Threat Modelling of IoT Systems Using Distributed Ledger Technologies and IOTA

Amalia Damianou, M. Amir Khan, Constantinos Marios Angelopoulos, Vasilios Katos
Bournemouth University, Poole, UK {adamianou, s5068096, mangelopoulos, vkatos}@Bournemouth.ac.uk

***Abstract*—Internet of Things has emerged as a key technological enabler for broader socio-technical and socio-economic paradigms, such as smart cities and Circular Economy. However, IoT systems are characterised by constraints and limitations which in order to be overcome they need to be deployed in conjunction and in synergy with other emerging ICT. Distributed Ledger Technologies (DLT) can help overcome challenges pertaining to data immutability, timeliness and security. However, the use of DLT does not satisfactorily mitigate security risks and vulnerabilities *per se* and currently cybersecurity aspects of IoT systems are addressed in a fragmented way. Furthermore, the conflict between the resource demanding Blockchains and the highly constrained nature of IoT devices hinders implementation efforts of corresponding systems. We consider networked systems that comprise both IoT and DLT technologies via the prism of Intelligent Transportation Systems (ITS). We elicit a three-tier threat model identifying attack vectors at the Device, the Network and the DLT layers. The identified attacks are then ranked by using the DREAD ranking scheme. The use of the threat model is demonstrated on a novel proof-of-concept IoT networked system implemented using the IOTA Tangle distributed ledger, where it helps to critically appraise the design of the system against the most critical attacks. Furthermore, the developed system is among the first in the literature to demonstrate the synergy of IoT and DLT on actual constrained embedded devices. The performance evaluation provides insights showing that such systems can be efficient and suitable for real-life deployment.**

***Index Terms*—Distributed Ledger Technologies; Internet of Things; Intelligent Vehicles**

I. Introduction

Over the past years, technological advancements have helped address key challenges of the Internet of Things (IoT) paradigm, such as global addressing schemes of embedded devices, seamless interconnection of sensors and actuators to the Internet and long-range wireless communication of low power embedded devices. As a result, the deployment of IoT networked systems is shifting from stand-alone systems that operate in isolation, such as wireless sensor networks deployed in a smart building, to large scale well-connected IoT systems covering big areas of interest such as smart cities.

As a result, IoT has emerged as one of the key technological enablers that in synergy with other emerging technologies (Distributed Ledger Technologies (DLT), Edge Computing and 5G networks, and other) underpin broader socio-economic paradigms. In the case of urban environments, IoT networked systems have played a key role in the definition of the various levels of smart city readiness. These include, a) instrumented cities, where the city infrastructure is digitised but interoperability among the various subsystems is limited, b) connected cities, where the interconnection of multiple infrastructure subsystems enables the development and improvement of city-wide services; and c) responsive cities, where the digital infrastructure of the city directly informs decision making and resource provisioning.

While much effort is put in improving the efficiency, interoperability and impact of IoT systems, the study of their cyber security aspects is fragmented and conducted using methods and tools that have been initially developed for regular computer systems and, therefore, do not address the specific challenges of IoT. What is more, cybersecurity is often considered in retrospect and after an incident has taken place, thus requiring retrofitting already commissioned systems. Given the increasingly critical role of IoT in several application domains, there is a dire need for a systematic approach in addressing security aspects of IoT networked systems that will enable the integration of relevant methods in their development lifecycle.

Our contribution. In this work we address large scale IoT networked systems in smart cities via the prism of Intelligent Transportation Systems (ITS). We consider systems that comprise both IoT and DLT technologies and elicit a three-tier threat model identifying attack vectors at the Device, the Network and the DLT layers. The identified attacks are then ranked by using the DREAD [1] ranking scheme. The use of the threat model is demonstrated on a novel proof-of-concept IoT networked system implemented using the IOTA Tangle distributed ledger to store generated data. In particular, the model helps to critically appraise the design of the system against the most critical attacks indicating how threat modelling can be integrated in the development lifecycle of IoT systems. Furthermore, the developed system is among the first in the literature to demonstrate the synergy of IoT and DLT on actual constrained embedded devices. Its performance evaluation provides insights showing that such systems can be efficient and suitable for real-life deployment.

II. Related Work

The growth of big cities population around the world poses great challenges. It is estimated that big cities consume 75% of natural resources globally and produce 50% of global waste [2]. As the forecast is that a growing percentage of the global population will reside in cities for the years to come, socio-technical paradigms, such as those of smart cities and circular economy [3], seek to leverage emerging ICT in designing and developing more efficient services and better informed decision and management mechanisms. To this end, IoT is one of the key enabling technologies as it allows massive and at scale monitoring of resources and collection of corresponding data. The ephemeral and lossy nature of IoT communications and systems as well as the shear volume of generated data raise issues in regard to data quality. The combination of IoT systems with Distributed Ledger Technologies, such as Blockchain, is investigated as a way of mitigating those issues.

In [4] the integration of IoT and Blockchain are studied and the main challenges identified are pertinent to the low-end specifications of IoT devices and the scalability issues of Blockchain (mainly with respect to efficiently managing the big volume of IoT transactions in a timely manner). Addressing this challenge, in [5] authors describe a lightweight Blockchain-based architecture for IoT, which they claim it eliminates the overheads of classic Blockchain, while maintaining most of its security and privacy benefits. In [6] authors propose a Blockchain-based architecture to protect the privacy of users and to increase the security of a vehicular ecosystem comprising connected vehicles in a smart city. However, contrary to our work here, they only describe the architecture and don't provide a working prototype. In [7] authors present an architecture in which they leverage Edge Computing in order to help mobile and IoT devices running a Blockchain application to validate faster transactions. Again, in this case, authors only describe the architecture and don't provide a working prototype. In [8] authors present a distributed access control system for IoT based on blockchain technology by means of its architecture. Contrary to our work, an implementation is not provided and the architecture provisions the use of hub management devices rather native interconnection of IoT devices. In [9] a systematic review is provided on the integration of IoT and Blockchain. Authors claim that Blockchain can address privacy and security valnerabilities of IoT systems due to its innate properties; namely, immutability, transparency, auditability, data encryption and operational resilience. While this may be the case to some extend, we argue that this approach does not suffice in order to proclaim an IoT networked system as secure.

As an indicative example, we consider IOTA; a DLT that has been developed to specifically address the IoT paradigm and which we also use in our PoC system. In February 2020, the dedicated desktop client Trinity was hacked, causing loss of coins from user wallets and the IOTA Foundation to shut down the entire network for nearly 2 months. In [10], the incident is described. In 2017, IOTA Foundation attempted to create a hash function for facilitating IOTA payments. However, an MIT research team revealed that there are vunlerabilities that can affect the payments [11]. In 2019, IOTA network experienced unavailability for over than 15 hours, which made users unable to send transactions, because of a bug. The main issue was related to the Coordinator of IOTA, which had been affected by the bug, making users unable to send transactions over the Tangle [12]. In the threat model we present in this work, we identify risks that emerge as a result of using Blockchain or other DLTs.

Threat modelling is a task usually undertaken bearing in mind a specific system that is under development. In [13] common threat modeling frameworks are reviewed, which however have been developed for regular computer systems operating over the Internet (e.g. banking systems). For this reason, these models strongly focus or consider exclusively software-based systems, thus allowing many vulnerabilities to pass through undetected when applied on IoT systems, which are typically cyber-physical. In [14] authors address this gap for IoT health devices. They present a threat model by considering commonly used health devices, such as connected inhalers and activity trackers. In this work, we also address the threat modelling gap in IoT by considering Intelligent Transportation Systems in smart cities that use DLT. However, our threat model is more generic and can easily be adapted to other domains as well.

III. Risk Assessment of Intelligent Transportation Systems

In this section we discuss Intelligent Transportation Systems (ITS) and indivative incidents that have occurred on live systems which help us conduct our risk assessment and identify corresponding attack vectors.

Intelligent Transportation Systems (ITS) include smart cars and traffic furniture, smart railway and air craft control systems, smart maritime surface vessels, etc. The rise of the ITS sector comes along with corresponding indcidents of cyber attacks as modern cars can be considered "computers on wheels" [16]. Small computers have augmented the traditional mechanical systems of a vehicle, and manage systems they are fitted with, like infotainment systems. Modern vehicles are equipped with the Controlled Area Network (CAN) bus and an On Board Diagnostics Socket (ODS) that provide physical access to the car system. On the other hand, since CAN bus is an established technology, several vulnerabilities have been detected [17]. As new services are being introduced, several of which operate over Internet connections, such as on-line infotainment, remote software updates and emergency calls to the driver these vulnerabilities pose a significant risk [18]. The problem is further agravated as vehicles are equipped with additional on-board sensors and new communication paradigms are being introduced, such as Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) comprising communications between vehicles and road infrastructure [].

There are several categories of IoT-enabled attacks on ITS systems. Preliminary works have identified and analysed

TABLE I
THE DREAD THREAT RATING SCHEME [15]

	Rating	High (3) (score: [12-15])	Medium (2) (score: [8-11])	Low (1) (score: [5-7])
D	Damage potential	The attacker can subvert the security system; get full trust authorization; run as administrator; upload content.	Leaking sensitive information.	Leaking trivial information.
R	Reproducibility	The attack can be reproduced every time and does not require a timing window.	The attack can be reproduced, but only with a timing window and a particular race situation.	The attack is very difficult to reproduce, even with knowledge of the security hole.
E	Exploitability	A novice programmer could make the attack in a short time.	A skilled programmer could make the attack, then repeat the steps.	The attack requires an extremely skilled person and in-depth knowledge every time to exploit.
A	Affected users	All users, default configuration, key customers.	Some users, non-default configuration.	Very small percentage of users, obscure feature; affects anonymous users.
D	Discoverability	Published information explains the attack. The vulnerability is found in the most commonly used feature and is very noticeable.	The vulnerability is in a seldom-used part of the product, and only a few users should come across it. It would take some thinking to see malicious use.	The bug is obscure, and it is unlikely that users will work out damage potential.

various real world cases of attacks over ITS systems that took place during recent past years. The first category of attacks includes exploitation of CAN bus vulnerabilities, unauthorised access to subsystems and data of them, injection of crafted messages and malware [16]. IoT-enabled attacks include exploitation of vehicle infotainment vulnerabilities, exploitation of radio communication protocols, such as LAN, DAN and WiFi, attacks against IoT devices, such as sensors, inside a vehicle and traffic control infrastructure. In [19], a remote attack based on low-cost radio equipment is presented. The attacker, being nearby the target car, can use a $15 radio transmitter in order to exploit CAN network and software vulnerabilities, and connect and send commands to the CAN bus. In [20], authors describe a similar attack, however, the distance between the target vehicle and the attacker is extended by setting up a bogus radio station, which is used for transmitting crafted Digital Audio Broadcast (DAB) messages. The aim of this attack is to compromise the infotainment and to control it directly by sending false messages to the driver. A similar attack, based on the exploitation of the Bluetooth or the telematics unit is described in [21]. Attacks based on WiFi connectivity vulnerabilities have been performed by professional penetration testers, who discovered that the mobile app that is used to remotely control a specific car model, was using car WiFi access point, instead of a GSM module. By cracking the WiFi password and replaying the old commands from the mobile app, attackers can alter these commands in order to remotely control systems of a vehicle. Attacks of this category either require that attackers have some physical proximity to the target vehicle, or that the vehicle obtains some special features, such as DAB and WiFi protocols.

Vulnerabilities of the CAN bus protocol can have serious consequences to various subsystems of a vehicle. In addition, infotainment systems can also be considered as vulnerable. In [22], authors describe the way in which an Internet-connected vehicle (a Jeep Cherockee), was remotely hacked by compromising its infotainment system. Researchers revealed an open port, used by the Harman Uconnect infotainment, in cellular network. Through this open port, malicious parties can scan the software and exploit vulnerabilities in the OMAP chip of the head unit.

Various kinds of sensors facilitate autonomous driving systems and provide data to systems like ACC, collision avoidance or lane keeping assist system. The systems connectivity to the network keep them exposed to remote attacks and system failures. In one case released by Tesla Motors [21], the loss of a human life was caused by a self-driving car where due to a system failure of the car's sensors, the car collided with an 18-wheel truck and trailer. There are several verified attacks of system failure because of sensors failure. In [23], the camera of a vehicle was blinded by a low-cost laser, which exploited the lack of authentication in Light Detection And Ranging (LiDAR) messages. Through this vulnerability, malicious parties gained access to older commands. In this way, the attacker could replay them to produce false artifacts and confuse the system. Other attacks, such as relay station and amplification attacks, demonstrate weaknesses in the Remote Keyless Entry (RKE) systems [24]. The above mentioned attacks require physical proximity to the vehicle target in order for the communication sensors to be compromised. At the same time, we should bear in mind that the control of a vehicle is gradually taken away from the driver and being placed on embedded autonomous control systems in order to automate the driving process. Therefore, the protection of the vehicle sensors from remote attacks over the Internet or other wireless networks should also be taken into consideration as a threat landscape.

IV. Threat Modelling for ITS using IoT and DLTs

Motivated by the aforementioned ITS cases, we consider ITS that employ IoT and DLT (including Blockchain) in the context of a smart city. For such systems, we identify several vector attacks and categorise them in three tiers; namely the Device, Network and DLT tiers. Tables II, III and IV provide the details regarding each type of attack.

Threat modelling provides the necessary approach in order to estimate the severity of the attack vectors that we elicit and to identify the impact that they may have on an ITS system and its users. This is achieved with the use of threat rating schemes that help calculate and assign risk rating values to each type of attack. In our case we apply the industry-standard DREAD rating scheme [15] (table I). A threat rated as high poses a very great threat to the system or its user and needs to be resolved urgently by implementing appropriate countermeasures. A threat rated as medium also needs to be addressed, but not as urgently as for a high-risk threat. A threat rated as low may not be addressed at all as it does not pose a significant threat or risk.

DREAD cyber threat intelligence modelling provides a rating system for identified risks by assessing and analysing various aspects of them, such as their potential to cause damage, and creating risk probabilities. In this way, organisations vulnerable to threats, evaluate the damage that has been done by one or more attacks and create damage assessment profiles for similar attacks in the future. The DREAD threat model provides a rating system and classifies threats under low, medium, and high-risk categories [25] [26].

DREAD evaluates attack vectors with respect to Damage, Reproducibility, Exploitability, Affected Users, and Discoverability of a threat, and how extensive is the affection of it to these five key points. Depending on the severity of a threat and its threat rating, calculated by taking into consideration these five key points, it is categorised as low, medium and high by giving a fine score withing a range of values for each category. After the risk analysis process though DREAD, each organisation should act in order to address these threats and minimise the probabilities for extensive damage, by adopting cybersecurity techniques [1].

Taking into consideration the aspects that DREAD evaluates regarding the risks and vulnerabilities of an ITS system, affected users are an essential part of this evaluation, since in most cases they are adversely affected by the exploitation of a risk or a vulnerability. Apart from DREAD various risk assessment frameworks are used for the same purposes, however, evaluating different aspects from DREAD, such as confidentiality, integrity and availability impact. Furthermore, carefully considering the oprational environment of an IoT system is also crucial since by nature IoT networked systems are cyber-physical systems whose compromise can greatly affect critical systems and infrastructure such as power supply networks, traffic management systems and e-health systems.

We identify risks of ITS based on three important tiers, the physical devices, the network and the Distributed Ledger.

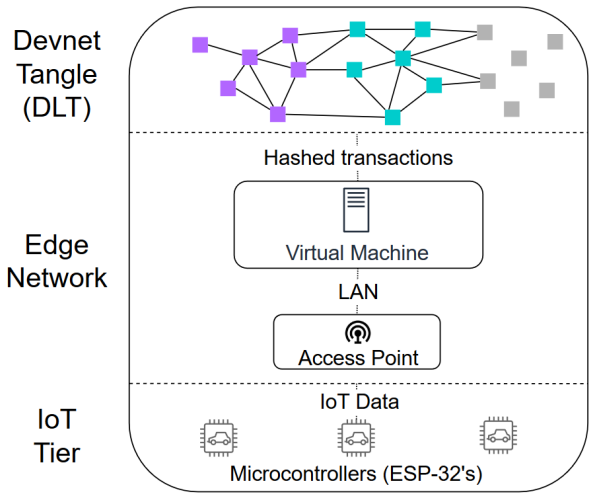

Fig. 1. Diagram that splits the PoC architecture into separate tiers from a top-down perspective.

We evaluate them adopting the DREAD threat modelling with respect to damage, reproducibility, exploitability, affected users and discoverability. Each threat is evaluated and assigned a score. After calculating their overall score, the threats are categorised to low, medium and high levels. The threat model is presented in the tables in the Appendix, and provides insights regarding the severity of each threat for an ITS. Most of the identified threats are evaluated to medium and high rating, thus they can be considered as serious threats for ITS.

V. A Proof of Concept ITS Combining IoT and DLT

Smart cities leverage emerging ICT to provide more effective services in a range of application domains. We focus on Intelligent Transport Systems that combine the use of both IoT and DLTs to enable a secure and scalable infrastructure. A real world application would appear as follows: in a smart city digital infrastructure (microcontrollers and sensors placed in periodic increments on roads, such as in traffic lights or road structures) is in place, thus enabling a vast range of metrics to be monitored pertinent to traffic flow. Smart connected vehicles can either be autonomously or manualy driven, and are able to communicate to traffic structure machine-to-machine.

If a traffic light is known to be red at a specific time and a vehicle violates the light while sending its periodic HELLO message, then the authorities will be able to review this data and see that this vehicle violated this red light. Any scenario where a vehicle has communicated to another machine can be reviewed if needed, such as in the occurrence of a car accident. Investigations will be split into two segments, the physical forensic investigation, examining aspects such as the road condition and the sobriety of the driver, as well as the digital forensic investigation, examining aspects such as a critical system of the vehicle having been compromised as a result of a cyber attack. Collected data can then be used to reconstruct the scene and facilitate the investigation. To this end, using a DLT can greatly contribute since it can provide

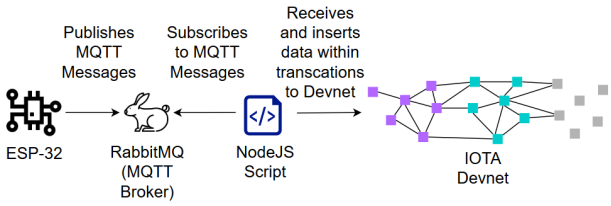

Fig. 2. Insight into the interaction between the microcontrollers and message broker.

usefull attributes to the system, such as data immutability and persistent timeliness, that can help with attribution and evidence corroboration.

The presented PoC system makes use of the IOTA DLT [27]. IOTA has been developed specifically to address the IoT paradigm; it makes use of the Tangle, a distributed ledger where blocks of transactions are organised in directed acyclic graphs. Tangle is currently available in two instances, the mainnet (the live version) and the devnet (used for development purposes). The Tangle is incredibly scalable as one transaction is linked to two others when being verified, in turn verifying the two others. This is different to the traditional one-to-one Blockchain architecture and allows for more transactions to widen the bottleneck of the validation process rather than shrink it. As a result, the rate at which transactions are validated and ledgered on the Tangle is significantly faster and resource efficient compared to typical Blockchain platforms.

The PoC system involves the use of the two core technologies. IoT devices acting as vehicles and traffic structures and a DLT in the form of IOTA developer network (Devnet). The aim of the system is to act as a working testbed for the evaluation of systems comprising IoT networks and DLT and to be used in their evaluation.

Figure 1 provides a high level architecture of what the testbed prototype looks like, and which technologies and hardware are involved. Starting at the IoT tier, microcontrollers are being used to collect data from the vehicles. This data will be in the form of variables such as speed of travel, location of ping or HELLO messages to other vehicles or data structures. The microcontrollers of choice are Espressif ESP-32 with WiFi radio interface.

At the Edge Network tier, the IoT devices communicate wirelessly to a virtual machine (VM) running Ubuntu 18.04.5 connected on the same LAN. Within this VM sits an MQTT message broker (RabbitMQ). This message broker allows for the IoT devices to communicate to the server using MQTT messages. MQTT was selected due to its focus on restrained hardware. Once the IoT devices have established a connection to the LAN and are able to communicate via the lightweight messaging protocol, they begin to publish messages to the broker. Also running on the VM, is a NodeJS script whose purpose is to connect to RabbitMQ and subscribe to the incoming messages. Once subscribed, the script then inserts the message data directly into the IOTA Devnet Tangle. The data within these messages are the variables that the IoT devices are recording and sending. Once inserted into the distributed ledger, the script prints out the corresponding hash value that is required for retrieving data from the tangle.

Figure 2 highlights how the message broker and the script act as middle men between the IoT devices and the IOTA DLT. IoT devices are low-power and restricted in their resource capacity with security risks and vulnerabilities, meaning no data stored on them is safe. The IOTA Tangle offers storage capacity and is considered to be secure. One entity creates the data and the other stores it, allowing for them to work in synchronised tandem. Therefore, the combination of both technologies address the shortcomings that IoT devices face. All source code of the testbed is freely available on Github [28]

A. *Comparison to a Real World Implementation*

If this system was to exist in a real world implementation, there would be distinctions from the testbed prototype created. Within the IOTA framework, private instances of a Tangle can be built and managed. Nodes run the software that gives them read and write access to the Tangle [29]. In the case of a smart city, the local council or another trusted authority can create and operate these private nodes meaning theyll be the only ones with access to the DLT. This is of the upmost importance as the data is distributed amongst all nodes, meaning it must be contained due to its sensitivity. The Tangle will be handling sensitive user data that contains location and private information specific to members of the public and beyond. With this in regard, private Tangle instances must be operated with no public access to them.

Further to this, the technologies that establish the communications between vehicles and traffic structures would be different. For example, instead of MQTT messages over Wi-Fi, a peer-to-peer connection would be established using 5G networks instead. Once the infrastructure is in place, the system will be ready to collect data from the vehicles. These metrics can include speed of travel, location of ping, HELLO messages and technical statistics of vehicle status (type pressure, oil level, brake fluid levels, etc.). These metrics would be vital to build a digital twin of a scenario at any moment in the past in the context of an investigation or to perfom some analytics.

Indicative scenarios implemented on the PoC system:

- Congestion Detection - Being able to detect and record traffic provides valuable data on which roads or routes are busy at which times. This information may provide valuable insight when considering changes to current roads or designing future traffic flow mechanisms.
- Adaptive Control - Adaptive control of roads and traffic flow would directly result to achieving more efficient traffic and road use. This may correlate to other statistics such as lives saved by emergency service vehicles. This could be achieved by creating green paths. Figure 4 is an example of how adaptive control can be used to create a green path for emergency service vehicles. The roads highlighted red have been stopped from accessing the

Overview			Details			Network		+/-
Name	**User name**	**State**	**SSL / TLS**	**Protocol**	**Channels**	**From client**	**To client**	
127.0.0.1:45112 ?	guest	running	○	MQTT 3.1.1	1	0 B/s	60 B/s	
192.168.0.24:65326 ?	smart-car	running	○	MQTT 3.1.1	1	10 iB/s	0 iB/s	
192.168.0.38:53361 ?	smart-car2	running	○	MQTT 3.1.1	1	10 iB/s	0 iB/s	
192.168.0.39:60626 ?	smart-car3	running	○	MQTT 3.1.1	1	10 B/s	0 B/s	
192.168.0.42:53338 ?	smart-car4	running	○	MQTT 3.1.1	1	15 iB/s	0 iB/s	
192.168.0.44:59980 ?	smart-car5	running	○	MQTT 3.1.1	1	15 iB/s	0 iB/s	

Fig. 3. Overview of connected devices.

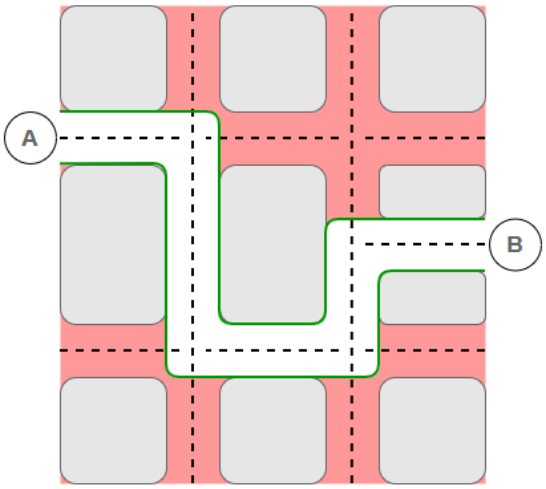

Fig. 4. Demonstrating a green path cleared for an emergency service vehicle to reach point B, from point A.

green path, by adaptively turning all of the traffic lights red. This could be a mechanism to ensure the emergency service vehicles encounter as least traffic as possible en route to point B, the destination.

- Connected Vehicles and Roads - This allows for the digital forensic investigations to take place on incidents that occur on roads. It provides further evidence to accurately establish what has occurred.

B. Performance Evaluation

Figure 3 displays the six connected nodes to the message broker at that moment in time. *smart-car* is one ESP-32 that is currently connected and publishing messages to the message broker. It is publishing at a rate of 10 bytes per second and this is defined within the firmware of the device. *guest* is the VM running the subscribe script that reads from the broker and inserts transactions into the Tangle. Therefore, this script is receiving the 60 bytes per second being published by the smart cars. All connected vehicles are displayed in this overview, totalling to five connected vehicles.

Figure 5 displays the queue that is created for the incoming and outgoing MQTT messages. The message rates per queue are defined here. For the queue used in our testbed scenario, all five ESP-32s are publishing messages every 2.6 seconds. The messages are then instantly delivered to the subscription script every 2.6 seconds also.

Figure 6 is a screen capture of a one hour time frame slot. The yellow line is the published messages and the green is the delivered ones. There are times of consistent traffic where data is being sent and received at the same rate. However, there are also fluctuations where data is not being sent by the devices, leaving no messages to be received in the queue by the subscription script. And contradictory to this, there are also times where more messages are being published than subscribed. Fluctuations in traffic can also be caused by data communication issues such as packet loss. This will have a direct impact on data flow when plotted on a graph. If messages aren't received by RabbitMQ, the devices are able to store them locally and retransmit when in the vicinity of another access point. How this correlates to a real world application is that vehicles will not be sending messages at a consistent rate, only when needed. For example, only when passing other vehicles or traffic structures. There could be instances where vehicles are in traffic causing an influx of transactions, a higher rate than being received at that moment in time. These messages will sit in a queue until ready to be processed and sent into the Tangle.

Figure 7 is a magnified view of a ten minute time slot. This better depicts the inconsistencies that exist when publishing and delivering messages. There are times when published and delivered messages are synced up together, and there are times where more messages are being published than delivered. Also important to note on figure 6 is the fluctuation of message rates in seconds. This could directly correlate to the current speed of travel on a particular route. The slower the travel in miles

Overview				Messages			Message rates			+/-
Name	**Type**	Features	**State**	**Ready**	**Unacked**	**Total**	**incoming**	**deliver / get**	**ack**	
mqtt-subscription-mqttjs_baeb4296qos0	classic	AD	running	0	0	0	2.6/s	2.6/s	0.00/s	

Fig. 5. Queue that the MQTT messages are being published and subscribed too.

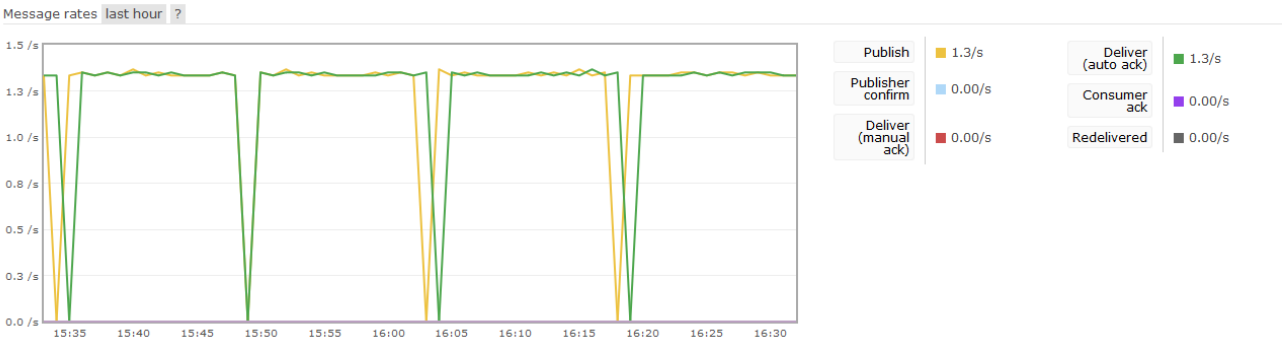

Fig. 6. One hour time slot capture of messages sent from IoT devices to the Tangle.

Fig. 7. Ten minute time slot capture of messages sent from IoT devices to the Tangle.

per hour, the slower the vehicles are reaching traffic structures to send HELLO pings.

C. Applying the ITS Threat Model

We apply the threat model to the implemented system by focusing on attack vectors that are rated high. Beginning with device attacks, focusing on cyber-enabled physical attacks. This attack method encompasses a wide range of security vulnerabilities that are present in cyber physical systems. An example of this attack would be changing a traffic light from red to green potentially sending vehicles into oncoming traffic. This would be a cyber-attack that had a physical outcome. Cyber-attacks could occur by a number of mechanisms including remote control of devices. Corresponding network and device attacks are both rated high for similar reasons, as they constiture possible entry points for a cyber physical attacker. However, within our testbed prototype remote over the air (OTA) updates have been disebled as a mitigation measure against efforts to deploy malevolent software.

Physical connectivity to exposed ports is an attack vector rated high due to the instantaneous repercussions that it can incur. In context to the PoC, if the ESP-32 micro USB ports are left exposed, someone with malicious intent would simply be able to upload malware code. This would compromise not only the device, but potentially the entire network. This links directly to network attacks of installing malware and uploading malicious firmware, which are both rated high. The prototype is currently exposed to these attacks. In a real world implementation of an ITS, all exposed ports must be safely secured to avoid such an attack. Permanent traffic structures must be securely locked and sealed to avoid break-ins, and there must be corresponding laws to deter malicious behaviour.

Distributed denial of service attacks performed on the DLT are a serious attack vector that DLTs do face. However, in the case of the Tangle, the bottleneck of transaction validation widens as the number of transactions increases rather than shrinks (as in typical Blockchains). This is due to the immense scalability the Tangle provides, rendering DDoS attacks less severe to our particular use case. This applies both to our

prototype and real world implementations.

VI. Conclusions & Future Work

Internet of Things has emerged as a key technological enabler for broader socio-technical and socio-economic paradigms, such as smart cities and Circular Economy. However, IoT systems are characterised by constraints and limitations which in order to be overcome they need to be deployed in conjunction and in synergy with other emerging ICT. Distributed Ledger Technologies can help overcome challenges pertaining to data immutability, data timeliness and data security. While several previous works have investigated the joint use of IoT and Blockchain by means of theoretical analysis and proposed architectures, not many implementations of such systems have been demonstrated mainly due to a conflict between the resource demanding Blockchains and the highly constrainted IoT devices. Furthermore, there is an identified gap in existing literature regarding IoT-specific threat models.

In this work, we addressed the aforementioned research questions via the prism of Intelligent Transport Systems. We considered systems that comprise both IoT and DLT technologies and elicited a three-tier threat model identifying attack vectors at the Device, the Network and the DLT layers. The identified attacks where then evaluated by using the DREAD ranking scheme. The use of the threat model was demonstrated on a novel proof-of-concept IoT networked system that makes use of the IOTA Tangle distributed ledger to store generated data by helping critically appraise the design of the system against the highest ranking attacks. Furthermore, the PoC system is among the first in the literature to demonstrate the synergy of IoT and DLT on actual constrained embedded devices; source code is available on Github [28].

In our future work we plan to address the topic of Digital Forensics in IoT systems. In particular, we will define a framework for the evaluation of the forensic readiness of IoT systems as well as a method for developing forensically ready IoT systems by leveraging the characteristics of DLT such as the IOTA tangle.

References

[1] Dread threat modeling: An introduction to qualitative and quantitative risk analysis. [Online]. Available: https://blog.eccouncil.org/dread-threat-modeling-an-introduction-to-qualitative-and-quantitative-risk-analysis/

[2] A. Morlet, J. Blériot, R. Opsomer, M. Linder, A. Henggeler, A. Bluhm, and A. Carrera, "Intelligent assets: Unlocking the circular economy potential," *Ellen MacArthur Foundation*, pp. 1–25, 2016.

[3] M. Geissdoerfer, P. Savaget, N. M. Bocken, and E. J. Hultink, "The circular economy–a new sustainability paradigm?" *Journal of cleaner production*, vol. 143, pp. 757–768, 2017.

[4] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with iot. challenges and opportunities," *Future generation computer systems*, vol. 88, pp. 173–190, 2018.

[5] A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an optimized blockchain for iot," in *2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI)*. IEEE, 2017, pp. 173–178.

[6] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "Blockchain: A distributed solution to automotive security and privacy," *IEEE Communications Magazine*, vol. 55, no. 12, pp. 119–125, 2017.

[7] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, "When mobile blockchain meets edge computing," *IEEE Communications Magazine*, vol. 56, no. 8, pp. 33–39, 2018.

[8] O. Novo, "Blockchain meets iot: An architecture for scalable access management in iot," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1184–1195, 2018.

[9] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and iot integration: A systematic survey," *Sensors*, vol. 18, no. 8, p. 2575, 2018.

[10] (2020) Following a wallet hack, the iota foundation hits turbulence. [Online]. Available: https://bravenewcoin.com/insights/following-a-wallet-hack-the-iota-foundation-hits-turbulence

[11] (2017) Cryptographic vulnerabilities in iota. [Online]. Available: https://medium.com/@neha/cryptographic-vulnerabilities-in-iota-9a6a9ddc4367

[12] (2019) Iota network down for 15 hours what happened? [Online]. Available: https://www.crypto-news-flash.com/iota-network-down-for-15-hours-what-happened/

[13] P. Aufner, "The iot security gap: a look down into the valley between threat models and their implementation," *International Journal of Information Security*, vol. 19, no. 1, pp. 3–14, 2020.

[14] A. Omotosho, B. Ayemlo Haruna, and O. Mikail Olaniyi, "Threat modeling of internet of things health devices," *Journal of Applied Security Research*, vol. 14, no. 1, pp. 106–121, 2019.

[15] N. Huq, R. Vosseler, and M. Swimmer, "Cyberattacks against intelligent transportation systems," *TrendLabs Research Paper*, 2017.

[16] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, "A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3453–3495, 2018.

[17] G. K. Rajbahadur, A. J. Malton, A. Walenstein, and A. E. Hassan, "A survey of anomaly detection for connected vehicle cybersecurity and safety," in *2018 IEEE Intelligent Vehicles Symposium (IV)*. IEEE, 2018, pp. 421–426.

[18] W. Wachenfeld, H. Winner, J. C. Gerdes, B. Lenz, M. Maurer, S. Beiker, E. Fraedrich, and T. Winkle, "Use cases for autonomous driving," in *Autonomous driving*. Springer, 2016, pp. 9–37.

[19] (2015) With 15 dollars in radio shack parts, 14-year-old hacks a car.

[20] (2015) Car hack uses digital-radio broadcasts to seize control (bbc). [Online]. Available: http://www.bbc.com/ news/technology-33622298

[21] (2016) Tesla driver dies in first fatal crash while using autopilot mode (the guardian). [Online]. Available: https://www.theguardian.com/technology/2016/jun/30/tesla-autopilotdeath-self-driving-car-elon-musk

[22] C. Miller and C. Valasek, "Remote exploitation of an unaltered passenger vehicle," *Black Hat USA*, vol. 2015, no. S 91, 2015.

[23] J. Petit, B. Stottelaar, M. Feiri, and F. Kargl, "Remote attacks on automated vehicles sensors: Experiments on camera and lidar," *Black Hat Europe*, vol. 11, no. 2015, p. 995, 2015.

[24] F. D. Garcia, D. Oswald, T. Kasper, and P. Pavlidès, "Lock it and still lose iton the (in) security of automotive remote keyless entry systems," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*, 2016.

[25] D. LeBlanc and M. Howard, *Writing secure code*. Pearson Education, 2002.

[26] A. A. Singh and K. S. Singh, "Network threat ratings in conventional dread model using fuzzy logic," *International Journal of Computer Science Issues (IJCSI)*, vol. 9, no. 1, p. 478, 2012.

[27] H. Hellani, L. Sliman, M. B. Hassine, A. E. Samhat, E. Exposito, and M. Kmimech, "Tangle the blockchain: Toward iota and blockchain integration for iot environment," in *International Conference on Hybrid Intelligent Systems*. Springer, 2019, pp. 429–440.

[28] (2021) Source code of the iota-its testbed. [Online]. Available: https://github.com/s5068096-A/IoTA-ITS-testbed

[29] Nodes. [Online]. Available: https://docs.iota.org/docs/getting-started/0.1/network/nodes

Appendix
DREAD Threat Model For ITS using IoT and DLT

TABLE II
ATTACKS AT THE DEVICE TIER AND THEIR EVALUATION ACCORDING TO DREAD.

Attack Vector	**Damage**	**Reproducibility**	**Exploitability**	**AffectedUsers**	**Discoverability**	**Rating**
Sniff traffic of network between device and backend	1	3	2	1	3	Medium
Information leak	2	2	2	3	2	Medium
Cyber-enabled physical attacks	2	2	2	3	3	High
Recover credentials from flawed firmware	2	3	3	3	2	High
Midification of devices and exploite them	3	2	3	3	2	High
Files delete of compromised ITS devices	3	1	1	2	3	Medium
Man-in-the-Middle attacks	2	2	2	3	1	Medium
Unauthorised access/ Unauthorised controlling of ITS devices	3	2	2	3	2	High
Infection by malware	3	2	2	2	2	Medium
DoS/DDoS attacks	3	3	3	2	3	High
Attacks on IoT-enabled transportation systems	2	2	2	2	2	Medium
Unavailable speed limitation sensors	2	1	2	2	2	Medium
Ransomware attacks/ infection of devices with ransomware	3	2	3	3	3	High
Exploitation critical devices	2	2	3	3	2	High
Localisation of vulnerable devices through Shodan	2	2	2	2	1	Medium
Remote control of devices	3	2	3	3	3	High
Physical connectivity to exposed ports	3	2	3	2	2	High
Using brute force or guessing credentials on a device	2	2	3	3	1	Medium
Exploitation of vulnerabilities in software, hardware	3	2	2	3	2	High
Sending improper commands to the controller	3	1	1	3	2	Medium
Discovery of topology	1	3	1	1	1	Low
Storage device connection loaded with malware to install	2	2	2	2	2	Medium
Sending fraudulent messages	3	2	3	3	3	High

TABLE III
ATTACKS AT THE NETWORK TIER AND THEIR EVALUATION ACCORDING TO DREAD .

Attack Vector	Damage	Reproducibility	Exploitability	AffectedUsers	Discoverability	Rating
Exploitation of network flow to connect to car WLAN	2	2	2	2	2	Medium
Connection to the CAN bus - remotely hijacking of vehicle	3	2	2	3	2	High
Reverse engineer CANSW to control several systems	2	2	2	2	2	Medium
Send crafted DAB data to compromise the infotainment	3	2	1	3	3	High
Troubleshooting DAB reception	2	2	2	1	2	Medium
Unauthenticated CAN access	2	2	2	2	2	Medium
Crack the WiFi preshared key/ control CAN	2	2	2	2	2	Medium
Sniff and analyse of sensors/devices	1	2	2	1	2	Medium
Remotely control of sensors/devices	3	2	2	3	3	High
Injection of old command to car system	2	2	2	2	2	Medium
Identification and abuse network misconfigurations	2	2	3	3	2	High
Exploitation of software/hardware vulnerabilities	3	2	2	3	2	High
Installing malware/spyware on systems	3	2	3	3	3	High
Install malicious firmware	2	2	3	3	2	High
SQL injection attacks	2	2	3	3	2	High
Abuse of weaknesses of authentication mechanisms	2	2	2	3	2	Medium
Inject of malicious software via ads banners	3	3	3	3	3	High
Cross-site scripting (XSS) attacks	3	2	2	3	2	High
Eavesdropping sensitive information	3	2	1	3	2	Medium
Lack of encryption/ poorly implemented encryption	1	2	2	3	1	Medium

TABLE IV
ATTACKS AT THE DLT TIER AND THEIR EVALUATION ACCORDING TO DREAD.

Attack Vector	Damage	Reproducibility	Exploitability	Affected users	Discoverability	Rating
Exploitation of embedded vulnerabilities	2	3	2	2	3	High
Distributed Denial-of-Service (DDoS)	3	3	3	2	3	High
Timestamp Hacking	3	2	2	3	2	High
Compromising centralised blockchain IOTA	3	2	2	3	2	High
Compromising users wallet	3	3	2	2	2	High
Sybil Attack	3	2	2	2	2	Medium
Eclipse Attack	3	2	2	2	2	Medium
Man-in-the-Middle (Address Attack)	2	2	2	3	1	Medium
Exploitation of smart contracts vulnerabilities	3	2	2	2	2	Medium
51% or Majority Attack	3	2	2	3	3	High
Selfish Mining	2	2	2	2	2	Medium
Routing Attack	2	2	3	2	2	Medium
Dictionary Attack	2	2	2	2	2	Medium
Alternative History Attack	3	2	2	3	3	High
Flawed Key Generation	2	2	1	3	2	Medium
Vulnerable Signatures	2	1	2	3	2	Medium