15. Ilmenauer TK-Manager Workshop
Technische Universität Ilmenau, 17. Mai 2019
DOI: 10.22032/dbt.38489
URN: urn:nbn:de:gbv:ilm1-2019200270

Schnell einsetzbares, vermaschtes Weitverkehrsfunknetz

von Matthias Aumüller

Matthias Aumüller erwarb 2017 seinen Master in Informatik an der Technischen Universität Ilmenau. Seitdem ist er als Wissenschaftlicher Mittarbeiter im Fachgebiet Kommunikationsnetze tätig. Zusätzlich arbeitet Herr Aumüller seit 2009 als Anwendungsentwickler im Bereich Rich Internet Applications. Ehrenamtlich ist er als stellvertretender Ortsverbandsvorsitzender im Amateurfunk tätig. Schon seit seiner Jugend beschäftigt sich Matthias Aumüller mit den Themengebieten IT, Netzwerken und Elektronik, was er durch sein Studium und seine Forschung im Bereich vermaschte Notfallnetzwerke vertiefen möchte.

DOI: 10.22032/dbt.38497

Motivation

Digitale Kommunikation spielt in Zeiten von Industrie 4.0, bedarfssynchroner Produktion (Just-in-time-Produktion), Instant-Messaging und digitaler Katastrophen-Warndienste im Alltag, aber auch in Ausnahmesituationen eine essenzielle Rolle. So werden viele Abläufe im täglichen Leben, in der Industrie sowie bei der Katastrophenhilfe durch digitale Kommunikation erleichtert oder sind sogar auf sie angewiesen.

Leider kann sich auf das Vorhandensein eines digitalen Kommunikationsmediums wie das Internet nicht immer verlassen werden. So

kam es in der Vergangenheit immer wieder zu Ausfällen, was sich vermutlich auch in der Zukunft wiederholen wird.

Für den Ausfall von Kommunikationseinrichtungen und Netzen kann es verschiedene Ursachen geben, welche im Folgenden vorgestellt werden sollen.

Wie der Energie- oder der Gesundheitssektor gehört auch die Informationstechnik und Telekommunikation zu der kritischen Infrastruktur eines Landes, durch deren Sabotage ein Land extrem geschwächt werden kann.

Militärische oder terroristische Angriffe auf die Energie- und Kommunikations-infrastruktur werden ernst genommen. So gibt es zum Beispiel seit 2001 eine *Kommission zur Bewertung der Bedrohung von elektromagnetischen Impulsangriffen auf die Vereinigten Staaten*[1].

Diese Kommission beschäftigt sich mit dem möglichen Angriff durch einen HEMP oder NEMP, bei dem durch eine in der mittleren oder oberen Atmosphäre gezündete Nuklearexplosion ein elektromagnetischer Puls ausgelöst wird. Je nach Höhe breitet dieser sich mehrere hunderte Kilometer aus und zerstört alle elektrischen Geräte in diesem Umkreis; inklusive der Kommunikationsinfrastruktur.

Neben den physikalischen Angriffen auf die Telekommunikationsinfrastruktur gibt es auch Angriffe, die das digitale Medium selbst als Angriffsvektor nutzen. Durch Internetkriminalität und den sogenannten „Cyberkrieg“ wurden bereits zahlreiche Ausfälle hervorgerufen.

Bereits 1997 drang ein vermutlich jugendlicher Angreifer in die Systeme des Flughafens von Worcester ein. Hierdurch wurde ein sechsstündiger Ausfall der Kommunikationssysteme verursacht. Als Vergeltungsschlag für die Luftangriffe der NATO auf den Kosovo und Serbien im Jahre 2000 griff Jugoslawien die NATO und die US-Navy Kommunikationsinfrastruktur an, welche dadurch für mehrere Tage lahmgelegt wurde.

Weitere Angriffe auf Konmmunikationsinfrastruktur gab es 2007 auf Estland (1-10 Stunden), 2008 auf Georgien und 2009 auf Kirgisistan (10 Tage), bei denen zahlreiche Systeme überlastet wurden, teilweise bis zum Totalausfall

[1] http://www.empcommission.org/

(Rege-Patwardhan, Cybercrimes against critical infrastructures: a study of online criminal organization and techniques, 2009).

Die Sorge vor Spionage und die „gezielte Störungen der Netze“ (Voelsen, 2019) sind bereits in der Politik Deutschlands verankert. So wird darüber diskutiert ob die Verwendung von Infrastrukturkomponenten der chinesischen Firma Huawei beim Mobilfunknetzausbau untersagt werden soll (Voelsen, 2019), da ein eingebauter Killswitch vermutet wird. Ähnliches gilt für die us-amerikanische Firma Cisco, welche bereits Spionage im Auftrag des Herkunftslandes betrieben hat.

Neben den Ausfällen durch Angriffe kommt es auch immer wieder durch technisches Versagen zu Netzausfällen. Dies kann beispielsweise durch Hardwareausfälle wie bei dem Ausfall eines zentralen Switches bei Lambdanet 2005 geschehen. Aufgrund dessen waren für 10 Stunden 250000 Domains des Webhosters all-inkl.com nicht erreichbar (Wilde, 2005) (BSI, 2018).

Ferner führen auch Software- und Konfigurationsprobleme häufig zu längeren Ausfällen.

Eine Softwarestörung wurde durch ein abgelaufenes Zertifikat im Dezember 2018 ausgelöst. Hierdurch verweigerte eine Software von Ericsson für Kernnetzkomponenten im Mobilfunknetz ihren Dienst. Der Ausfall wirkte sich auf Mobilfunknetze in verschiedenen Ländern aus. Unter anderem war das O2 Netz in Großbritannien betroffen, durch dessen Ausfall 30 Millionen Mobilfunkkunden zwei Tage vom Internet abgeschnitten waren (Ericsson, 2019) (Briegleb, 2018).

Oft zu Ausfällen kommt es auch aufgrund der immer stärker werdenden Abhängigkeit zum Stromnetz. Bei vielen Kommunikationseinrichtungen reicht die Notstromversorgung nur noch für wenige Stunden. Dies zeigt der Stromausfall aufgrund von Tiefbauarbeiten in Berlin Köpenik, bei dem am 19.02.2019 nach dem Ausfall des Stromnetzes auch Teile des Telefonnetzes sowie die Mobilfunkstationen ausfielen (DARC, 2019) (Schönball, 2019).

Auch Missmanagement und fehlende Wartung von Infrastrukturkomponenten können zum Ausfall dieser führen. Dies gilt sowohl für Kommunikations- als auch für Energienetze. Auf eine marode Infrastruktur, so wird vermutet, sind

etwa die häufigen Stromausfälle in Südafrika zurückzuführen. Hierdurch kommt es des Öfteren zu geplanten sowie ungeplanten Blackouts (Drechsler, 2019).

Noch schlimmer stellt sich die Situation in Venezuela dar. Dort kam es aus ähnlichen Gründen für knapp eine Woche zum Netzausfall (tagesschau.de, 2019) (AFX, 2019).

Zu zahlreichen, aber meist kleineren Ausfällen kommt es auch immer wieder durch das Zutun von Tieren. Diese können zum Beispiel dadurch hervorgerufen werden, dass Tiere wie Vögel oder Eichhörnchen mit ihrem Körper Kurzschlüsse verursachen. Aber auch die Einlagerung von Nahrung oder das Bauen von Nestern in zur Lüftung vorgesehenen Aussparungen führte schon zu verschiedenen Ausfällen (Cyber Squirrel, 2019).

Besonders verheerend auf die Infrastruktur und die Bevölkerung können sich auch extreme Wetterereignisse auswirken. So löste 2011 ein Tsunami eine Überschwemmung und Nuklearkatastrophe an der Ostküste Japans aus. Insgesamt fielen 14000 Basisstationen aus (Kulas, Kunde, & Hinsch, 2013).

Innerhalb Europas besteht eine Meldepflicht (Gesetz über den Amateurfunk (Amateurfunkgesetz - AFuG 1997), 1997, S. §3 Art. 13a) für signifikante Störungen und Sicherheitsvorfälle in Kommunikationsnetzen. Diese müssen über eine lokale Regulierungsbehörde, in Deutschland die Bundesnetzagentur und das BSI, an die ENISA gemeldet werden.

Im Jahre 2017 haben die 28 EU-Lander sowie zwei EFTA Staaten insgesamt 169 Zwischenfälle gemeldet. Verursacht wurde diese Vorfälle durch Systemfehler (60.1 %), menschliches Versagen (18.3 %), Naturereignisse (17.2 %) und böswillige Handlungen (2.4 %) (ENISA, 2018). Hierbei sei angemerkt, dass Fehler, die durch Tiere ausgelöst wurden zu Naturereignissen zählen (Dekker, Karsberg, Mattioli, & Levy-Bencheton, 2015).

Für Firmen können Ausfälle der Kommunikationsinfrastruktur verheerende, existenzbedrohende Folgen haben. Im Rahmen des Business Continuity Management werden Pläne erarbeitet, um die wichtigsten Geschäftsprozesse am Laufen zu halten. Zum aufrecht erhalten der Kommunikation mit

Zweigstellen oder wichtigen Zulieferern können Weitverkehrsfunknetzwerke aufgebaut werden.

In Katastrophensituationen werden in allen betroffenen Landratsämtern in Deutschland Leitstellen eingerichtet. Um eine digitale Kommunikation zwischen diesen Leitstellen auch bei einem Ausfall des Internets zu ermöglichen können Weitverkehrsfunknetzwerke in Betracht gezogen werden.

Bei großflächigen Katastrophen können verschiedene Leitstellen von unterschiedlichen Hilfsorganisationen miteinander verbunden werden. Hierdurch können Organisationsübergreifend Daten ausgetauscht werden.

Die betroffene Bevölkerung kann miteinander vernetzt werden, um vermisste Personen zu finden, mit Angehörigen zu kommunizieren oder wichtige Güter wie Medizin oder Lebensmittel zu bestellen.

Eine solche Infrastruktur könnte auch dazu genutzt werden Sensordaten, die in einem Katastrophengebiet gesammelt werden, zu übermitteln. Denkbar wären hier jegliche Sensordaten wie Temperaturen, Wärmebilder (z.B. bei Brandgefahr), Wasserstände bei Überschwemmungen oder Strahlungswerte.

Aufgabenstellung und Zielsetzung

Um den Problemen, die durch den Ausfall eines Kommunikationssystems entstehen, entgegenzuwirken, entsteht ein neues Kommunikationsnetz. Betrieben wird das Netzwerk vornehmlich durch Funkamateure, denn eine Hauptaufgabe des Amateurfunks ist der Notfunk (Gesetz über den Amateurfunk (Amateurfunkgesetz - AFuG 1997), 1997, p. §2 Abs. 1). Zudem besteht bei Funkamateuren bereits ein breites Wissen und großes Interesse bezüglich der betreffenden Vorschriften, Betriebstechnik und Hochfrequenztechnik. Wissensfelder wie IT und Netzwerktechnik drängen sich auch immer mehr in den Amateurfunk.

Um die Kosten möglichst gering zu halten und die Technik schnell einsetzen zu können werden bereits vorhandene Technologien verwendet. Besonders bei der Hardware werden wenn möglich Geräte, die sich bereits im Amateurfunk etabliert haben, eingesetzt. Weitere Vorteile, die für die Zusammenarbeit mit Funkamateuren sprechen, sind das Vorhandensein von Lizenzen für

zusätzliche Frequenzbänder, die Erlaubnis mit stärkerer Leistung zu senden und der vorhandene Kontakt mit den zuständigen Behörden wie den bereits erwähnten Landratsämtern.

Ziel ist es ein Kommunikationssystem zu schaffen welches sich binnen weniger Tage aufbauen lässt. Die Software lässt sich in wenigen Minuten installieren, die Einstellungen erfolgen möglichst automatisch und benutzerfreundlich. Eine vermaschte Netzwerkstruktur ermöglicht hohe Bitraten und Redundanz.

Das so aufgebaute Netzwerk bietet die Möglichkeit zu telefonieren sowie Text- und Multimedianachrichten austauschen. Es überträgt alle Formen von Daten wie Bilder oder Videos. Das System kann mit anderen Netzwerken verbunden werden. Zudem ist es möglich, weitere beliebige Dienste zu hosten. Ein besonderes Augenmerk wird hierbei auf die möglichst sparsame Ausnutzung der Links gelegt.

Vorgehensweise

Um Grundlagen zu schaffen werden verschiedene Kommunikationsnetze untersucht. Besonders im Fokus stehen von Funkamateuren in Deutschland, aber auch in der ganzen Welt betriebene Weitverkehrsfunknetze und drahtlose Zugangstechnologien. Es werden aber auch andere den Anforderungen entsprechende Netze untersucht.

Hierzu gehören die auf IEEE802.11 basierenden, von Funkamateuren betriebenen Netze HAMNET, AREDN[2], HamWAN[3] und Mi6WAN[4]. Als Zugangstechnologien werden neben IEEE802.11 auch DMR, D-Star, Packet Radio und weitere Amateurfunk-Betriebsarten untersucht.

Neben den Amateurfunk-Netzwerken gibt es zahlreiche vermaschte Netze, die hauptsächlich zur Bereitstellung von Internet dienen. Durch ihre große Entwicklergemeinschaft besitzen sie ein großes Software-Portfolio und zahlreiche interessante Eigenschaften, die man sich für ein neu geplantes Netz

[2] https://www.arednmesh.org/
[3] https://hamwan.org/
[4] https://w8cmn.net/mi6wan/

zu Nutze machen kann. Hierzu zählen die Freifunk-Netze[5] mit zahlreichen lokalen Gruppierungen in Deutschland, guifi.net[6] aus Spanien und das qMp[7].

Auch betrachtet werden die mehr unter wissenschaftlichem Fokus stehenden Funknetze WiLDNet (Patra, et al., 2007), Roofnet (Aguayo, et al., 2003) und LifeNet (Mehendale, Paranjpe, & Vempala, 2011).

Um zu identifizieren, welche Ansätze in das geplante Netzwerk übernommen werden sollen, müssen diese miteinander verglichen und für das Szenario optimiert werden. Um den finanziellen Aufwand gering zu halten, aber die Tests in einem möglichst großen Netzwerk durchführen zu können, soll dies größtenteils emuliert werden.

Zur möglichst frühzeitigen Erkennung von Problemen, zum Beispiel mit spezieller Hardware, werden einzelne Geräte mit in das emulierte Netzwerk eingebunden. Zur Emulation des Netzwerkes wird Mininet verwendet. Mininet bietet über eine Python API komfortabel Zugriff auf Funktionen des Linux-Kernel, mit denen sich ein virtuelles Netzwerk mit voneinander isolierten Knoten erzeugen lässt. Dass sich Mininet auch zur Emulation von größeren Netzwerken eignet zeigte ein Student in einem Resarch Project (Mohsin Khan, 2018).

Zur Erzeugung eins realitätsnahen Szenarios wurde die Topologie des HAMNETS aus der Monitoring- und Verwaltungsdatenbank HAMNET-Database[8] exportiert und als virtuelles Netzwerk nachgebildet. Um die Linkeigenschaften realitätsnah zu gestalten wurde von allen über SNMP erreichbaren HAMNET-Knoten ein Abzug erstellt, um per Data-Mining Gesetzmäßigkeiten und Regeln zu extrahieren.

Um auch zeitliche Verläufe und Trends zu erkennen entsteht gerade im Rahmen einer Masterarbeit ein Monitoring System, was zukünftig einige Knoten des HAMNET sowie das neu entstehende Netzwerk überwachen soll.

In der Absicht die entstehende Architektur in verschiedenen Szenarien und unterschiedlichen Netzwerke testen zu können wurde von einem Student ein

[5] https://freifunk.net/
[6] https://guifi.net/
[7] https://qmp.cat/
[8] https://hamnetdb.net/

Topologiegenerator implementiert, welcher es ermöglicht Mesh-Netze mit unterschiedlichen Eigenschaften in Mininet zu erzeugen (Demirocak, 2019).

Eine zentrale Problemstellung in Mesh-Netzwerken ist das Routing. Zum Vergleich verschiedener Routing-Dienste in einer vorher in Mininet generierten Netzwerktopologie wurde die Erstellung der Konfigurationsdateien und das Starten der Dienste durch Verwendung eines Templatesystems automatisiert. Hierdurch ist es bereits möglich die Dienste „olsrd“ mit dem Routingprotokoll „olsr“, „babeld“ mit „babel“ sowie „bird“ mit den Protokollen „babel“ und „bgp“ zu konfigurieren und zu starten. Weitere Dienste wie „oonf“(olsr2) und „batman-adv“ sowie zusätzliche von „bird“ unterstützte Protokolle sind bereits in Arbeit.

Um die Protokolle direkt vergleichen zu können müssen Metriken ermittelt werden. Einige Metriken wurden in zwei Stundentenprojekten identifiziert, bei denen exemplarisch jeweils zwei Routingprotokolle miteinander verglichen und Messungen zum Durchsatz, Paketverlust, Delay (Gegolli, 2018) und erzeugtes Verkehrsaufkommen (Demirocak, 2019) durchgeführt wurden. Diese Messmethoden sollen weiter verbessert, automatisiert und auf andere Szenarien übertragbar gemacht werden. Zusätzlich sollen noch Metriken wie die Konvergenzzeit ergänzt werden.

Diese Messungen sind weitestgehend automatisiert, um bei Änderungen den Diensten oder ihrer Konfiguration eine Continuos Integration zu ermöglichen.

Parallel zu den Routing Protokollen ist auch eine Möglichkeit zum Evaluieren von Transportprotokollen entstanden. In einem Studentprojekt mit Mininet sind Methoden zur Messung verschiedener Eigenschaften von verlässlichen Transportprotokollen entstanden. Hierzu zählen „time to first byte“ und Durchsatz (Fejza, 2019). Auch diese Methodik wird weiter verbessert und in das Gesamtkonzept integriert.

Um generell die Last auf das Netzwerk zu verringern und dadurch die Dienstgüte für Services die, nicht auf das Netzwerk verzichten können, zu verbessern wird an einem Dienste-Scheduler gearbeitet, der die Services möglichst nah am Verbraucher platziert.

Um den so gestarteten Diensten auch Zugriff auf eine Datenbank zu ermöglichen wurden im Rahmen eines Studentenprojektes verschiedene, verteilte Datenbanken im Hinblick auf den Einsatz in Mesh-Netzwerken untersucht (Solangi, 2019).

Bevor einzelne Dienste gestartet werden können muss die aktuelle Version der Software an alle infrage kommenden Serverknoten verteilt werden. Hierfür wurden bereits von einem Studenten in einer Recherchearbeit infrage kommende Protokolle ermittelt (Chruscz, 2019). Von einem weiteren Studenten wurden Wege zur Datenübertragung getestet, welche den Einfluss auf andere Übertragungen möglichst gering halten (Mohsin Khan, 2019).

Zur ständigen Überwachung der Dienste, Links und Sensoren entsteht ein universelles Monitoring. Einige Ansätze mit verschiedenen Systemen wie Icinga2 und Prometheus werden im Moment im Rahmen einer Masterarbeit auf ihre Tauglichkeit untersucht.

Parallel dazu wurde bereits ein weiterer Ansatz des Monitorings getestet. Dieser besteht aus drei in JavaScript implementierten Microservices. Ein Microservice fragt den Knotenzustand über snmp ab und schickt diese Informationen gesammelt an einen zentralen Dienst weiter, welcher die Werte in die Streamdatenbank RethingDB schreibt. Ein dritter Dienst stellt eine API für Webclients bereit, hierüber lassen sich die Datenströme abonnieren und per Websocket an den Webbrowser weiterleiten, in dem sie dann live angezeigt werden.

Zur Realisierung von Kommunikationswegen über verschiedene Adressierungsarten (Anycast, Broadcast, Multicast, Geocast) muss eine Middleware etabliert werden. Die dafür benötigte Infrastruktur wird im Rahmen eines Praktikums in Zusammenarbeit mit einem Studenten geschaffen und soll anschließend in einer Masterarbeit weiter verfeinert werden.

Getestet werden soll dieses System auch auf reeller Hardware. Dazu wurde auf der Grundlage eines Studentenprojektes ein Testbed-Provisionierungssystem aufgebaut. Dieses ermöglicht es Single-Board-Computer über das Netzwerk mit einem beliebigen Betriebssystem zu starten.

In Zukunft müssen die noch separierten Systeme in eines Integriert werden. Für einen reibungslosen Einsatz muss die prototypisch in Studentenprojekten entstandene Software refactored bzw. neu geschrieben werden. Erst dann kann das System komplett vermessen und zur bestmöglichen Erfüllung der Anforderungen optimiert werden.

Abkürzungen

AREDN.	*Amateur Radio Emergency Data Network*
BSI.	*Bundesamt für Sicherheit in der Informationstechnik*
EFTA.	*Europäische Freihandelsassoziation*
ENISA.	E*uropäische Agentur für Netz- und Informationssicherheit*
HAMNET.	*Highspeed Amateurradio Multimedia NETwork*
HEMP.	*High-Altitude Electromagnetic Pulse*
NEMP.	*Nuclear Electromagnetic Pulse*
qMp.	*Quick Mesh Project*
WiLDNet.	*WiFi Based Long Distance Network*

Literaturverzeichnis

AFX, d. (Mar 2019). Venezuela: Tote und Plünderungen – So fatal war der Stromausfall. t-online.de. Von https://www.t-online.de/nachrichten/ausland/krisen/id_85403846/venezuela-tote-und-pluenderungen-so-fatal-war-der-stromausfall.html abgerufen

Aguayo, D., Bicket, J., Biswas, S., Morris, R., Chambers, B., & De Couto, D. (2003). MIT roofnet. *Proceedings of the International Conference on Mobile Computing and Networking.*

Briegleb, V. (11. 12 2018). *Ericsson-Hardware: Abgelaufenes Zertifikat führte zu Netzausfällen.* Von heise online: https://heise.de/-4248148 abgerufen

BSI. (2018). Von https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g01/g01010.html abgerufen

Chruscz, N. P. (2019). Verteilung von Software und Daten in drahtlosen, vermaschten Weitverkehrsnetzen.

Cyber Squirrel, 1. (2019). CyberSquirrel1.com. Von https://cybersquirrel1.com/ abgerufen

DARC. (Feb 2019). Blackout in Berlin dauerte mehr als 24 Stunden. DARC e.V. Von https://www.darc.de/der-club/distrikte/i/ortsverbaende/19/nachrichten/detailansicht-archiv/news/blackout-in-berlin-dauerte-mehr-als-24-stunden/ abgerufen

Dekker, D. M., Karsberg, C., Mattioli, R., & Levy-Bencheton, C. (2015). Guideline for Threats and Assets. Von https://resilience.enisa.europa.eu/article-13/guideline_on_threats_and_assets abgerufen

Demirocak, K. (2019). Evaluation of Ad-Hoc Routing Protocols in Wireless Wide Area Networks.

Drechsler, W. (Mar 2019). Weltgeschichte: Stromausfälle legen Südafrika lahm. Handelsblatt GmbH. Von https://www.handelsblatt.com/politik/international/weltgeschichten/drechsler/weltgeschichte-stromausfaelle-legen-suedafrika-lahm/24117064.html?ticket=ST-241126-hsIasnzDMs6TbV3RXWJ5-ap2 abgerufen

ENISA. (Aug 2018). Annual report Telecom security incidents 2017. European Union Agency for Network and Information Security. Von https://www.enisa.europa.eu/publications/annual-report-telecom-security-incidents-2017 abgerufen

Ericsson. (2019). *Update on software issue impacting certain customers.* Von Ericsson: https://www.ericsson.com/en/press-releases/2018/12/update-on-software-issue-impacting-certain-customers abgerufen

Fejza, I. (2019). Evaluation of Reliable Transport Protocols in Wireless Wide Area Networks.

Gegolli, D. (2018). Comparison of OLSR and BATMAN Advanced with Mininet.

Gesetz über den Amateurfunk (Amateurfunkgesetz - AFuG 1997). (1997). Bundesministerium für Post und Telekommunikation, Referat 314.

Kulas, M., Kunde, A., & Hinsch, M. (Mar 2013). SAMMLUNG REALER AUSFÄLLE UND STÖRUNGEN VON KOMMUNIKATIONSNETZEN. Von https://www.informatik.uni-hamburg.de/TKRN/world/staff/kdh/tools/netzausfaelle/netzausfaelle.html abgerufen

Mehendale, H., Paranjpe, A., & Vempala, S. (2011). *Lifenet: a flexible ad hoc networking solution for transient environments* (Bd. 41). ACM.

Mohsin Khan, B. (2018). Evaluation of Performance and Scalability in Wireless Scenarios with Mininet.

Mohsin Khan, B. (2019). Distribution of Software and Data in Mesh Networks.

Patra, R. K., Nedevschi, S., Surana, S., Sheth, A., Subramanian, L., & Brewer, E. A. (2007). WiLDNet: Design and Implementation of High Performance WiFi Based Long Distance Networks. *NSDI*, *1*, S. 1.

Rege-Patwardhan, A. (2009). Cybercrimes against critical infrastructures: a study of online criminal organization and techniques. *Criminal Justice Studies, 22*, 261-271.

Schönball, R. (Feb 2019). Nicht alle Netzbetreiber auf Blackout vorbereitet. Von https://www.tagesspiegel.de/berlin/stromausfall-in-koepenick-nicht-alle-netzbetreiber-auf-blackout-vorbereitet/24019498.html abgerufen

Solangi, G. M. (2019). Analysis and Comparison of Distributed Databases in Mesh Networks.

tagesschau.de. (Mar 2019). Kuriose Schuldzuweisungen nach Stromausfall in Venezuela. Von https://www.tagesschau.de/ausland/venezuela-stromausfall-105.html abgerufen

Voelsen, D. (2019). 5G, Huawei und die Sicherheit unserer Kommunikationsnetze: Handlungsoptionen für die deutsche Politik. 8.

Wilde, M. (Oct 2005). Totalausfall beim Webhoster all-inkl.com [2. Update]. *heise online*. https://heise.de/-140588