Implementing Cyber Security tools and/or techniques in Local transportation system in Berlin – A Literature Review

The aim of this literature review is to explore what cyber security tools and techniques are implemented in the local transportation system of Berlin. A discussion of main similarities as well as differences in the literature analysed will be provided in the following. The target group of this literature review are people that want to know more about how much is written about cyber security tools and techniques in the Berlin transportation systems in scientific literature.

Local classical (subway, rail, bus etc.) as well as modern (carsharing apps, scooter rental apps, …) transportation systems have widely implemented or are built on information and communication technology (ICT) nowadays. Using ICT inevitably offers many attack vectors as well as a plethora of lucrative assets to hackers such as for example safety of passengers, private information of passengers and the need to rely on punctuality and availability of transportation systems. This widespread use of ICT and those valuable assets inevitably lead to the fact that malicious actors will try to exploit vulnerabilities for monetary gain. In 2017 for example Deutsche Bahn, responsible for Berlin`s suburban railway, was hit by a ransomware attack leading to failures in various systems, which caused massive delays for some passengers. (Graham, 2017) To further emphasise the importance of transportation systems it needs to be mentioned that the German government passed a law in 2016 that stated transportation systems is one of the few critical infrastructures that needs special protection. (Bundesministerium der Justiz, 2016). This clearly shows that cyber tools are necessary to defend critical infrastructure such as transportation systems from cyber-attacks.

This literature review focuses on scientific databases such as google scholar, IEEE Intelligent Transportation Systems Society and others. The literature review is done iteratively in various steps. At first relevant articles are scanned by reading the abstract and conclusion to get an overview of literature available to the topic. Then key articles are identified, and redundant or older articles are sorted out, to identify articles that provide a good and current understanding of the topic. Another great source to identify key literature is to scan through the references of an article that contributes to the topic. Sometimes you find very good other not yet identified literature within this reference section. Any issues with the literature e.g., major opposing views are also identified in this step to get a thorough understanding of the topic. To support the literature review a tool called Mendeley is used that helps to make notes, highlight important pieces, and supports the sorting of literature by relevance to my topic. Web browser plugins for transferring articles, books etc. including their metadata to Mendeley are also used to be time efficient.

Within the review of literature, it was identified that there is no one source that answers the research question. The topic must be divided into literature about classical transportation systems (TS) and modern interconnected and intelligent transport systems (ITS). To showcase literature about classical transport systems, it was identified that literature about railways is comprehensive enough to also represent other means of transportation like buses, since they are built in a very similar way.

A good starting point for classical transportation systems is “Cybersecurity for railways - A maturity model“ by Kour, Karim and Thaduri, 2020, since it lists all assets of modern day interconnected transportation systems. It also gives a good background because cyber security techniques are essential to have even for classical transportation systems nowadays. The article also provides data on the current state of cyber security on three railway companies. Two of three analysed real world rail companies had significant gaps within their cyber security. Some lacked essential capabilities such as providing appropriate Risk Management, Threat and Vulnerability Management as well as Event and incident response capabilities.

Another relevant piece of literature is “Cybersecurity-The Forgotten Issue in Railways'' by Valdivia *et al.*, 2018. This article points out that cybersecurity does not currently play an important role in

modern railways. Cyber Security is simply less important than safety and therefore as the authors claim simply forgotten to be taken care of. The article lists many reasons why this is the case. One being that within development the focus is solely on safety. Security is being added only at the end of the development, which makes security implemented poorly. Another reason as mentioned by the authors that hinders cyber security to be well implemented is the lack of standardisation within the railway industry. Currently there is no standard available that helps manufacturers to build elements of a modern-day interconnected railway system. There is just guidance available, which may or may not be followed by some.

The Cybersecurity in the Railway sector (CYRAIL) consortium is a group that was founded in 2015. The group is sponsored by the European Union and its goal is to specify measures and strategies to improve the overall cyber security posture of railways in Europe. (Cyrail Consortium Members, 2016). After working for several years, the CYRAIL consortium published in 2018 a book called "CYRAIL Recommendations on cybersecurity of rail signalling and communication systems". This book exactly provides improvement to the core issues that were identified by the two literature sources cited earlier in this literature review. The book is divided into several sections and primarily deals with cyber security tools and techniques the industry should deploy to improve cyber security in the rail sector. One section is dedicated to risk management. This section provides an approach for complex structured transportation systems by having a layered risk management approach, meaning that at first a high-level cyber security risk assessment (HLCRA) is conducted which will lead to finer granulated risk assessment in specific areas. But not only methods like risk management are mentioned, tools like Intrusion Detection Systems (IDS) are mentioned as key components for any transportation system to counter cyber-attacks. A large section is also dedicated to measures preventing risks. In this chapter detailed information is provided about encryption algorithms for example. Incident response which any transportation system provider should maintain is also well described. In this section human factors, detection strategies and technical solutions are discussed. This book listing many cyber security tools and nearly all techniques is completed by a chapter about a cyber resilience mechanism, that describes its four phases: anticipate, whit stand, recover & evolve in sufficient detail.

"eMaintenance in railways: Issues and challenges in cybersecurity" by Kour *et al.*2019 is an interesting article to mention, since CYRAIL provides a very comprehensive report on how to secure the railway sector. Nonetheless as complete as it is, it lacks to discuss supporting activities to railways like maintenance. CYRAIL only focuses on the core of railway operations. The article by Kour et al. however describes many of the cyber security challenges a railway company must face besides its main scope. A very god example to illustrate the lack, is the fact that maintenance in rail has due to the rise of IoT devices a very high number of sensors available. This data is fed to a huge database, where AI for example might detect anomalies in trains based on the vibration measured in tracks. This massive number of sensors and sensor data available and the fact that the data is used to guide safety relevant actions like maintenance is, leads to the fact that this is an asset to protect. The protection of those IoT assets is however very hard to do in a cost-effective way. Methods and measures must yet be designed to counter this problem. The authors suggest either training AI to neglect false positives of sensors or to build sensors in a way that they show when they are tampered with.

A bigger gap in literature is hard to identify with classical transportation systems since it is well covered by scientific literature. An analysis of opposing views in literature can also not be done, since most of the articles agree on main concepts such as that cyber security is not well implemented. Nonetheless there is a gap in literature since the literature only postulates cyber security methods and suggests certain cyber security tools. The literature does not cover the implementation of those tools and methods and its performance. This gap can be used to form a good research question for a dissertation. Additionally, it can be mentioned that beside the main scope of the topic still gaps exist

as shown with the lack in consideration of maintenance and its security. This could also be another very good research question.

Intelligent Transportation Systems (ITS) is the future of transportation systems. Within ITS advanced technologies combine the various ways of transportation like classical railway, busses, taxi but also modern ways of travelling like car sharing, scooter rental, carpooling, autonomous vehicles, etc. Since full ITS are not yet found in the real world, the academic literature is covering a lot of theoretical ideas about that topic.

Sedjelmaci, Hadji and Ansari, 2019 in "Cyber Security Game for Intelligent Transportation Systems" for example have modelled cyber security games to simulate modern transportation systems. They also implemented a security framework in each of the games to verify its effectiveness. As they could demonstrate this security framework, which mainly consists of an Intrusion Detection System (IDS), showed good results. As they stated they have however not yet investigated artificial intelligence (AI) driven IDS. But there is not only this gap, which could be further explored, there are also other cyber security tools and techniques like intrusion prevention systems (IPS) not yet considered here.

Sedjelmaci *et al.*, 2018 focus in their article "A Generic Cyber Defense Scheme Based on Stackelberg Game for Vehicular Network" on road vehicles, which is a subset of a complete ITS. They also only use one model to verify their theory. They however already deploy IDS and IPS in their simulation. Whilst this article now covers more cyber security tools and techniques, it however is limited in scope compared to the previous article. An obvious gap to further analyse would therefore be to deploy their thoughts on a complete ITS. Additionally Sedjelmaci *et al.*, 2018 have postulated the boundary condition of their system, that any security information must be relatively small to maintain the operability of an real world IDS with limited performance, since it would otherwise likely fail. Identification of further boundary conditions of the simulations currently available could also be a topic to explore on its own with a research question in a dissertation.

Haydari, Zhang and Chuah, 2021 shed light from a different angle on ITS within their article called "Adversarial Attacks and Defence in Deep Reinforcement Learning (DRL)-Based Traffic Signal Controllers", since they discuss cyber security within traffic signal systems. They also postulate that IDS is an effective way to counter cyber-attacks in the future for widespread and interconnected IoT networks, which smart traffic lights are. They also omit IPS as well as other cyber security tools in their article however. They also use game theory to model their research. This article contrasts with the other two mentioned, since it is discussing traffic lights not vehicles. It is however important to point out that the methodology is very similar to the other articles, since they are using similar models.

Literature on ITS does not provide major opposing theories. They all align in the fact that IDS is a must have tool to defend against cyber-attacks for example. Worth mentioning however is the fact that despite classical transportation systems the ITS is discussed mostly on a very theoretical early level. A good research question can easily be created when the topic is focused on ITS, since the gap in literature is wider than with classical transportation systems. But not only implementation of theories can be a good topic to choose here, similar as proposed with classical transportation systems, one could for example do a thesis based on surveys and interviews and narrow down on not yet answered questions.

The journal article from Mallah, López and Farooq, 2020 called "Cyber-Security Risk Assessment Framework for Blockchains in Smart Mobility" is neither bound to classical nor modern transportation systems. It rather introduces the idea of blockchain technology to improve the robustness of the network against intrusion. Blockchain technology could be able to defend against falsified or tampered information coming from a malicious node. This article shows that there are still gaps in cyber security tools and techniques for modern as well as classical transportation systems.

In conclusion it can be stated that the initial research question needs to be further broken down, since the topic is very broad. One could either focus on classical or modern transportation systems. To cover both aspects is impossible.

Conclusion

The literature analysed does not have major opposing views, since they align on most of the key points in general. They share very similar views on what tools to implement for example. They also agree on the importance of cyber security in transportation systems. Literature on classical transportation systems also aligns greatly on the fact that there is a lot to implement to be sufficiently secure.

Both topics modern as well as classical transportation systems would provide ideal chances to verify the theoretical information by coded simulations or in the case of classical transportation systems even with hardware simulations.

Scientific Information about transportation systems in Berlin is however non existing. The only reliable information can only be found in newspapers unfortunately. This is a very significant gap, which can be seen as a chance. One could also do a dissertation on the gap in literature about Berlin`s transportation system. Surveys and interviews seem to be a feasible way of dealing with this gap.

References

Bundesministerium der Justiz (2016) *BSI-KritisV - Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz*. Available at: https://www.gesetze-im-internet.de/bsi-kritisv/BJNR095800016.html (Accessed: 27 February 2022).

Cyrail Consortium Members (2016) 'Brochure - CYRail Recommendations on cybersecurity of rail signalling and communication systems'. Available at: https://cyrail.eu/IMG/pdf/brochure_cyrail_web.pdf.

Graham, C. (2017) 'Cyber attack hits German train stations as hackers target Deutsche Bahn', *13.05.2017*. Available at: https://www.telegraph.co.uk/news/2017/05/13/cyber-attack-hits-german-train-stations-hackers-target-deutsche/ (Accessed: 27 February 2022).

Haydari, A., Zhang, M. and Chuah, C.-N. (2021) 'Adversarial Attacks and Defense in Deep Reinforcement Learning (DRL)-Based Traffic Signal Controllers', *IEEE Open Journal of Intelligent Transportation Systems*. doi: 10.1109/OJITS.2021.3118972.

Kour, R. *et al.* (2019) 'eMaintenance in railways: Issues and challenges in cybersecurity', 223(10), pp. 1012–1022. doi: 10.1177/0954409718822915.

Kour, R., Karim, R. and Thaduri, A. (2020) 'Cybersecurity for railways-A maturity model', *Journal of rail and rapid transit*, 234(10), pp. 1129–1148. doi: 10.1177/0954409719881849.

Mallah, R. Al, López, D. and Farooq, B. (2020) 'Cyber-Security Risk Assessment Framework for Blockchains in Smart Mobility'. doi: 10.1109/OJITS.2021.3106863.

Sedjelmaci, H. *et al.* (2018) *A generic cyber defense scheme based on stackelberg game for vehicular network; A generic cyber defense scheme based on stackelberg game for vehicular network*, *2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC)*. doi: 10.1109/CCNC.2018.8319229.

Sedjelmaci, H., Hadji, M. and Ansari, N. (2019) 'Cyber Security Game for Intelligent Transportation Systems', *IEEE Network*, 33(4), pp. 216–222. doi: 10.1109/MNET.2018.1800279.

Valdivia, L. J. *et al.* (2018) 'Cybersecurity-The Forgotten Issue in Railways: Security Can Be Woven into Safety Designs; Cybersecurity-The Forgotten Issue in Railways: Security Can Be Woven into Safety Designs', *IEEE Vehicular Technology Magazine*, 13. doi: 10.1109/MVT.2017.2736098.

Bibliography

An, S. H., Lee, B. H. and Shin, D. R. (2011) 'A survey of intelligent transportation systems', *Proceedings - 3rd International Conference on Computational Intelligence, Communication Systems and Networks, CICSyN 2011*, pp. 332–337. doi: 10.1109/CICSYN.2011.76.

Buchegger, S. and Alpcan, T. (2008) 'Security games for Vehicular networks', *46th Annual Allerton Conference on Communication, Control, and Computing*, pp. 244–251. doi: 10.1109/ *Four Cyber Attacks On UK Railways In A Year | Science & Tech News | Sky News* (no date). Available at: https://news.sky.com/story/four-cyber-attacks-on-uk-railways-in-a-year-10498558 (Accessed: 4 March 2022). ALLERTON.2008.4797563.

Cheshire, T. (2016) 'Four Cyber Attacks On UK Railways In A Year | Science & Tech News | Sky News'. Available at: https://news.sky.com/story/four-cyber-attacks-on-uk-railways-in-a-year-10498558 (Accessed: 4 March 2022).

Dimitrakopoulos, G. and Demestichas, P. (2010) 'Intelligent transportation systems: Systems based on cognitive networking principles and management functionality', *IEEE Vehicular Technology Magazine*, 5(1), pp. 77–84. doi: 10.1109/MVT.2009.935537.

Figueiredo, L. *et al.* (2001) 'Towards the development of intelligent transportation systems', *IEEE Conference on Intelligent Transportation Systems, Proceedings, ITSC*, pp. 1206–1211. doi: 10.1109/ITSC.2001.948835.

Guerrero-Ibáñez, J., Zeadally, S. and Contreras-Castillo, J. (2018) 'Sensor Technologies for Intelligent Transportation Systems'. doi: 10.3390/

James, S. J., James, C. and Evans, J. A. (2006) 'Modelling of food transportation systems – a review', *International Journal of Refrigeration*, 29(6), pp. 947–957. doi: 10.1016/J.IJREFRIG.2006.03.017.

Joseph, A. D. (2006) 'Intelligent Transportation Systems', *IEEE Pervasive Computing*, 5(4), pp. 63–67. doi: 10.1109/MPRV.2006.77. s18041212.

Kour, R., Karim, R. and Thaduri, A. (2020) 'Cybersecurity for railways-A maturity model', *Journal of rail and rapid transit*, 234(10), pp. 1129–1148. doi: 10.1177/0954409719881849.

Paganini, P. (2018) *Massive DDoS attack hit the Danish state rail operator DSBSecurity Affairs*. Available at: https://securityaffairs.co/wordpress/72530/hacking/rail-operator-dsb-ddos.html (Accessed: 4 March 2022).

Schuller, D. (2021) 'IT-Sicherheit: Berliner Verkehrsbetriebe wollen unwichtig sein | heise online'. Available at: https://www.heise.de/news/IT-Sicherheit-Berliner-Verkehrsbetriebe-wollen-unwichtig-sein-5032533.html (Accessed: 28 February 2022).

Sedjelmaci, H. *et al.* (2018) *A generic cyber defense scheme based on stackelberg game for vehicular network; A generic cyber defense scheme based on stackelberg game for vehicular network*, *2018*

15th IEEE Annual Consumer Communications & Networking Conference (CCNC). doi: 10.1109/CCNC.2018.8319229.

Shladover, S. E. (2021) 'Opportunities and Challenges in Cooperative Road Vehicle Automation', 05. doi: 10.1109/OJITS.2021.3099976.

Sussman, J. (2000) *INTRODUCTION TO TRANSPORTATION SYSTEMS*. Available at: https://trid.trb.org/view/653797 (Accessed: 4 March 2022).

Whittaker, Z. (2018) 'Rail Europe had a three-month long credit card breach | ZDNet'. Available at: https://www.zdnet.com/article/rail-europe-had-a-three-month-long-credit-card-breach/ (Accessed: 4 March 2022).