Security Issues in UAV-Based Infrastructure Monitoring

Francesco Buccafurri
Full Professor
DIIES Dept., University Mediterranea of Reggio Calabria
bucca@unirc.it

Francesca Scoleri
Master graduate at
DIIES Dept., University Mediterranea of Reggio Calabria
francesca.scoleri1@gmail.com

Abstract

Infrastructures can be monitored by using complex IT architectures involving also the usage of UAVs. UAVs may operate by forming ad-hoc networks and may be integrated with advances sensors, like *LIDAR (Light Detection and Ranging)* to build a digital model of the infrastructure. Starting from a previous experience of application of this approach to monitoring road infrastructures, in this paper, we analyze the security issues of such approaches, by identifying three categories of attacks, namely (1) *attacks on routing*, (2) *attacks on measurements*, and (3) *UAV impersonation*. For all these attacks, we identify a possible trust-based approach to mitigate the risk. This kind of approach allows us to improve the resilience of the system and can be combined with standard cybersecurity protection mechanisms.

Keywords

Cybersecurity; UAVs; Trust, Blockchain; Critical Infrastructures.

1. Introduction

The adoption of *Unmanned Aerial Vehicles* (UAVs) for infrastructure monitoring is an emerging approach allowing us to improve the quality, the effectiveness, the continuity, and the affordability of monitoring activities. UAVs can be integrated with advances (passive or active) sensors capable of retrieving accurate measures describing the status of the infrastructure, and can be part of a complex IT system that leverage the UAVs to build a *Wireless Sensor Network* (WSN) referring to a *Base Station* (BS) which measures are continuously sent.

Among other infrastructures, this paper focuses on road infrastructures, by leveraging a preliminary study conducted in Scoleri (2016), in which UAVs are used to implement the monitoring task.

Analysis of degradation evolution of road pavements must ensure road safety. Degradation evolution causes increased rehabilitation costs. A high-velocity survey of the road network is necessary to estimate hazardous conditions and maintenance scheduling, and to detect the progress of portions of the infrastructure that are often difficult to reach. A systematic approach to pavement management is necessary to provide effective characteristics of pavement deterioration and its evolution over time. The goal of preventive maintenance is not limited to the elimination of critical issues, but is geared toward the identification of solutions that ensure adequate effectiveness over time and durability of solutions. Pavement consists of a succession of layers with different mechanical and physical characteristics. Several types of road superstructures can be listed: flexible (friction layer, binder layer, base layer, unbound base layer, subgrade), semi-rigid (as above, but with a cement-treated base layer), and rigid (concrete slab resting on one or more layers). The phenomenon of *fatigue* is one of the main causes of pavement structure deterioration. Read (1996) proposed the following definition, "Fatigue in asphalt pavements is the phenomenon of cracking. It consists of two main stages, initiation and propagation, and is caused by tensile deformation generated not only by traffic-induced loading, but also by temperature variations and construction procedures." A road pavement

management system is described as a systematic approach that provides the technical and economic analysis tools needed to choose the best maintenance, rehabilitation, and reconstruction strategies for the road network.
As shown in Scoleri (2016), to provide an effective survey of road distress, it may be useful to obtain adequate photographic documentation provided by drone navigation in the airspace of the site under analysis. A post-processing phase is usually necessary.

This is decisive in the case of bridge deck inspections, to reach heights of more than 300 m above the ground and close-up shots in a few seconds, without creating dangerous situations for operators. This type of monitoring allows high-quality images to be obtained with less logistical effort and shorter duration.
An important innovation, which can facilitate the characterization of the road network and its surroundings is the adoption of UAVs, which represent the latest frontier for high-resolution, low-altitude filming, thanks to the development and deployment of increasingly specialized and geometrically higher-performance sensors that make remote sensing a continuously innovating research segment.

The methodology proposed in Scoleri (2016) concerns the use of lightweight UAV technologies to reduce cost and computational load. Several types of aircraft can be listed in the category of micro-UAVs: quadricopter (4 propellers), six rotors (6 propellers), eight rotors (8 propellers). The driving modes are as follows:
Visual flight, which allows the sensors to be carried using radio control up to a maximum of about 250 meters from the operator. Most suitable in confined and accessible areas (archaeological site, landfill site, road junction);
FPV flight (an acronym for First Person View, flying in first person), allows an approach to the target to be detected because the pilot is carried by a visor that receives images directly from a camera on the aircraft. Used in morphologically complex and hazardous areas;

Autonomous flight, provides maximum safety over long distances. The flight route is preset and the position of the aircraft is controlled either by the on-board GPS or an alternative system. In the field of road maintenance, the use of a thermal imaging camera_is useful in detecting pavement characteristics subject to water infiltration or stagnation, resulting in both the evolution of road surface degradation and the loss of grip in the wheel-pavement contact and, therefore, the reduction of road safety. A thermal imaging camera then records the intensity of radiation in the infrared part of the electromagnetic spectrum and converts it into a visible image. After the completion of the road movie, it moves on to the detailing phase through the use of dedicated software, which allows the selection, acquisition and storage of images and subsequent processing. In Figure 1, the architecture of the solution proposed in Scoleri (2016) is reported.

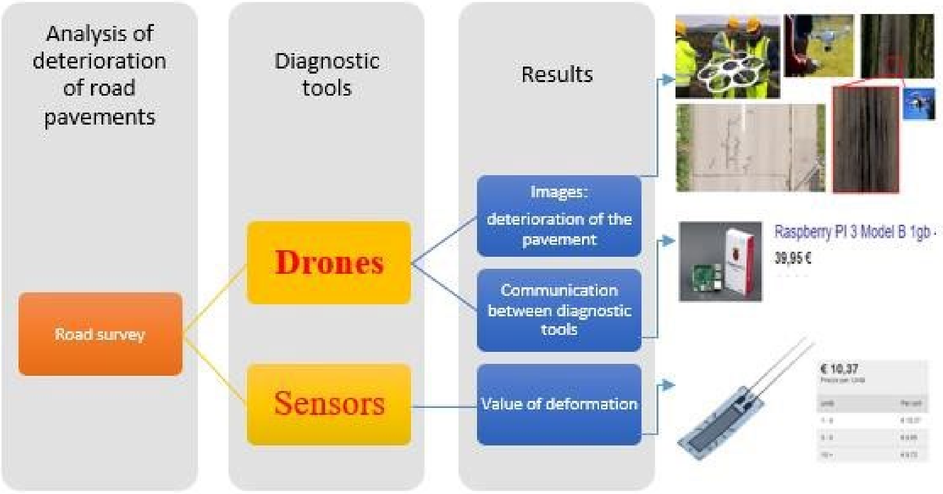
Analysis of deterioration of road pavements
Diagnostic tools
Results
Road survey
Drones
Sensors
Images: deterioration of the pavement
Communication between diagnostic tools
Value of deformation
Raspberry PI 3 Model B 1gb -
39,95 €
€ 10,37

Figure 1. *UAV-based architecture for road infrastructure monitoring.*

The practical architecture proposed in Scoleri (2016) is based on the integration of innovative methods of road surface deterioration detection and analysis. Such a system provides support for road asset management. In this context, the

main tools of infrastructure deterioration, UAVs and sensors, become strategic elements that can facilitate road maintenance phases. As far as this application is concerned, telecommunication systems are crucial.
This is even more interesting when considering the possibility of monitoring without affecting the operation of the road network and monitoring roads while ensuring the continuity of flows and compliance with vehicle safety conditions.

The objective of this paper is to study some security issues of the solution presented in Scoleri (2016). Specifically, the paper aims to contrast the problem of the possible compromise of UAVs by an attacker, which jeopardizes the monitoring process. The relevance of this threat model in the considered scenario is strictly related to the critical activities for which UAVs are employed.

2. Literature Review

UAVs were originally designed, manufactured, and used for military applications. With the development of aviation, civilian use of drones is now quite common: their flexibility, lack of serious accidents, and relatively low cost have been appreciated. The majority of drones are used in the following activities: monitoring, photogrammetry, precision agriculture, meteorology, disaster response, transportation of medicines in distressed areas, control of illegal buildings, filming of sporting events, archaeology (Martínez et al. 2015), accident inspections, border control, and prevention/observation/remediation of the effects of natural causes (fires, floods, earthquakes) (Cilona et al.; 2016) in addition, traffic surveillance is an important issue in urban planning and monitoring (Saleem et al., 2016). Drones are also used to conduct three-dimensional environmental surveying (Hien, 2016).

Sensor networks are a distributed platform for the collection, fusion, and aggregation of data related to an observed process, regardless of its geographic extent. Sensors can generate innovation in the IoT (an acronym for "Internet of Things," a neologism referring to the global Internet's extension of concrete objects and places) and are also of great interest to commercial companies. This architecture replaces wiring: a sensor network consists of a number of small sensor nodes that are densely distributed in or very close to the area to be analyzed. The nodes detect changes in relation to certain parameters or events and communicate them to other devices. They can also be used in areas that are poorly accessible or inaccessible.

A wireless sensor network (WSN) is a specific type of network, characterized by a distributed architecture. It comprises a set of autonomous electronic devices (such as sensors) that can collect data from their surroundings and communicate with each other. Each sensor node can be used in different modes: a sensor can be interrogated periodically to obtain continuous information, to verify that a specific condition has been reached, or in hybrid mode, where a physical quantity is monitored periodically and, if it exceeds a certain threshold, the sensor can directly alert the controller. An ad-hoc network is a set of devices located in a limited area that are able to communicate with each other wirelessly. Ad-hoc networks can be mainly of two types: *pure* or *hybrid*. The first case represents a group of randomly arranged, potentially free-to-move, independent terminals that communicate with each other; the second case represents a system similar to the previous one, but in which one or more nodes are connected to a cellular or wired system. One advantage of this type of network is that terminals can act not only as end systems (transmitters or receivers), but also as relay (i.e., intermediate nodes) that forward data packets when the transmitter and receiver are unable to communicate directly. As we will see later, this fact can be a source of insecurity.

Ad-hoc networks can be subject to malicious activity. Possible attacks are: node capture, physical tampering of the node, spoofing (an attack that employs identity forgery in various ways), sniffing (passive interception of data passing through a computer network), DoS "denial of service" (a malfunction due to a cyber attack). Specifically, an attack such as DoS aims to consume the resources of one or more network nodes by sending false messages so that the attacked node initiates energy- and time-consuming operations. A routing protocol (Ching et al. 2021) determines a path between two network nodes that do not have the ability to communicate directly with each other. In ad-hoc networks, nodes must be able to organize themselves independently and determine routes to the base station. AODV (Ad-hoc On-demand Distance Vector) is a protocol designed for ad hoc networks that builds routes only when they are actually needed. For this purpose, AODV sends a route request packet (RREQ) to the network that the recipient node can store and use as a route to reach the source node of the RREQ packet. The recipient of the request responds with a Route Replay (RREP) packet that, thanks to the information acquired by the nodes during the propagation of the request, returns to the source by creating and storing a communication path between the two nodes. A more general

overview on routing protocols for UAVs and vehicular networks can be found in (Nazib et al. 2021). A comprehensive survey on various technological aspects regarding UAVs can be found in (Sharma et al. 2020).
Our paper is also related to the application of trust to UAVs networks. This is an emergent topic in the field of vehicular networks in general. Hbaieb et al. 2022, claim that the advent of the emerging technologies like blockchain, cloud, SDN as well as artificial intelligence bring new opportunities to propose more relevant approaches within the trust management mechanisms within the IoV context.

3. Improving the Resilience of the UAV-based Solutions: a Trust-based Model

In this paper, the considered security issues are mostly contrasted by using trust-based approaches. We organize this section by splitting it into two subsections. The first subsection identifies the main threats affecting trust-based mechanisms. The second subsection presents the security issues of the UAV-based monitoring solution and how we can apply countermeasures to mitigate them.

3.1. Attacks on Trust-Based Systems

In this section, we recall the main attacks on trust-based systems, on which our proposal operates.

Self-Promoting attacks (Hoffman et al. 2009), concerning the possibility that an entity promotes itself by means of fake actions aimed to increase trust. Typically, such attacks are contrasted by excluding that mechanisms able to increase trust exist, but only mechanisms aimed to decrease the trust of involved parties. This solution is not applicable in every case because, sometimes, the existence of ways to increase the trust of some entities is necessary in the specific application domain.

Slandering attacks (Hoffman et al. 2009), which aim at falsely decreasing the trust of other entities. For example, in human-based trust systems, when trust is calculated on the basis of positive or negative feedbacks that (human) clients provide about service providers, slandering attacks may be performed by competitors, even in absence of transactions between the client and the service provider. While trust-systems with no mechanism capable of increasing trust often exist, to decrease trust is in general necessary to isolate the malicious behavior of compromised entities.
Both self-promoting and slandering attacks can be amplified by proliferating fake entities, and using these fake entities to deceive the community.

This kind of attack is called **Sybil attack** (Douceur, 2002). A sybil attack generates interaction between fake entities to compromise the trust-system.
Finally, **Whitewashing** attacks (Hoffman et al. 2009), exploit the difficulty to establish peer identities: in this case, an entity, which wasted his trust value, creates a new identity to change its trust to the default initial value.

3.2. The Proposed Trust Model

Among the technologies described earlier, we consider the application of active sensors of type LIDAR (Light Detection and Ranging) on board of UAVs forming an ad-hoc network using the protocol AODV for routing packets to the base station. The UAV network allows us to build a digital model of the real-life environment.
In this section, we describe the main security arising in the UAV-based architecture, we identify possible detecting methods, and countermeasures. They are also based on a trust model assigning to each UAV a trust value obtained as the product of three components (both ranging from 0 to 1), i.e., the *routing trust* T_r, the *measurement trust* T_m, and the *identity trust* T_i.

More in detail, we the main elements of our model are

1) A set of UAVs *U*,
2) The WSN of UAVs
3) The Base Station BS
4) The masurements sent by UAVs to BS, each represented by a tuple $m=\langle u,v,t,trust(m)\rangle$, where, *u* is the UAV responsible for the measurement *m*, *v* is the value of *m*, *t* is the timestamp of the measure, and *trust(m)* is the trust associated to the measure. The function trust is obtained as a sum of three components, i.e.:

$$trust(m) = T_r \cdot T_m \cdot T_i$$

The way the three components of the trust are computed is illustrated below. The function *trust* is at the basis of the *tolerance-based* approach we propose. *Tolerance* is a way to manage cybesecurity attacks. It means that we have not the ambition of detecting with certainty the attack in real-time, containing it, eradicating it and recovering the system at the pre-attack stage. Tolerance is a way to allow the continuity of the IT system also in presence of the cyberattack. It is a form of *resilience* of the system, but it can be adopted if the system embeds a sufficient degree of redundancy, in such a way that the function played by the attacked subsystem can be replaced by other subsystems. Moreover, we have to guarantee that the attacked subsystem cannot harm the whole system. Thus, that no *lateral movements* are possible for the attacker and the weight of the function played by the attacked sub-system is reduced. This reduction should be proportional to the compromision degree of the subsystem. The trust-based approach allows us to implement this principle.

In our setting, we use the trust of every measure to wheight the measurement caming from UAVs. Therefore, the digital model of the infrastructure, at time t, can be formalized as:

$$d(t) = f((trust(m_1) \cdot v_1), \dots, (trust(m_k) \cdot v_k))$$

where the function *f* is applied to all the measurements received at time *t*, each weighted with the corresponding trust value.

In the following, we focus on the three components of the trust function.

4. Routing Trust

A first issue we have to consider regards the ad-hoc network. In particular, an attacked UAV **may perform a sinkhole attack**, in which the attacker convinces legitimate nodes to route their packets through a malicious node. When this attack succeeds, the malicious node is able to attract all the traffic (or a relevant portion of the traffic). Therefore, it can launch further attacks, such as tampering or dropping packets sent by legitimate nodes. To successfully perform a sinkhole attack, a malicious node pretends to guarantee a high-quality route with reference to the routing protocol in use. As mentioned earlier, the most common WSN routing protocols (e.g., AODV) do not provide defense mechanisms to this kind of attack. In general, we can say that AODV is not designed with security in mind. Therefore, legitimate nodes generally receive only the advertised routes and no security check is performed on them. Next, the quality of the advertised route is compared with the quality of an already known route (if any). Therefore, if an old path is replaced with a forged path (received from a malicious node), the attack succeeds.

We better describe the sinkhole attack by means of the following example:

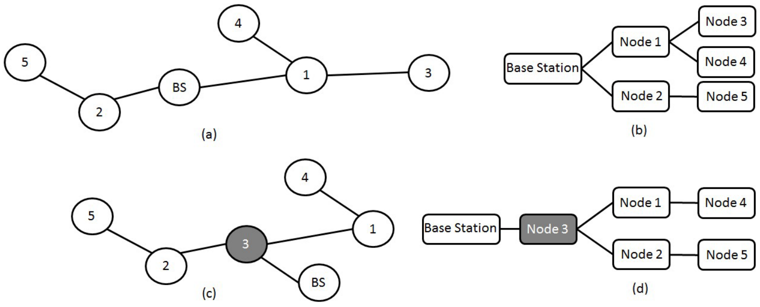

Figure 2. *Phases of a sinkhole attack: (a) A WSN where nodes are not compromised, (b) The hierarchy of routing data towards BS, (c) The WSN state when the attack is successfully performed by node 3, (d) The hierarchy of routing data as obtained by the sinkhole attacker through forged packets.*

1. Initially, the network is composed of only legitimate nodes (Figure 2.(a)).
2. Each node establishes its routing table according to the AODV routing protocol. The tree in Figure 2.(b) represents the routes established by nodes to reach the BS in case of absence of attack. In the figure, each node has chosen the closest node to the BS to route packets directed to the BS itself. For example, node 3 is a leaf of the routing tree since it has the lowest quality link to the BS.
3. Suppose now that a legitimate node is compromised. The sinkhole attack is launched.

4. The compromised node requires a route to a given destination node.
5. The compromised node sends a forged response to the previously sent request. The objective of this message is to falsely advertise a high quality route to the same destination as the previous step. This deceives the neighboring nodes, which might choose to replace their older route with the new advertised route (crossing the compromised node).

Figures 2.(c) and 2.(d) show an example of topology and routes established after a successful sinkhole attack. In the example, node 3 is a legitimate node that is compromised by an attacker and so it forges information about the quality of its link from the BS. After the attack succeeds, any packet can be compromised by node 3 since all packets are forwarded through that node. In this way, more severe attacks can be launched on the target system.

A method to contrast the first problem is to include in the system a trust-based layer enhanced architecture designed to tolerate intrusion attempts. In this context, by tolerance we mean the capability of the WSN to keep providing the service it is intended to even when a malicious entity compromises successfully a legitimate WSN node and then routing attacks occur in the network. The proposed solution allows us to improve resilience to cyber-attacks by incurring in little overhead in terms of additional messages exchanged between WSN nodes.

In our case trust can be measured collaboratively, by each node of the WSN, namely each UAV, by periodically asking their neighbors about routing quality measures, and testing them through alternative paths and/or measuring roundtrip times. This can be used to manage the routing trust and to allow UAVs to decrease the value T_r for UAVs for which the test fails. As T_r is used as a multiplicative factor of the choice function used by the AODV protocol for route selection, this way, the UAV is not chosen anymore so that it cannot harm the routing mechanism. However, when a node is detecting as possible actor of a sinkhole, also its measurement trust T_m is decreased. As T_m is used as multiplicative factor of the function used to build the digital model of the infrastructure, the more the UAV is suspected to be malicious, the less its contribution can harm the whole model. In this case, we are not aware of a malicious behavior of the UAV regarding its measurement task, but only regarding the routing task. Anyway, we can assume that the UAV is compromised. Therefore, a general malicious behavior can be expected.

5. Measurement Trust

Another possible malicious behavior is that a UAV, while behaves well in the routing task, **sends false measures to the BS**. This risk can be counteracted by organizing the flight of the UAV fleet in such a way that each UAV autonomously attempts to join the position of another UAV for an interval of time called join time, and then moves on to other positions. In other words, periodically, each UAV approaches other UAVs and interrogates them about the measurements it is taking, sending the base station the answer. The network then collaboratively performs a test of the veracity of the information the different UAVs send to the BS thus enabling it to update the measurement trust values of individual UAVs. This way, T_m is calculated.

Another kind of attack to measurement may regard the service provider itself. Consider that both monitoring and maintenance of the infrastructure could be contracted out to an outside firm by the government entity that owns the infrastructure. The firm might have an advantage in hiding the degraded state of some component in order to avoid additional maintenance costs. In this attack, then, the adversary is the service provider (not just UAVs attacked by an external attacker). In this case, the UAVs provide the correct measurements to the BS, but the back-end elaboration performed by the service provider tampers data in such a way that the resulting digital model of the infrastructure does not highlight elements that the service provider wants to hide to the government entity. We call this attack: *all-is-well attack.*

A way to contrast this attack is to use the blockchain technology, which is widely applied nowadays to the context of Internet of Things (Wang et al., 2019). In this case, the property we want to exploit of the blockchain technology is its immutability and, thus, the possibility of notarizing information on it. We mainly refer to public blockchains (like Bitcoin or Ethereum), but also permissioned blockchains can be used, by properly establishing a consortium among parties with conflicting interests, like, in this case, a number of companies operating in the context of the monitored infrastructure and a number of government entities, also not directly involved in the specific contract. According to our approach, all the measurements, suitably collapsed periodically into batches of information and compressed via cryptographic hashes, are stored into the blockchain, in such a way that they can be exposed as forensic evidence in case of legal dispute.

6. Identity Trust

The last problem we consider in this paper is **impersonation**. Obviously, classical authentication techniques can be used to contrast this problem, possibly based on challenge-response-based and cryptographic mechanisms.
UAV networks, concerning identification of peers, may suffers from various attacks such as *forgery attack*, *man-in-the-middle attack* and *reply attack*. All these attacks can be prevented if identity authentication is strong. Therefore, identity authentication is a fundamental task to perform in secure and reliable way before the drones start to communicate with each other. A problem is that standard cryptographic mechanisms such as RSA-certificate based authentication mechanisms require appreciable resource computation, which is, instead, very limited in the case of UAVs. Lightweight identity authentication methods, possibly based on ECC (*Elliptic Curve Cryptography*) (Teng et al. 2019) or on intelligent approach (Jiang et al. 2020) are thus welcome.
However, we cannot exclude that the attacker is able to compromise the computer system on board of the UAV to the extent that it is able to access any secret stored in it. Therefore, even very robust standard authentication mechanisms can be successfully used by the attacker without impersonation being able to be detected by either the other nodes in the network or the BS.

A way to mitigate this risk is to work on the basis of a trust-based approach. This is accomplished in our trust model by including the component T_i (identity trust), playing as a multiplicative factor of the function used to build the digital model of the monitored infrastructure, as for the component T_m. The identity trust is managed and updated on the basis of a machine learning (ML) approach. This is done by equipping both the UAVs and the BS of a ML model, which learns, in the cold state of the system, the behavior of each UAV. The global model is kept by the BS, but its update is done incrementally by using a federated-learning approach by using updates sent by the single UAVs. We prefer to update the global model via local models (thus, using federated learning) to allow the model to capture a global view of UAVs. This global view takes into account both the hierarchical behavior (i.e., the behavior regarding the interaction of the UAV with the BS) and the social behavior (i.e., the behavior regarding the interactions among UAVs in the network). Obviously, we expect correlation between the decreasing of the routing trust and the decreasing of the social component of the identity trust, due to the anomalous social interaction occurring when the routing test fails.

The usage of federated learning opens to possible malicious attempts of UAVs. As, in this case, no problems of privacy arise, the only possible attack is and *adversarial attack*. In this case, one UAV, possible colluding with other UAVs aims to deceive the global model. An attack like this is called *free-rider attack* (Fraboni et al. 2021), in which the attacker collaborates to the global ML model just by sending fake updates. Also adversarial attacks like the free-rider attack can be contrasted by using, in turn, trust-based approaches.
In the Table 1, we report the main features of the approaches used for the computation of the three components of trust.

Table 1. *Main features of trust computation*

	Collaborative	**Test**	**Blockchain**	**ML-based**	**Crypto**
Routing	✓	✓	✗	✗	✗
Measurement	✓	✓	✓	✗	✗
Identity	✓	✗	✗	✓	✓

7. Conclusion

In this paper, we highlight a number of possible security issues and innovative countermeasures in a UAV-based infrastructure monitoring system. In particular, we considered attacks on routing, attacks on measurements, and UAV impersonation. For each attack, we identity a strategy to contrast and mitigate the corresponding risk. The proposed strategies are trust and blockchain based. Due to the vastness of the topic, and by considering the aim of this paper, we chose to provide a horizontal view of issues and countermeasures, instead of focusing on some vertical problems. As a consequence, solutions are only sketched, and a deep implementation and validation of them is left to future work. As a conclusive consideration, we highlight two important aspects. The first is that the threat model we consider is very realistic, by considering the specific application domain. Indeed, infrastructures may be typically critical infrastructures of a country. Therefore, they can be target for attacks coming from state-sponsored, criminal or terroristic hacking organizations. Suppose for example that the infrastructure we are monitoring is a road infrastructure (like the case by which this paper takes inspiration). In this case, a cyberattack might be launched in coordination with a physical attack to the infrastructure (a bridge, for example), to masquerade the physical attack and then maximize the damage to people and environment. The second consideration, is that even though the issues discussed in this paper are somewhat orthogonal to the specific domain of interest, we tried to contextualize them, thus making the proposal effective. As an example, the *all-is-well attack* is tailored to the application-domain scenario.

References

Ching, T. W., Aman, A. H. M., Azamuddin, W. M. H., Sallehuddin, H., & Attarbashi, Z. S.. Performance analysis of internet of things routing protocol for low power and lossy networks (RPL): energy, overhead and packet delivery. In *2021 3rd International Cyber Resilience Conference (CRC)* (pp. 1-6). IEEE, 2021.

Cilona, A., Aydin, A., Likerman, J., Parker, B., & Cherry, J. Structural and statistical characterization of joints and multi-scale faults in an alternating sandstone and shale turbidite sequence at the Santa Susana Field Laboratory: Implications for their effects on groundwater flow and contaminant transport. *Journal of Structural Geology*, *85*, 95-114, 2016.

Douceur, J. R. The sybil attack. In *International workshop on peer-to-peer systems* (pp. 251-260). Springer, Berlin, Heidelberg, 2002.

Fraboni, Y., Vidal, R., & Lorenzi, M. Free-rider attacks on model aggregation in federated learning. In International Conference on Artificial Intelligence and Statistics (pp. 1846-1854). PMLR, 2021.

Krstovski, S., Quality index, www.ieoociety.org/newsletter/. Accessed May 21, 2020.

Hbaieb, A., Ayed, S., and Chaari, L. A survey of trust management in the Internet of Vehicles. Computer Networks, 203, 108558, 2022.

Hien, W. N. Urban heat island research: Challenges and potential. *Frontiers of Architectural Research*, 2016.

Hoffman, K., Zage, D., & Nita-Rotaru, C. A survey of attack and defense techniques *for reputation systems. ACM Computing Surveys (CSUR), 42(1), 1-31*, 2009.

Jiang, C., Fang, Y., Zhao, P., & Panneerselvam, J. Intelligent UAV identity authentication and safety supervision based on behavior modeling and prediction. IEEE Transactions on Industrial Informatics, 16(10), 6652-6662 , 2020.

Lee, J., Measurement of machine performance degradation using a neural network model, *International Journal of Modelling and Simulation*, vol.16, no. 4, pp. 192-199, 1996.

Martínez, S., Ortiz, J., Gil, M.L., Geometric documentation of historical pavements using automated digital photogrammetry and high-density reconstruction algorithms, *Journal of Archaeological Science*, Vol. 53, pp 1-11, 2015

Nazib, R. A., & Moh, S. Routing protocols for unmanned aerial vehicle-aided vehicular ad hoc networks: A survey. IEEE Access, 8, 77535-77560, 2020.

Read, J. M. *Fatigue cracking of bituminous paving mixtures* (Doctoral dissertation, University of Nottingham), 1996.

Saleem, Y., Rehmani, M. H., & Zeadally, S. Integration of cognitive radio technology with unmanned aerial vehicles: issues, opportunities, and future research challenges. *Journal of Network and Computer Applications*, *50*, 15-31, 2015

Scoleri, F., Advanced application architecture for road infrastructure monitoring and management, *Thesis of the master degree in transportation engineering*, DIIES Dept., University of Reggio Calabria (Italy), 2016.

Sharma, A., Vanjani, P., Paliwal, N., Basnayaka, C. M. W., Jayakody, D. N. K., Wang, H. C., & Muthuchidambaranathan, P. Communication and networking technologies for UAVs: A survey. Journal of Network and Computer Applications, 168, 102739, 2020.

Teng, L., Jianfeng, M., Pengbin, F., Yue, M., Xindi, M., Jiawei, Z., Gao, G, and Di, L. Lightweight security authentication mechanism towards UAV networks. In 2019 International Conference on Networking and Network Applications (NaNA) (pp. 379-384). IEEE, 2019.

Wang, X., Zha, X., Ni, W., Liu, R. P., Guo, Y. J., Niu, X., and Zheng, K. Survey on blockchain for Internet of Things. Computer Communications, 136, 10-29, 2019.

Biographies

Francesco Buccafurri is a full professor of computer science at the University Mediterranea of Reggio Calabria, Italy. In 1995 he took the PhD degree in computer science at the University of Calabria. In 1996 he was visiting researcher at the database and knowledge representation group of Vienna University of Technology. His research interests include cybersecurity and privacy, social networks, deductive-databases, knowledge-representation and nonmonotonic reasoning, model checking, data compression, data streams, agents, P2P systems. He has published more than 160 papers in top-level international journals and conference proceedings. He serves as a referee for international journals and he is a member of a number of conference PCs. Francesco Buccafurri is Associate Editor of Information Sciences (Elsevier) and IEEE Transactions on Industrial Informatics, he is included in the editorial board of a number of other international journals, and played the role of PC chair and PC member in many international conferences. He is member of the IEEE computer society.

Francesca Scoleri took the Bachelor degree in Civil Engineering in 2014 at University Mediterranea of Reggio Calabria. Then, in 2016 she took the Master (first-level) degree in transportation engineering, defending a thesis on IT-based road infrastructure monitoring. She is currently high-school professor of Physic.