IoT Enabled Highways Maintenance: Towards an Understanding of Emerging Cyber Security Threats

Ludwig Trotter
Lancaster University,
United Kingdom

Mike Harding
Lancaster University,
United Kingdom

Mateusz Mikusz
Lancaster University,
United Kingdom

Nigel Davies
Lancaster University,
United Kingdom

IoT technologies are increasingly being deployed to support the operation and maintenance of complex highways infrastructure assets. However, the use of interconnected cyber-physical systems in such critical infrastructure raises important privacy, safety and security issues. While security issues in IoT transport systems and autonomous vehicles are well studied, there is minimal research relating to cyber security in the field of highways maintenance. In this paper, we introduce the problem domain, evidence the lack of existing research and provide example threats to IoT highways maintenance systems based on a real-world case study.

INTRODUCTION

Transport has long been perceived as an important application area for the IoT. Indeed, even in Weiser's seminal ubiquitous computing paper, the motivating scenario includes a transport dimension as “Sal” uses a “forward view mirror” to monitor traffic and find a parking spot at her destination. This close association between pervasive technologies such as the IoT and transportation reflects the criticality of transport in modern society. As we strive towards an increasingly

global, connected society in which mobility is viewed as a service the IoT is playing a key role in transport sectors including logistics, traffic management, autonomous vehicles and multi-modal ticketing.

While topics such as autonomous vehicles attract significant levels of research attention, our work focuses on the more mundane yet crucial topic of maintaining the infrastructure that supports mobility – the physical roads, rails and associated assets that enable people and goods to move. In particular, in this paper we consider the use of the IoT to support highways maintenance (HM), i.e. the process of keeping roads and associated assets (bridges, tunnels, street furniture etc.) in working order. HM traditionally involves relatively low-skilled manual activities such as cleansing (road-sweeping), repairing (fixing potholes) and protecting (road gritting) highways infrastructure assets. Recently, maintainers have begun to explore new approaches to maintenance, evolving from traditional offline reactive "pen-and-paper" processes dependent primarily on tacit worker knowledge, to highly connected, cyber-physical data-driven methods. For example, after the 2007 floods, the UK government led a review of flood management processes, an outcome of which was a Department for Transport initiative to promote the use of data-driven approaches to support more informed, proactive decision-making, to deliver efficient cost-effective management of highway drainage [15]. Beyond applications in drainage, IoT technology is currently being deployed in other maintenance activities such as structural health monitoring and studies have identified a rise in operational performance by utilizing smart wireless sensor networks to monitor deterioration in infrastructure assets such as bridges and tunnels [13].

However, as IoT usage increases within the sector, failure to secure such systems from malicious activity will leave both physical and digital transport assets open to attacks with significant cost and safety implications. Consider, for example, the case of a simple cyber-physical system that collects data from roadside drainage assets to inform cleaning schedules. Potential attacks could result in serious surface water flooding incidents, long-term damage to valuable highways assets (tarmac damage), increased risk of accidents and significantly impact journey time reliability with corresponding economic impact. Furthermore, the future integration of real-time maintenance data with intelligent transport systems such as "Connected and Autonomous Vehicles" [6] will significantly increase the opportunities for malicious attackers to compromise these systems, e.g. by reporting incorrect road conditions to vehicles.

The use of IoT systems in such critical infrastructure thus raises important safety and security issues. We seek to begin to address this gap in current research – furthering the community's understanding of the potential threats and vulnerabilities of IoT based systems used in highway maintenance and highlighting the need for further research in this area. Evidence of a lack of prior research in this area is provided based on the results of a systematic literature review of current IoT transport research (see section 4).

2 UNDERSTANDING HIGHWAYS MAINTENANCE VULNERABILITIES

Our early insights into cyber-security threats in IoT-based HM systems are based on our recent experiences of developing a novel cyber-physical system designed to help highways maintainers monitor the state of their drainage assets and to automatically determine when maintenance is required. The system was developed over a two-year period by a multidisciplinary team with technical expertise in pervasive systems, data science and wireless communications. The results included a novel highway wireless communications network based on the LoRa standard and a rugged IoT sensor probe capable of monitoring and communicating the real-time conditions of highways drainage assets (known in the UK as road-side gullies). Following an iterative design and evaluation process the gully probe and supporting wireless network underwent several alterations due to the technical, environmental and process challenges of deploying and supporting a cyber-physical system on the highways network. The final system supported real-time monitoring of highways drainage assets, transmission of in-field data through a road-side wireless communications network to a centralised data processing platform, inference of new statistical models to predict asset conditions (e.g. future risk of flooding), and, new forms of information

visualisation to support decision-making activities. It is now deployed in multiple locations in the UK.

Our involvement in the end-to-end process of developing a novel cyber-physical maintenance system has provided valuable insights into potential vulnerabilities and threats maintainers are likely to encounter. We categorise vulnerabilities according to the 'three pillars' model of cyber-security [1] where a vulnerability represents an identified weakness of a 'resource' (i.e. technology, people and processes) involved in the activity of supporting and performing HM. Furthermore, we describe threats that aim to exploit vulnerabilities based on the STRIDE model to align with commonly used terms (e.g. intrusion, tampering and spoofing) [5].

2.1 Technology

The deployment of IoT technology within the HM infrastructure leads to a growth in the volume of sensitive datasets, computing systems and physical devices – each of which introduces potential attack areas.

2.1.1 Need to instrument physical assets

The physical security of IoT components is a common consideration during the deployment of cyber-physical systems [3]. In contrast to transport modes such as rail and air where physical security measures (i.e. fencing, barriers) are implemented to mitigate against physical intrusion, highways assets such as traffic lights, bridges and signposts reside primarily within public environments (e.g. residential streets) providing relatively easy access to would-be attackers.

Our experiences of deploying IoT assets for HM have highlighted how maintainers can begin to address physical security vulnerabilities. For example, network components can be installed in locations that provide a level of security from physical intrusion such as high on lamp-posts or sealed within the asset. However, for monitoring asset conditions at ground-level it remains extremely challenging to physically secure IoT equipment.

The risk of physical threats to in-field technology for maintainers could be far-reaching – repairs to damaged IoT hardware or callouts of operatives to attend to assets that report false problems may have major cost and safety implications**. The deployment of IoT technology dictates that maintainers must begin to consider the challenge of physical access and investigate new approaches to ensure instrumented highways assets are physically secure.**

2.1.2 Need to capture and manage new forms of data

Historically highways maintainers' awareness of asset conditions and performance has been limited – for example, in many areas of the UK the highways drainage asset inventory is incomplete and outdated due to the cost of performing asset inspections. As cyber-physical assets become more prevalent across the network, managing large quantities of data from IoT sensors poses new challenges for maintainers. While cybersecurity threats to data stored in online repositories are well known, for maintainers the threat of information disclosure of new datasets that describe the state of highways assets and the maintenance activities performed carries a number of specific risks – e.g. members of the public could use performance data to question why their street drainage system had not been cleaned prior to a major flood, managing authorities could use the data to monitor contractual KPIs, and competitors could use the information in preparing bids for new contracts. **While new awareness over the condition of highways infrastructure is beneficial to maintainers it introduces privacy and security risks through information disclosure threats that could compromise contractual agreements, impact reputation and result in economic loss.**

2.1.3 Use of data in 3rd party safety-critical applications

The transport sector is shifting towards a paradigm of 'intelligent mobility' delivering greater integration, intelligence and automation of transport services. The provision and availability of

new forms of asset data has the potential to enhance the performance of many aspects of the intelligent mobility paradigm. For example, HM data could be integrated with connected and autonomous vehicle systems to support navigation that is sensitive to road conditions and maintenance activities. Our understanding of HM vulnerabilities is limited, yet the integration between autonomous vehicle and HM systems introduces new attack channels in which attackers could compromise perceived low-risk, low-security systems (i.e. maintenance systems) to manipulate high-impact assets to maximise influence over particular aspects of the network (e.g. traffic flows, congestion, damage to assets). For example, performing changes to data that describes a highway's predicted flood risk could be utilised in real-time autonomous vehicle navigation software to orchestrate massive changes in fleet routing.

It is therefore important that maintainers and transport planners begin to consider the use of data beyond the support of maintenance activities. For maintainers, integration with 3rd party systems introduce new attack surfaces that must be secured, while new interconnected sub-systems must begin to support capabilities to quickly identify malicious activity across the transport ecosystem (similar to fraud detection algorithms in the banking sector). **The paradigm shifts towards intelligent mobility and the deepening integration across intelligent mobility services will enable the use of IoT HM data across new transport applications and services. Greater integration introduces new attack surfaces and the potential for proxy intrusion attacks through less secure maintenance systems.**

2.2 People

2.2.1 New relationships with developers & technical stakeholders

The IoT is facilitating the digitisation of existing working practices, change in organisational roles and empowerment of workers [11]. HM activities have traditionally required manual operatives to undertake physical work on the network, such as fixing potholes, repairing street lamps and cleansing highways assets. Similarly, the coordination and planning of maintenance work has involved fairly straightforward processes, with the planning of work based primarily on local knowledge and worker intuition. Our recent collaboration with maintainers has emphasised the growing reliance on external technical support to develop and understand new aspects of the maintenance process, such as interpreting sensor data and applying it to inform decisions. This raises security concerns, particularly spoofing or ’elevation of privilege’ threats where multiple stakeholders (e.g. I.T administrators, data architects, data analysts) can access system components used to support maintenance activities.

For traditional maintainers, the challenge is in understanding how to securely manage the emerging complexity and diversity of existing and new workers and raises technical considerations of how to support authentication and authorisation models for both physical and digital assets. For example, in-field workers will require physical access to assets instrumented with IoT components to undertake maintenance activities such as cleansing a road-side drain but physical proximity could be viewed as an ’elevation of privilege’ threat where in-field workers gain unregulated access to system hardware. **New dependencies on 3rd party developers and technical support workers represent a significant shift in the culture of the maintenance workforce. More complex maintenance activities that involve a growing number of manual and technical workers have the potential to introduce new threats that disrupt operations or compromise data privacy.**

2.2.2 Need for IoT training & certification

While HM typically involves relatively simple manual labour, in contrast, the act of instrumenting highway assets with IoT hardware can require a complex understanding of both the physical asset and the technical components that need to be installed and configured. For example, our experience of deploying IoT infrastructure to monitor road-side drainage has illustrated the challenges in-field operatives would likely encounter, such as the need to understand in detail the drainage asset type and relevant depth in order to install the drainage sensor probe in the correct

position. As a second example, the positioning of wireless communication receivers to relay transmission from drainage sensor probes requires an understanding of both wireless propagations to ensure receivers are in range, and appropriate training to connect devices to mains power via street lamp-posts. These emerging activities highlight new challenges for maintainers to support a repeatable and verifiable installation of IoT hardware to avoid erroneous data. This is particularly important as accidental or malicious actions could be performed by in-field operatives through the incorrect configuration of in-field hardware that would go undetected. For maintainers, the risks of losing trust and confidence in the data could compromise coordination and planning activities. **The installation of the IoT on highways networks is complex. Without new IoT training and certification for in-field operatives, maintainers risk repudiation threats where the quality of the installation and the data cannot be verified.**

2.3 Process

2.3.1 Lack of domain-specific IoT standards & regulation

HM industry understanding and knowledge of implementing the IoT, as represented by domain-specific standards and regulations to help guide maintenance and local authority organisations, is limited. Currently, managing highways authorities are open to technology providers implementing a broad range of IoT wireless communications technologies (e.g. LoRa, SigFox or NB-IoT) to facilitate the transfer of data from IoT sensors to cloud-based services. Without an awareness of how these networks perform within a road-side context, and suitable procedures in place to ensure deployed IoT technology is reliable and complies with highways sector acceptance measures (as applied in the rail sector), latent vulnerabilities have the potential to emerge that enable attackers to compromise safety and security of the wider highways network. For example, where uncontrolled access to road-side wireless networks by multiple IoT applications is not regulated, new opportunities for eavesdropping or manipulation of services could be facilitated. **Further IoT research and innovation is required within the HM sector to begin to develop domain-specific standards and governance to address currently unregulated development, deployment and management of cyber-physical systems to mitigate against associated security threats and risks to the wider highways network.**

3 IoT Security in Related Domains

The consideration of security threats is not uncommon in other transport and infrastructure IoT domains—including autonomous vehicles, rail, and smart grids. While the general objectives of securing the IoT are common, it is only when a particular application of the technology is understood in context that researchers can begin to effectively articulate the unique characteristics (e.g. valued assets, vulnerabilities and risks) of a security problem posed to sector organisations, and the different strategies required to address them.

In this section, we analyse the characteristics of related application domains (§3.1 - §3.3) that leverage data-driven, cyber-physical technologies and discuss the novelty and applicability of emerging HM security vulnerabilities in contrast to these domains. Key differences are highlighted in table 1 and described in section 3.4.

Vulnerabilities	Domain Characteristics			
	Highways Maintenance	**Connected Autonomous Vehicles (CAVs)**	**Smart Grid**	**Rail**
Technology (4.1)				
(4.1.1) Need to instrument physical assets	IoT deployed in physically insecure, open public spaces. Large-scale deployment area.	CAVs are physically secured with limited external IoT sensing technology that can be tampered with. Small-scale deployments.	Assets are contained and secured within isolated physical environments (e.g. sub-stations). High health & safety risk (i.e. electrified). Large-scale deployment area.	Assets are contained and secured within physical environments (e.g. fenced track). High health & safety risk (e.g. high-speed rolling stock). Medium-scale deployment area.
(4.1.2) Need to capture and manage new forms of data	Data not currently available and risks of disclosure poorly understood. Data relates to infrastructure with minimal risk to individual privacy. Complex network of data-sharing stakeholders.	Extensive experience of managing IoT data within the sector. Critical datasets managed locally in-vehicle.	Some experience of managing IoT data. Coarse-grain data already available - fine-grain data (e.g. smart meters) demands new approaches and raises new privacy risks.	Limited experience of managing IoT data within the sector. Infrastructure is managed by a single organisation (i.e. Network Rail) with lower complexities in data sharing.
(4.1.3) Use of data in 3rd party safety critical applications	No established IoT networks for integrating data with 3rd parties. Little understanding of how data could be used in other domains (e.g. CAVs).	Security standards for CAVs and data use already established. Area of intense research & innovation in the use of data.	Well established protocols for isolating the network from consumers. Data transmission via dedicated networks.	Very controlled environment with dedicated data network (e.g. European Train Control System level 2). Existing experience with cps.
People (4.2)				
(4.2.1) New relationships with developers & technical stakeholders	Little in-house technical expertise. Dependence on 3rd party developers and technical support. Limited experience of engaging with advanced IoT technology.	Extensive in-house technical expertise. Specialised on specific tasks such as AI.	Moderate In-house technical expertise.	Moderate In-house technical expertise primarily within mechanical engineering.
(4.2.2) Need for IoT training & certification	Existing workers lack skills to interpret data and install in-field IoT hardware.	High-tech industry. Highly skilled workers.	High-tech industry. Highly skilled workers.	Highly trained engineering with expertise.
Process (4.3)				
(4.3.1) Lack of domain-specific IoT standards & procedures	Limited IoT standards or guidance established within the sector. No previous experience of maintaining IoT technologies.	Installation at production time. Security guidance documents available to the sector.	Smart grid industry is a heavily managed and regulated for field workers. More advanced in-field procedures.	Rail industry is a heavily managed and regulated. Technology acceptance standards well established (e.g. Product Acceptance Committee).

Table 1. Comparison with related domains

3.1 Connected and Autonomous Vehicles

Security vulnerabilities and issues have been well studied in the context of systems and communication protocols supporting autonomous driving [4, 12]. In particular, vehicle-to-vehicle and vehicle-to-infrastructure communication are crucial to ensure the safety of passengers as part of collision warning systems or automated traffic flow management [4]. Raya et al. have identified open security issues such as providing secure positioning of the vehicle, data verification to protect against forging attacks, and DoS resilience against jamming of the network infrastructure [12]. To address these issues, the authors have developed a dedicated security architecture which has the potential to be applied to other IoT domains. For example, Raya et al. suggest the use of dedicated hardware components for handling crucial data using encrypted communication protocols and storage to increase the burdens for malicious access, and verification procedures on a per-data-package basis to protect against "in-transit traffic tampering" [12]. In the context of utilising the IoT for HM, following such existing security architectures could help with protecting against known security vulnerabilities.

3.2 Rail Network

IoT and digital technologies are commonly used for controlling rail traffic flow and track availabilities [7]. As part of efforts for protecting critical infrastructures, the UK Department for Transport issued a "guidance to industry" for the national rail sector to contribute to "reducing its vulnerability to cyber attack" [7]. The guidance document emphasises the emerging threats and vulnerabilities due to the use of standardised components and communication protocols, and the interconnectivity of controlling systems. Specific threats include remote cyber attacks against the software and communication infrastructure that could cause disruptions in the rail network, loss of sensitive information regarding the rail infrastructure, and put both customers and maintenance workers at risk. The guidance document contains recommendations to help protect rail systems against cyber attacks, including the design and implementation of modern technologies and standards "with security in mind as an integral part of the system", and considering security as an important aspect of the system throughout its entire life-cycle including installation, maintenance and disposal.

3.3 Smart Grids

Similar to the U.K.'s efforts in helping to secure the railway infrastructure, the U.S.'s National Institute for Standards and Technology issued a set of "Guidelines for Smart Grid Cyber Security" [14]. Whilst specific vulnerabilities have not been included in the document, the authors point out that vulnerabilities in the grid network can have economic, safety and ecological impact on communities, resulting in unique performance and resilience requirements compared to other IoT systems. To support industry and institutions in implementing appropriate precautions and procedures in their software systems and processes, a detailed set of requirements and risk assessment guidelines have been outlined as part of the document ranging from high-level requirements (e.g. awareness of the risk of vulnerabilities and processes for incident responses), to specific requirements pertaining to the implementation of sufficient cryptography, data integrity and access control mechanisms. It may be possible that elements of these guidelines can be generalised out to other domains of the IoT including HM systems. For example, the recommendation for appropriate permission and access control, and the auditing of systems connected to the IoT infrastructure can be seen as a crucial part of keeping systems secure beyond smart grids.

3.4 Comparative Analysis

3.4.1 Technology

Physical Environments. Physical access security controls are critical to ensure threats such as tampering with cyber-physical asset hardware are minimised. For highways sector organisations (see §2.1.1) this is particularly challenging given that the majority of the highways infrastructure

is open and publicly accessible. In related domains such as the UK's National Grid and Rail Network infrastructure cyber-physical assets are deployed within an isolated environment that is highly protected (e.g. fencing), primarily due to the threat to human safety (i.e. electrification of substations, high-speed rolling stock) and hence physical vulnerabilities of IoT assets are perceived to be less of a security concern. For non-infrastructure domains such as connected and autonomous vehicles (CAVs) IoT instrumentation is typically encased internally within the vehicle body, and leverage established physical security mechanisms (e.g. door locks and alarms) developed within the automotive sector.

Data Management and Availability. The use of cyber-physical technologies raises new technical and security challenges for organisations when attempting to effectively manage new forms of data that describe business processes and provide detailed insights into the internal operation of an organisation (see §2.1.2). While the risks of reputational and economic damage from data leaks are well known in many commercial sectors, for the HM sector the implications of capturing and managing new forms of data that describe the detailed performance of business assets (e.g. drainage conditions) are not well understood. While industries producing CAVs also face new risks, in contrast to the highways sector they are comprised of "technology-first" organisations that already understand the implications of sensitive data disclosure to attackers, and employ well-informed technical strategies to handle and secure the storage of data in the cloud. Differences in data management also occur in each domain – for example, data from in-vehicle IoT sensors are managed locally to support artificial intelligence (AI) decisions that control key vehicle operations such as steering and the drivetrain. This reduces the need to be concerned with vulnerabilities and threats that may target data stored in the cloud.

3.4.2 People

Diverging Workforce and Skills. The HM workforce has traditionally been dominated by manual in-field operatives undertaking physical work on the network, such as fixing potholes and cleansing highways assets. As the sector moves towards more innovative data-driven processes, new technical skills must be integrated and managed within what is currently a low-tech literally domain to develop and support emerging technical systems (see §2.2.2). In contrast, the energy and rail maintenance sectors have extensive experience of managing internal workforces that comprise both highly certified technicians and more low-skill operatives. Therefore, these domains are much better equipped to adjust to new innovative approaches internally without the need to outsource aspects of their work to 3rd party developers, and subsequently avoid the risk of introducing new vulnerabilities that could open them up to additional cyber security threats (see §2.2.1).

3.4.3 Process

Technical innovation and management procedures. The level of technical innovation within the HM sector has been relatively stagnant in comparison to advances in adjacent domains such as in smart grid energy and rail infrastructure management. As a result, internal procedures and guidance centred around the development, adoption and management of new emerging cyber-physical technologies are lacking within the sector, and therefore expose maintainers to a number of process-related security challenges (see §2.3.1). In contrast, within the rail sector regulated product acceptance processes exist internally to ensure new technologies meet specific performance criteria, while further guidance and best practice resources are enforced that aim to ensure cyber security threats are addressed.

4 EVIDENCING A LACK OF PRIOR RESEARCH

While general IoT security is an area of intense research activity [8] we are particularly interested in the potential for domain-specific threats that are not covered by such general work.

4.1 Methodology

To explore the extent of prior research we conducted a systematic literature review, loosely based on the "Procedures for Performing Systematic Reviews" proposed by Kitchenham [10]. By choosing a systematic approach we aimed to conduct a comprehensive and transparent analysis of the literature to address the following three research questions:

RQ1: Is there a body of literature that addresses security concerns in IoT–based HM?

RQ2: Which threats/threat models have been identified in the literature in the scope of IoT based HM?

RQ3: Are there design guidelines or recommendations provided by the literature to address threats in IoT HM systems?

4.1.1 Search Process

Data Sources

HM systems represent a multidisciplinary field of research including transportation, civil, mechanical and electrical engineering, electronics, communication technologies and computer science. We selected four widely recognised digital libraries, covering the majority of publications in each relevant discipline:

ACM Digital Library: Computer science, communication technologies

IEEE Xplore: Computer science, electrical engineering, communication technologies

ScienceDirect: Computer science, transportation, civil, mechanical and electrical engineering

Scopus: Computer science, transportation, civil, mechanical and electrical engineering, electronics, communication technologies

Keywords

We developed a comprehensive set of search terms comprising of four keyword groups (highways, IoT, maintenance, security) from which our search queries were built. All keywords were based on an initial manual literature survey and were proposed and discussed among all authors. The keyword table (see table 2) includes a large number of synonyms, common abbreviations and acronyms (e.g. IoT), country-specific names (e.g. motorway and freeway) as well as related terms. In total we identified a set of 56 keywords, resulting in a total of 18000 unique queries.

Search keywords	
highway:	motorway, auobahn, freeway, road, street, traffic, roadside, intersection, junction
internet of things:	iot, Cyber-physical system, Sensor Networks, Web of Things, Internet of Everything, Smart infrastructure, Connected devices, connected things, connected objects, Networked devices, Networked things, Networked objects, Smart devices, Smart things, Smart objects, Car-to-infrastructre, C2M, Vehicle-to-infrastructure, V2I, V2X, Machine-to-Machine, M2M, M2X, machine-to-infrastructure, IoV, M2I, inter-connected, intelligent transportation systems,
maintenance:	management, operation, improvement, repair, road works
security:	vulnerabilities, vulnerable, vulnerab, attack, threat, privacy, resilience, violence, trust

Table 2. Search categories and synonyms

Inclusion and exclusion criteria

Following the systematic approach, inclusion and exclusion criteria were determined. We included literature from our four data sources that were: peer-reviewed; written in English; contained any valid keyword combination; and, was a description/study/simulation of a system with an IoT component that supports HM or was a literature review of IoT-based HM. We excluded: duplicate publications of the same study/article; papers where the search terms were used in a different meaning/context (e.g. security related to road safety); papers where security considerations were not related to IoT-based HM.

Computerised approach

Due to the large number of keyword combinations, we developed a Python script to query the source databases. The software searches for scientific articles that contain valid search keyword combinations in the abstract and returns meta-data related for the results (i.e. the name of the source library, the library-id, DOI, names of author(s), title, abstract, the name of the publication and author keywords).

To reduce the number of queries we issued to the libraries the search was split into a primary search excluding the security keywords and a secondary search, applying the security keywords on the initial results. By doing so, we were able to reduce the number of queries against the digital libraries by 90%. In total, we performed 1,800 queries across each digital library totalling 7,200 queries.

4.1.2 Review Process

The review process consisted of three distinct steps. Following a screening process where irrelevant and duplicate data were removed, we conducted an initial review based on the collected metadata and our inclusion and exclusion criteria. During this initial review, we produced a short summary of the paper and classified each paper as:

> **Accept:** The publication is related to the subject and relevant according to the inclusion criteria.
>
> **Borderline:** The publication might be related to the subject and/or might be relevant according to the inclusion criteria.
>
> **Reject:** The publication is not related to the subject and/or not relevant according to the inclusion criteria.
>
> **Delete:** The publication is not related to the subject e.g. false positive, linguistic ambiguities.

Each assessment was peer-reviewed by at least one other reviewer. In case of discrepancies, a third author reviewed the paper and mediated until a consensus was reached. The remaining papers marked “accept” or “borderline” were subjected to an in-depth analysis.

4.2 Results

Searching for papers on HM and the IoT returned a total of 1,972 publications. Restricting these papers to those that also discussed security resulted in a set of 308 papers that we used for our literature review. From this set, 111 publications were removed based on further application of our inclusion/exclusion criteria (34 duplicates, 77 not peer-reviewed) leaving 197 publications remaining.

A review of these 197 publications identified a strong focus (32 papers) on Vehicular Traffic Management Systems, i.e. traffic flow control systems, dynamic speed management, intersection management, collision avoidance, emergency unit dispatching or incident detection. These systems are closely linked to HM and may even rely on data aggregated from IoT sensors deployed by highways operators. Hence, major concerns such as operational safety, security and privacy [9] are of relevance to IoT-driven HM.

During the review, we also identified a large number of publications in the field of car-to-car and car-to-infrastructure communication (28 publications) as well as wireless sensor networks (18 publications). The identified research covers many security issues such as secure communications and threat models for vehicular networks [2].

Applying our classification scheme to identify papers that directly addressed HM, the IoT and security we classified 20 as accept or borderline during the meta-data review and these were subjected to an in-depth analysis. While the meta-data and abstracts indicated that these papers might be of direct relevance, closer examination revealed very little information relating to ***RQ1*** and none of the reviewed publications contained relevant information related to the research questions ***RQ2*** and ***RQ3***. In summary, our literature review indicates a clear gap in research that focuses on cyber-security threats in IoT-based HM systems.

5 CLOSING REMARKS

Modern society relies on safe, secure and efficient transport networks. Increasing pressure on these networks is leading their owners and operators to deploy IoT technologies in an effort to improve the overall effectiveness of the networks. However, our research suggests that little attention has been paid to the domain-specific security threats that arise when deploying IoT within the transport sector – and in particular when using the IoT to support routine HM and operational tasks. In this paper, we have not proposed specific solutions but instead have focused on describing examples of challenges for the highways sector and evidencing lack of prior work through a systematic literature review. In so doing, we hope to catalyse new research in the field in order to ensure we are able to continue to rely on our transport infrastructure in the future.

ACKNOWLEDGMENTS

This work has been partially funded by the UK EPSRC as part of "PETRAS IoT Research Hub – Cybersecurity of the Internet of Things" (EP/N023234/1) and by InnovateUK and NERC as part of "Data-driven Precision Surface Water Management for Urban Environments" (NE/N007808/1).

REFERENCES

1. ISO/IEC 27001:2013. Information technology — security techniques — information security management systems — requirements. Standard, International Organization for Standardization (ISO), Geneva, CH, October 2013.
2. T. Alpcan and S. Buchegger. Security games for vehicular networks. *IEEE Transactions on Mobile Computing*, 10(2):280–290, 2011.
3. S. Babar, A. Stango, N. Prasad, J. Sen, and R. Prasad. Proposed embedded security framework for internet of things (iot). In *2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace Electronic Systems Technology (Wireless VITAE)*, pages 1–5, Feb 2011.
4. S. Biswas, R. Tatchikou, and F. Dion. Vehicle-to-vehicle wireless communication protocols for enhancing highway traffic safety. *IEEE Communications Magazine*, 44(1):74–82, Jan 2006.
5. S. F. Burns. Threat modeling: A process to ensure application security. *GIAC Security Essentials Certification (GSEC) Practical Assignment*, 2005.

6. Centre for the Protection of National Infrastructure, Centre for Connected and Autonomous Vehicles. Principles of cyber security for connected and automated vehicles. Technical report, UK Department for Transport, AUGUST 2017.
7. Department for Transport. Rail cyber security – guidance to industry. Technical report, Department for Transport, February 2016.
8. J. Granjal, E. Monteiro, and J. S. Silva. Security for the internet of things: a survey of existing protocols and open research issues. *IEEE Communications Surveys & Tutorials*, 17(3):1294–1312, 2015.
9. B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady. Enhancing security and privacy in traffic-monitoring systems. *IEEE Pervasive Computing*, 5(4):38–46, Oct 2006.
10. B. Kitchenham. Procedures for performing systematic reviews. *Keele, UK, Keele University*, 33(2004):1–26, 2004.
11. C. Loebbecke and A. Picot. Reflections on societal and business model transformation arising from digitization and big data analytics: A research agenda. *The Journal of Strategic Information Systems*, 24(3):149 – 157, 2015.
12. M. Raya, P. Papadimitratos, and J. p. Hubaux. Securing vehicular communications. *IEEE Wireless Communications*, 13(5):8–15, October 2006.
13. F. Stajano, N. Hoult, I. Wassell, P. Bennett, C. Middleton, and K. Soga. Smart bridges, smart tunnels: Transforming wireless sensor networks from research prototypes into robust engineering infrastructure. *Ad Hoc Networks*, 8(8):872–888, 2010.
14. The Smart Grid Interoperability Panel - Cyber Security Working Group. Introduction to NISTIR 7682 – Guidelines for Smart Grid Cyber Security. Technical report, U.S. Department for Commerce, September 2010.
15. UK Department for Transport. Guidance on the management of highway drainage assets. Technical report, UK Goverment, NOVEMBER 2012.

ABOUT THE AUTHORS

Ludwig Trotter is a postgraduate student in Human-Computer-Interactions at Ludwig-Maximilians-University Munich and Research Assistant at the School of Communications and Computing at Lancaster University, UK. His research focuses on fostering understanding of safety and security issues related to the use of IoT in highways maintenance. Contact him at l.k.trotter@lancaster.ac.uk.

Mike Harding is a Research Fellow in the School of Computing & Communications and the Data Science Institute at Lancaster University. His research explores the experimental design of next-generation IoT & pervasive data science technologies that aim to address prominent economic, social & environmental challenges in the areas of transport infrastructure management & urban mobility. Contact him at m.harding@lancaster.ac.uk.

Mateusz Mikusz is a Research Associate and final-year PhD student at the School of Communications and Computing at Lancaster University, UK. His research focuses on pervasive data analytics, mainly in the context of digital signage. Mikusz received his master's degree (Diplom-Informatiker) from the University of Stuttgart. Contact him at m.mikusz@lancaster.ac.uk.

Nigel Davies is a Professor of Computer Science at Lancaster University, UK, and co-director of Lancaster's Data Science Institute. His research is in the area of pervasive computing and is characterized by an experimental approach involving large-scale deployments of novel systems. Contact him at n.a.davies@lancaster.ac.uk.