wireless Networks and Workshops.
27. Alderson LD, Brown GG, Carlyle WM (2015) Operational Models of Infrastructure Resilience. Risk Analysis 35: 562-586.
28. Landegren F, Sulaman SM, Moller P, Host M, Johansson J (2016) A method for assessing resilience of socio-technical IT-systems. European Safety and Reliability Conference, pp: 2199-2206.
29. Rathi N, Saraswat J, Bhattacharya PP (2012) A Review on Routing Protocols for Application in Wireless Sensor Networks. International Journal of Distributed and Parallel Systems (IJDPS) Vol. 3.
30. Verdu S (1990) On Channel Capacity per Unit Cost. IEEE Transactions on Information Theory 36: 1090-1030.
31. Ponemon Institute (2016) Cost of Data Center Outages. Data Center Performance Benchmark Series.
32. Stavroulakis P (2003) Reliability, Survivability and Quality of Large Scale Telecommunication. John Wiley & Sons Ltd.
33. Yodo N, Wang P (2016) Engineering Resilience Quantification and System Design Implications: ALiterature Survey. Journal of Mechanical Design, Vol. 138.
34. Ayyub BM (2015) Practical Resilience Metrics for Planning, Design, and Decision Making. Journal of Risk and Uncertainty in Engineering Systems, Part A: Civil Engineering 1: 1-11.
35. Heddebaut M, Deniau V, Rioult J, Copin G (2015) Method for detecting jamming signals superimposed on a radio communication, Application to the surveillance of railway environments. IEEE International Symposium on Electromagnetic Compatibility (EMC).
36. Jenelius E, Mattsson (2012) L-G. Road Network Vulnerability Analysis of area-covering disruptions:A grid-based approach with case study. Transportation Research Part A 46: 746-760.
37. Mattsson LG, Jenelius E (2015) Vulnerability and resilience of transport systems-A discussion of recent research. Transportation Research Part A 81: 16-34.
38. Agarwal P, Efrat A, Ganjugunte S, Hay D, Sankararaman S, et al. (2010) The Resilience of WDM Networks to Probabilistic Geographical Failures. EE Technical Report, Colombia University 21: 1525-1538.
39. Strasser M, Danev B, Capkun S (2009) Detection of Reactive Jamming in Sensor Networks. ETHZurich D-INFK Technical Report 634: 1-14.
40. Kha HH, Tuan HD, Nguyen HH (2012) Fast Global Optimal Power Allocation in Wireless Networks by Local D.C. Programming. IEEE Transactions on Wireless Communications 11: 510-515.
41. Commander CW, Pardalos PM, Ryabchenko V, Uryasev S, Zrazhevsky G (2007) The wireless network jamming problem. Springer Science+Business Media, LLC 14: 481-498.
42. Slater D, Tague P, Poovendran R, Li M (2009) A Game-Theoretic Framework for Jamming Attacks and Mitigation in Commercial Aircraft Wireless Networks. American Institute of Aeronautics and Astronautics.
43. Lazos L, Liu S, Krunz M (2009) Mitigating Control-Channel Jamming Attacks in Multi-channel AdHoc Networks. WiSec'09, March 16-18, Zurich, Switzerland, pp: 169-180.
44. Revelle C, McGarity AE (1997) Design and Operation of Civil and Environmental Engineering Systems. John Wiley & Sons, inc
45. Tse D, Viswanath P (2005) Fundamentals of Wireless Communication. Cambridge University Press.
46. Balanis CA (2016) Antenna Theory, Analysis and Design. Fouth Edition. John Wiley & Sons Inc.
47. Jackson D (1999) Classical Electrodynamics.
48. Bruneau M, Chang SE, Eguchi RT, Lee GC , O'Rourke TD, et al. (2004) A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities. World Conference on Earthquake Engineering 19: 733-752.
49. Eaton (2013) Blackout tracker. Power Outage Annual Report pp: 1-71.

50. Florwick J, Whiteaker J, Amrod AC, Woodhams J (2013) Wireless LAN Design Guide for High Density Client Environments in Higher Education. Cisco.

51. International Telecommunication Union (ITU), International Teletrac Engineering Handbook. Geneva, 2005.

52. Mansson D, Thottappillil R, Nilsson T, Lunden O, Backstrom M (2008) Susceptibility of Civilian GPS Receivers to Electromagnetic Radiation. IEEE Transactions on Electromagnetic Compatibility 50: 434-437.

53. The National Center of Excellence for Aviation Operations Research. Total Delay ImpactStudy, A Comprehensive Assessment of the Costs and Impacts of Flight Delay in the United States. NEXTOR, Final Report, 2010.

54. Shen W, Ning P, He X, Dai H (2013) Ally Friendly Jamming: How to Jam Your Enemy and Maintain Your Own Wireless Connectivity at the Same Time. Proceedings of the IEEE Symposium on Security and Privacy Pages 13: 174-188.

55. START. Terrorism in Belgium and Western Europe; Attacks against Transportation Targets; Coordinated Terrorist Attacks. National Consortium for the Study of Terrorism and Responses to Terrorism, 2016.

56. Bellur BR, Lewis MG, Templin FL (2002) An Ad-hoc Network for Teams of Autonomous Vehicles. United States Office of Naval Research (ONR) pp: 1-6.

57. Bhattacharjee PK, Pal RK (2011) Vehicular Ad Hoc Network in Mobile Communications with Diff-erent Routing Protocols. Assam University Journal of Science & Technology, Physical Sciences and Technology 7.