Mobile Networks and Applications (2019) 24:881–889
https://doi.org/10.1007/s11036-018-1146-4

Crowdsourcing Analysis in 5G IoT: Cybersecurity Threats and Mitigation

Ana Nieto[1] · **Antonio Acien**[1] · **Gerardo Fernandez**[1]

Published online: 4 October 2018

Abstract
Crowdsourcing can be a powerful weapon against cyberattacks in 5G networks. In this paper we analyse this idea in detail, starting with the use cases in crowdsourcing focused on security, and highlighting those areas of a 5G ecosystem where crowdsourcing could be used to mitigate local and remote attacks, as well as to discourage criminal activities and cybercriminal behaviour. We pay particular attention to the capillary network, where an infinite number of IoT objects coexist. The analysis considers the different participants in a 5G IoT ecosystem.

Keywords 5G security · Proactive security · Cybersecurity · Digital witness

1 Introduction

The main objective behind crowdsourcing is to pose a problem to a participative community, willing to resolve the challenge, after which they expect a reward [7]. This idea has been applied to the *Internet of Things* (IoT) context in several ways, through users and their IoT devices, for very diverse purposes (i.e. Section 3). However, it has not yet been sufficiently discussed how these features can help mitigate the effect of cyberattacks in truly complex networks. These are severely exposed due to the wide array of technologies at different levels of abstraction, as is the case of the fifth generation of cellular networks (5G).

Considering that the 5G IoT is the ecosystem formed by 5G including the IoT context, in this paper we discuss how crowdsourcing could help stop or mitigate the effect of attacks in 5G IoT, when applied at different levels, considering the participants involved (users, infrastructure and service providers) as crowds.

This paper is motivated by the rapid expansion of 5G technologies and the slow adaptation of IoT devices to these changes. It is unrealistic to think that IoT devices will be more secure when 5G networks are fully deployed, or to trust 5G technologies (c.f. Section 2) to solve IoT security problems on their own. Instead, in this article we adopt a different point of view: since the IoT devices will introduce numerous security problems, it is necessary to provide cooperation mechanisms so that the data of these devices can be used for the detection and mitigation of threats. This additional overhead would be acceptable for 5G networks, but the sources (crowds) have to be convinced to cooperate.

The concept of crowdsourcing links these two worlds naturally, by defining interests for participants—users and providers—to motivate the mutual cooperation in order to stop cybercrime.

The paper is structured as follows. Section 2 describes the new context introduced by 5G IoT. Section 3 discusses a set of use cases for crowdsourcing and how these can evolve towards cybersecurity in 5G. Section 4 analyses the areas in 5G that could harness crowdsourcing for cybersecurity. Based on these results, Section 5 introduces a model to analyse the use case of end-user collaboration considering a native solution for IoT. Section 6 shows preliminary results about how a witness-based mechanism can contribute to mitigate the effect of attacks based on the proximity of the offender to the victim. Finally, Section 7 concludes the paper.

✉ Ana Nieto
nieto@lcc.uma.es

Antonio Acien
acien@lcc.uma.es

Gerardo Fernandez
gerardo@lcc.uma.es

[1] Ada Byron Research Centre C/ Arquitecto Francisco Peñalosa, no 18 Ampliación Campus de Teatinos, Universidad de Málaga, 29071 Málaga, Spain

2 5G and the Internet of Things (IoT)

One of the most notorious changes introduced in 5G is the massive use of software-defined networks (c.f. Fig. 1). In particular, there will be three fundamental parts in a 5G environment that will be defined by software, increasing the flexibility of the cellular network: network slices, the communication infrastructure and network functions.

Network slices are defined based on *specific use case requirements*, but using shared (network) resources. The IoT is considered an important use case in 5G [1, 14, 18], for which specific slices should be defined. IoT network slices have to consider the resource-constrained nature of the devices and other requirements related to the specific purpose of the network slice (e.g. e-home, industrial IoT). Therefore, the need for the network to provide special coverage for IoT objects is clear. Nevertheless, how IoT objects will be adapted to this contextual change, in particular to not be a threat to the infrastructure, is still an open challenge. Moreover, while the proliferation of attacks is affecting to the current, deployed cellular networks, in 5G the problem is even more worrisome, since the speed improvements in the communications also allow a more efficient diffusion of the attacks, and the software layers are intrinsically related.

In addition, the communication infrastructure will be defined by software, which means a higher decoupling between software (control decisions) and hardware (network devices). One of the open challenges in 5G is how to implement a *Dynamic Radio Access Network* (DyRAN), which will allow the *mix of generic 5G services*, enabling real-time decisions about the access of the devices to the network based on the service requirements. Note that behind this technology there are management decisions which affect (shared) network resources. Therefore, controlling misbehaviour in this vulnerable part of the network will be essential to avoid resource starvation. The lack of responsibility for these actions is a clear problem in the IoT [11], which, in turn affects 5G networks.

An important feature in 5G is to make use of *Device-to-Device* (D2D) communication to increase the coverage of the network, for example, using *network relays* [13]. Therefore, in a cellular network, D2D communications will be typical in the capillary network (due the functionality of IoT devices and mobile platforms), but also as part of the infrastructure in order to work. This opens the door to a new set of vulnerabilities and attacks that can be propagated hop by hop to reach a vulnerable device from which critical parts of the infrastructure can be accessed (e.g., software controllers). As is throughly described in the latest ENISA 5G security report [1], SDN controllers are vulnerable to attacks against the communication APIs used between the controllers and also between the controllers and the SDN elements that will be close to the user.

Note that a marked difference in 5G compared to previous generations, is the need to bring the technology to the user. Thus, hot topic movements such as *Mobile Edge Computing* (MEC) will bring the Cloud closer to the capillary network of devices. This will bring about, in addition to improvements in performance, improvements in data management to exploit the architectural changes. Therefore, 5G environments will be better prepared to work with *massive data from the capillary network*. This is a crucial factor that will make 5G environments much better prepared than their predecessors for crowdsourcing solutions.

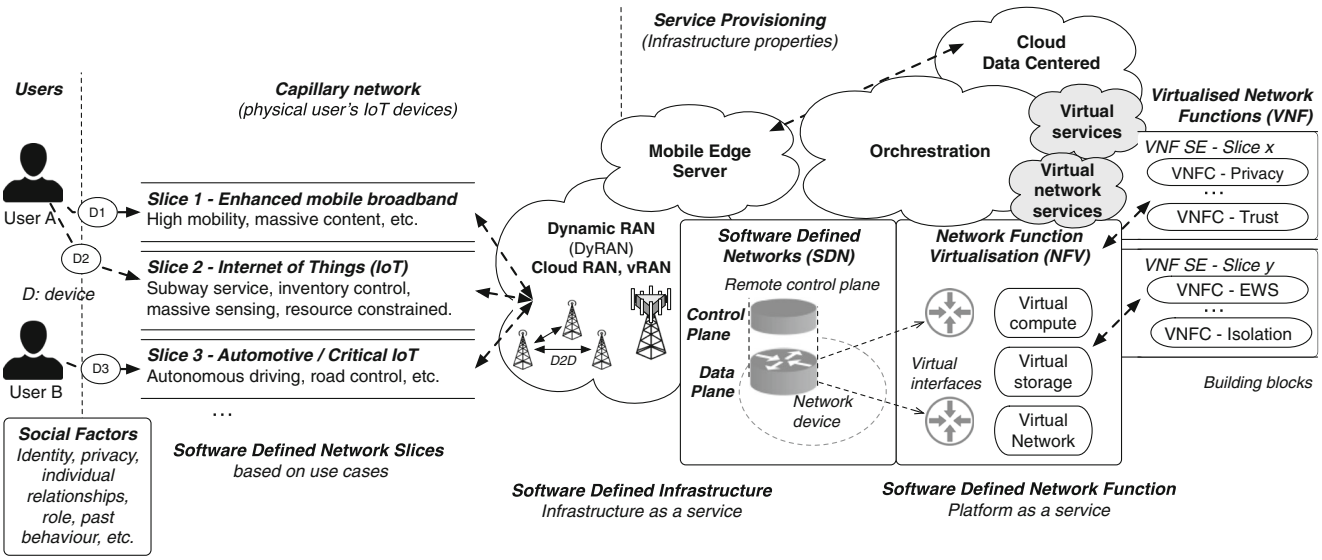


Fig. 1 Crowds and 5G technologies

Finally, the ability to virtualise network functions will be critical in providing specific network services while minimising hardware dependency. Using *Network Function Virtualisation* (NFV), the network services could be installed in a standard hardware platform. Furthermore, the software can be replaced easily than the hardware. This also helps security, in the sense that an attack could be contained and the affected services stopped and launched again, while new services are launched to attend to the user's demands. However, the use of software also exposes the system to unknown vulnerabilities.

3 Crowdsourcing use cases and evolution to 5G IoT cybersecurity

In this section the use cases for crowdsourcing that can be adapted to be used for 5G cybersecurity are discussed.

3.1 Commercial purposes

As part of the 5G business model, parts of the physical infrastructure can be shared among several service providers (SPs) (c.f. MEC, Section 2). In this context, it will be critical to promote crowdsourcing between SPs to to identify attacks that can affect a shared infrastructure of a common set of services. Therefore, security mechanisms must be deployed for sharing relevant information between the SPs to mitigate the effects of a possible propagation of an attack while ensuring that these services meet privacy and confidentiality requirements, as well as other ethical aspects. This will be essential to ensure the shared information does not encourage corporate espionage.

A similar approach to crowdsourcing can be found in projects like the *Malware Information and Sharing Platform* (MISP) [16] which is a software platform for sharing information between organisations about recent threats, fostering the development of countermeasures by generating *Indicators of Compromise* (IOC) for antivirus software, firewalls and Intrusion Detection Systems. For instance, the CIRL MISP Threat Sharing Service [8] comprises more than 700 different organisations and companies (mainly European) where analysts share knowledge about current malware campaigns, correlating the information available and providing new evidence as soon as it is collected.

3.2 Fast response after natural disasters

The power of crowdsourcing applications to warn of natural disasters is highlighted in [5], where crowdsourcing is proposed to mitigate disasters through the cooperation of individuals using social media. Although the results of this paper could help improve the mitigation mechanisms after an attack, the nature of cybercrime is complex enough to require different mitigation techniques. First, in cybercrime scenarios there are human actors with the *intention* to cause harm to an individual or to society [2]. Second, the pattern to predict the attack or to predict the extent of the damage are not the same. While natural disasters can be predicted through observation, and when they occur the damage can be clearly seen, cyberattacks are much more complex. Clear examples of this are the *Advanced Persistent Threats* (APT). These are latent and therefore go unnoticed in the targeted system, waiting to act in the moment they have the best chance of causing the most damage to the system. In other words, APTs do not necessarily follow a known, identifiable pattern. These attacks will also affect cellular networks.

3.3 Mitigation of physical attacks

In [10] crowdsourcing data is generated from mobile phones with integrated chemical-agent detectors in order to provide an *Early Warning System* (EWS) within a security network, which quickly warns of detected threats. The proposed solution depends on a sensor network infrastructure which sends commands to a secure network to fight against physical attacks.

However, software attacks are very different from physical attacks and require new models to be analysed. It must be highlighted that one of the main problems in 5G networks is that the infrastructure is unable to store detailed information about the IoT devices after a certain time (due the density of the networks, and the capabilities of the relay nodes). Therefore, after a time, the relays *forget* if a *new* input-node to the cell was a *malicious node*. Physical layer security mechanisms attempt to address these issues [13, 19], but depends on network information that they simply don't have (e.g. the location of the attacker). One way to solve or mitigate these problems is to deploy part of the security controls at the edge or in the user's IoT devices, or to implement crowdsourcing mechanisms between trustworthy devices to identify potential threats.

3.4 Social media

One example of massive crowdsourcing are social networks [17]. These have encouraged the need of the user to be *always-on*. Social applications, such as *Whatsapp*, *Twitter*, *Facebook*, to name a few, serve to effectively spread news items, even before these are published in the traditional media. These and other *open* platforms have permitted, for example, the cooperation between anonymous people to stop the propagation of the recent *WannaCry* malware [6]. In the same way, these communication highways generate rich information for analysis to identify patterns

and relationships between individuals. This is a serious concern with regards to privacy.

Therefore, social media is another vehicle for 5G crowdsourcing in two ways: 1) traditional crowdsourcing between humans but focused on identifying misbehaviour or physical attacks against the devices of the infrastructure (e.g. relays), and 2) crowdsourcing to extract relevant information to be processed by automatic tools to identify patterns (e.g. automatic analysis using open source intelligence but centered on parameters of interest for the service providers).

3.5 End-user collaboration

Crowdsourcing is fundamental as a tool for end-user collaboration against attacks targeting user devices. In this regard, the concept of *digital witness* (DW), is defined in [11] for IoT environments. The idea is to help citizens report misbehaviour, attacks and offences against themselves or other citizens, and to store digital evidence in order for it to be used in a court of law. This solution requires the cooperation of people to stop those attacks that *as humans we cannot see, but our devices can detect*. This reasoning can be applied at the edge of a 5G IoT network, providing the DW functionality as a service (c.f. Section 5.1.3). In [3] the authors applied similar concepts to obtain electronic evidence from vehicular networks (cars as witness), which is very useful considering that vehicular networks are a key use case in 5G. A common requirement in previous related work is that everyone insists on the need to have a trusted third party element, either embedded or as part of an external query trustworthy system.

4 Crowdsourcing for 5G IoT security

Crowdsourcing can be classified, in accordance with different factors, as stated in [7], where eight general characteristics are identified: (a) there is a clearly defined crowd; (b) there exists a task with a clear goal; (c) the recompense the crowd receives is clear; (d) the crowdsourcer is clearly identified; (e) the compensation to be received by the crowdsourcer is clearly defined; (f) it is an online-assigned participative process; (g) it uses an open call of variable extent; (h) it uses the Internet. While the concept has evolved to include autonomous entities (e.g. sensors), these criteria are still being applied. Table 1 shows the relationships between the characteristics of crowdsourcing as listed and what we consider to be potential crowds in 5G (Fig. 1) i.e. users, the IoT devices in the capillary network, legacy RATs, and the service providers.

4.1 Users

The users in a 5G network have at least one IoT device, and have the possibility to *personalise* the software of their devices, for example, installing specific tools for crowdsourcing.

The role of the user in 5G cybersecurity is twofold. First, as mentioned in Section 3.4, social media as a crowdsourcing mechanism can be used to warn of cyberattacks or to help coordinate individuals to help understand the threat. Second, Table 1 shows a different point of view, close to the idea of end-user collaboration, but applied to physical attacks or traditional digital evidence (e.g. images). Thus, the user can contribute to

Table 1 Crowdsourcing for 5G IoT Cybersecurity

Crowd			Crowdsourcer		Publishing		
(a) Who	(b) Task	(c) Reward	(d) Who	(e) Benefit	(f) Process	(g) Call	(h) Internet
Users	Social media for coordination & Warning of crime	Duty to the community	Subscriber	(Cyber) criminal profiles	Certified software from LEA	All end -users	Through 5G
Capillary network	Warn of misbehaviour and attacks	Increase trust/ reputation	Legacy RATs	Cybercriminal profiles	D2D Service	All devices	Using a device or 5G
Legacy RATs	Warn of local attackers, fake relays and BSs	Protect themselves from local attacks	SP at the core	Physical 5G infrastructure	Inclusion in RAT protocols	Antennas and relays	Access to the 5G infrastructure
Service Provider (SP)	Identify vulnerabilities in the SW and the physical infrastructure	Access to the information provided by other SPs	Service Providers	Shared database for cybersecurity	The process, and the call has to be private to certain SPs with common interests		

the prosecution of traditional criminals, using the 5G infrastructure as a resource to share the information. These attacks could be from physical attacks against the physical components of the infrastructure (e.g. vandalism against legacy RAT elements) captured by the citizen to prove that a well-known cybercriminal is close to a critical infrastructure. How to address these requirements while still integrating privacy issues is a critical concern. Permitted actions should be the same as those actions allowed using the traditional compliant mechanisms for citizens.

4.2 Capillary network—IoT devices in 5G

The capillary network in 5G is formed by IoT devices, some of them able to connect to other devices via D2D (Section 2). In 5G this concept is extended to *Machine Type Communication* (MTC) [15]. According to [4], the devices have different ways of connecting to the 5G infrastructure: a) direct, b) aggregation, c) short-range D2D. All these types of access are grouped under what is known as *Massive MTC* (mMTC). Critical services, such as road safety and industrial manufacturing, require *Ultra-reliable MTC* (uMTC). In addition, to increase the coverage of the antennas, whilst avoiding the obstacles in the signal propagation, the 5G infrastructure uses relays (Section 4.3). Therefore, the devices or machines have to connect to the antennas using the relays.

The devices in the capillary network can use crowdsourcing mechanisms to warn of misbehaviour and local attacks on D2D. The crowdsourcer will be the legacy RATs where the final coordination of IoT devices to access the 5G infrastructure is done (Section 6). Note that, to make this possible, it is mandatory to ensure the integrity of the devices, and probably not all the devices are able to provide reliable information about the attack. Moreover, in 5G it will be necessary to deploy local security controls in the IoT devices. There are many reasons for this, but, mainly, the density of devices makes it unfeasible to control and analyse all the traffic at the core, and in real time. Moreover, certain traffic can be dangerous once it passes the capillary network and moves to the core.

Finally, SDN allows different criteria to be applied to the different use cases and flows. This makes it possible to deploy traffic analysis and mitigation mechanisms based on the data provided by the crowds, in specific network slices. As Fig. 1 shows, a single user can have more than one device connected to the 5G infrastructure, and a device can require services from two different network slices (e.g. a car for navigation and for HD video). This entails a serious concern about the crowdsourcing in the capillary network; when devices send data to other devices (e.g. for aggregation) or to the legacy RATs (e.g. summary of the attack) it must be carefully considered whether the user's identity can be deduced from the data provided (linkability, etc.). It is essential to ensure that 5G IoT crowdsourcing mechanisms are designed in accordance with privacy principles.

4.3 Enablers for dynamic RAN

The IoT devices in the capillary network connect to the physical components of the 5G infrastructure (e.g. powerful 5G antennas and relays) using the available *Radio Access Technologies* (RAT) (e.g. LTE-A, mmWave). One of the improvements in 5G is that it uses DyRAN (Section 2), enabling the devices to act as temporary access nodes, amongst other advantages [4]. This part of the 5G ecosystem is highly exposed to physical attacks, particularly in the case of relay networks. Relays are much needed in 5G because they allow the coverage of the antennas to be increased. Therefore if the relays are affected, the communication between the IoT devices in a specific area and the SPs is interrupted. In addition to physical attacks, it is possible to affect the communications by supplanting the base station closest to the relay (or to any DyRAN device) and drop the traffic, or perform a DoS attack by jamming.

The traditional security solutions in this context are called *physical security* as some of these consist in bypassing the attacker by changing the communicating parameters between the relays [13]. However, it is not always possible to apply these solutions due to a lack of low-level security functionality or because the information about the attacker is not available (e.g. the location and the transmission range). Another major problem are attacks which exploit vulnerabilities to gain control of the relays, and those that are performed remotely (because the relays will be connected with a command and control system through the Internet).

Crowdsourcing can help mitigate some of these security issues if the DyRAN enablers are able to store and share information about the state of the relays. This information will be processed at the core of the network, because relays are part of the 5G infrastructure, and the rest of the elements need to be informed as quickly as possible.

4.4 Service provisioning

The boundaries of crowdsourcing from a security point of view between SPs are detailed in Section 3.1. However, there are additional aspects in service provisioning that can affect 5G security. These are related to the technologies shown in Fig. 1.

SPs are responsible for facilitating a fast deployment of services to satisfy the user's demands. A clear consensus is that NFV is a key technology to satisfy this purpose in 5G (Section 2). One example of how NFV can be used for security can be seen in Fig. 1. NFV enables *Virtual*

Network Functions (VNF) to be defined with security (SE) requirements for specific services. The security requirements can be separated into *VNF Components* (VNFC), which allows their use by other VNF SE such as dockers. However, as described in Section 2, isolation mechanisms can be bypassed by more sophisticated malware.

Therefore, crowdsourcing mechanisms can be useful for secure service provisioning in two ways. First, to collect information about the physical components of the 5G infrastructure (Section 3.1) and, second, to control the software components; virtual services, controllers, etc. One way to control the software components using crowdsourcing is to provide tools for the clients of the multi-tenant architecture to evaluate the services from a security point of view. Another way is to designate virtual components with more security restrictions to act as crowdsourcers and collect information of the orchestrator of the virtual environment.

5 Entity-based crowdsourcing model

Figure 2 shows the key components to be considered in a model for mitigation of cybersecurity threats through crowdsourcing.

The model considers four main entities:

- Crowds. Provide the data according to pre-established principles and agreements with the crowdsourcers. These can be users and devices, either public or private to the 5G infrastructure (c.f. Table 1).
- Crowdsourcers. Determine the crowdsourcing plan and provide the management of the rewards. Some potential 5G infrastructure crowdsourcers are listed in Table 1.
- Processing Units. Components responsible for data management and providing answers. Early detection units, when these are allocated in the edge (e.g. using MEC) or remote detection units, when these are provided in the core of the network.
- External, impartial sources. External trusted parties, agents who are responsible for providing additional support that is not provided by the crowdsources. A direct example is a *Legal Agency Enforcement* (LEA), as is shown in the use case in Section 6.

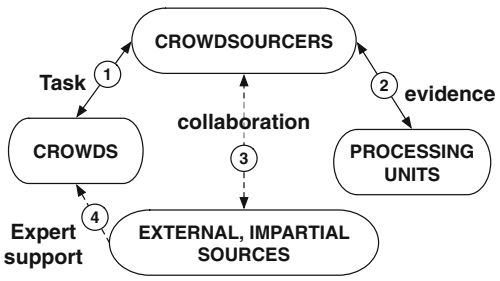


Fig. 2 Crowdsourcing-based collaboration

This model should be adapted to the use case to be implemented. For example, Fig. 3 shows this model applied to a specific use case. This use case, in particular, focuses on the end-user collaboration described in Section 3.5. The use case covers one of the most notorious, identified open challenges in 5G IoT: how to fight against attacks in a part of the 5G ecosystem that is not entirely under the control of the SP.

The rest of the section describes the crowdsourcing model using this specific use case.

5.1 Applying the crowdsourcing model for end-user collaboration

The use case concentrates on the user and capillary network (Table 1). In this context, different types of IoT devices are possible (e.g. sensors, vehicles, mobile phones, and drones) subscribed to services provided by the 5G infrastructure (e.g. traffic control information, video, and autonomous navigation).

We identify three types of crowds in 5G IoT which are mapped into this scenario (Fig. 3): (i) users, (ii) IoT devices enabled for D2D, and (iii) digital witnesses (c.f. Section 3). A device can have the role of digital witness if it satisfies the conditions in [11] (e.g. anti-tampering behaviour, binding credentials and security capabilities) and is certified by an LEA. These actors provide different data about their environment. Therefore, Fig. 3 shows three practical examples about crowdsourcing in 5G IoT described below.

5.1.1 User (social media)—service provider

The first sequence for crowdsourcing is as follows. (1) The service provider (SP) announces the task and reward (e.g. vouchers for users to be spent on a premium service) and a possible service to those users who want to collaborate in the crowdsourcing experiment (e.g. subscription to receive information about attacks in their surroundings). The subscribers are other users or entities who also collaborate in the crowdsourcing. (2) The user sends traditional digital evidence (e.g. pictures of vandalism). This evidence is manually collected, for example, by using the camera of the device. (3) Depending on the type of evidence and the urgency, the SP may request the intervention of the LEA, or simply use this information to perform other internal tasks to improve the 5G infrastructure. The user will receive the reward after a validation process according to the initial conditions of the challenge.

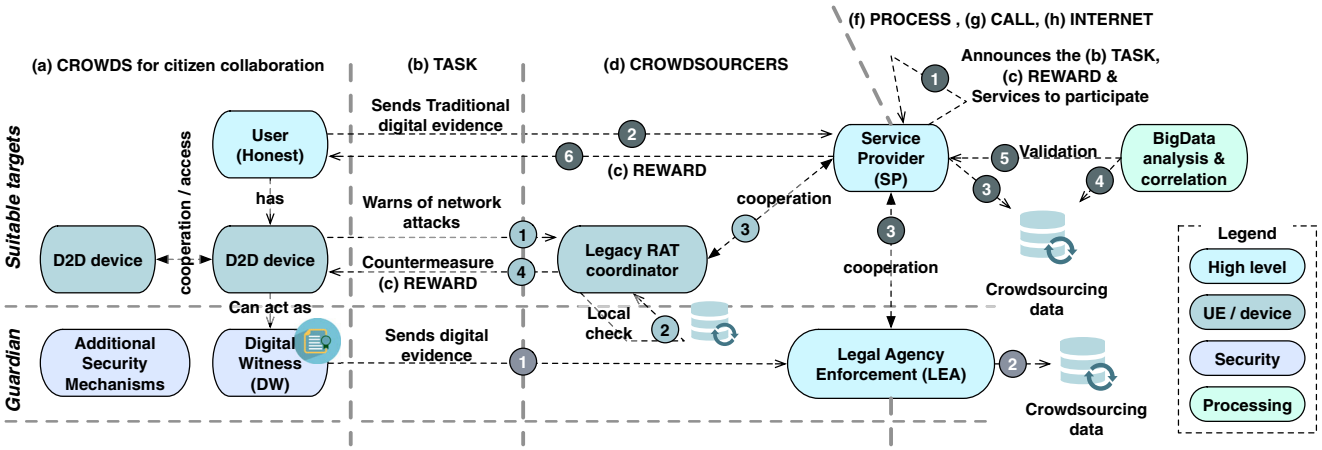


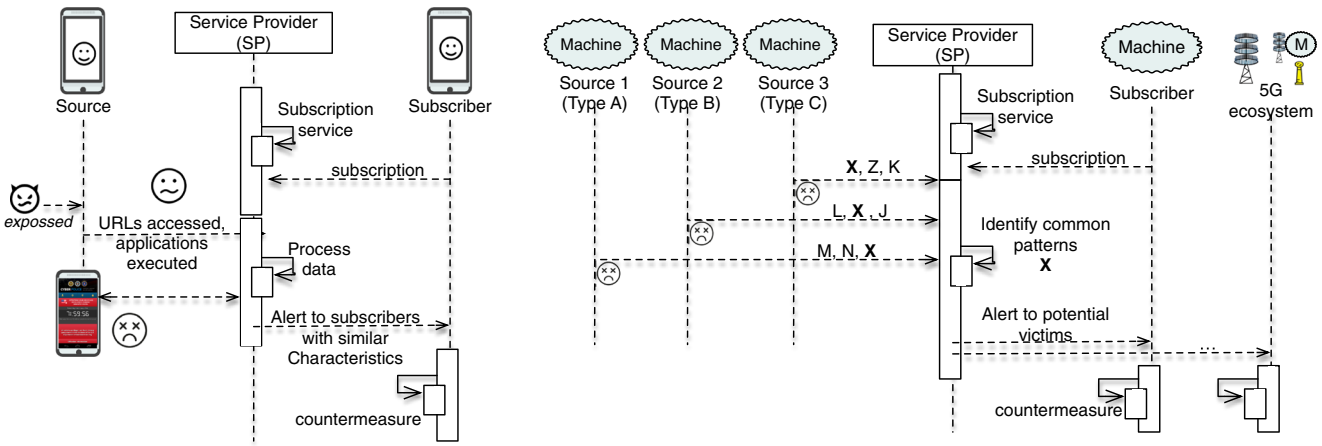
Fig. 3 Model for end-user collaboration for mitigation of cybersecurity threats in 5G IoT

Note that in this sequence the user is honest. However, a clear requirement is to identify dishonest behaviour of users and to penalise these kinds of actions. This can be done, for example, ensuring the traceability of the information provided by the user, in order to determine the responsibility of the user when he/she provides information that could compromise other users or the infrastructure. For example, the traceability could be possible using the user's personal devices as the following section shows. Note that this entails a serious concern about privacy and how this can be ensured providing a correct balance between privacy and security.

5.1.2 D2D devices—5G infrastructure

The task in this case is to warn of misbehaviours and network attacks (Table 1). The communication is performed at the low level and does not require the participation of the user. This, therefore can be an additional service of the infrastructure to help protect the capillary network. (1) The task performed by the IoT device is *to provide information about local attacks and vulnerabilities in the software of the devices*. (2) The coordinator of this feature for RAT evaluates the data with local information and (3) it contacts the SP if it needs more information or if the data provided by the devices needs further analysis. (4) The coordinator communicates what countermeasure are to be taken and assigns the reward (e.g. increase the reputation).

In addition, Fig. 4a shows some examples where personal devices can be effective early detection systems in this context. When a personal device realises that it is executing a new ransomware malware (e.g. Flocker [9]), for example by detecting the encryption process, it can (anonymously) send the last actions performed (URLs accessed, applications executed, etc.) to the SP. This information can be used by the SP to query malware intelligence services, like MISP introduced in Section 3.1, to correlate and warn other connected devices subscribed to



(a) Early Warning Service for Subscribers (b) Common patterns from heterogeneous IoT devices

Fig. 4 Crowdsourcing for mitigation in 5G IoT environments

the service. Therefore, a distant user can benefit from this interaction without even knowing that a new ransomware campaign is actually running. A similar idea is to identify common patterns of infection from multiple IoT devices, in order to identify if the malware can affect heterogeneous platforms and to alert the users and administrators of the sectors of the infrastructure affected (Fig. 4b).

Another scenario that fits perfectly is the detection of web phishing and spear phishing. There are actually many ways to detect these types of attacks, even modern web browsers are capable of detecting them. This information can also be shared with the SP to inform other connected devices that some live phishing sites are actually attracting users.

5.1.3 Digital witness—LEAs

The *digital witnessing* (DW) feature is provided as a service. The objective is to propose crowdsourcing services able to warn other users of a possible attack in one specific area. In this case, (1) the DW sends digital evidence (electronically stored information in the device, such as logs or information about their applications and can contain personal data) signed using the security protocols accepted by the LEA. In some critical cases, a DW can require the validation of the information before being sent to the LEA (e.g. using biometric features). This is specified during the configuration of the device [11]. (2) The LEA processes the information and takes countermeasures that could require the initiation of legal proceedings. (3) If it is required, the LEA should contact the SP to get more information or cooperate to stop certain threats against the 5G ecosystem.

There is no direct *material* reward for the DW. Initially, as is described in [11], the owner of the DW acts following a *duty to the community*. However, the SP can promote the crowdsourcing using similar rewards like in the previous case. The additional advantage of the digital witness is that it allows traceability, which can help identify and penalise misbehaviours.

Some requirements are clear at this point. First, the anonymity of the people involved in certain tasks must be ensured and kept from the rest of participants in the crowd. Neither must critical information about the sources be public to the rest of the crowd. Finally, information about vulnerabilities should be shared only with the affected users/devices. Some directions about how to introduce privacy-aware mechisms in digital witness-based scenarios are provided in [12].

6 Experimental results

To illustrate the effect that one of these attacks would have on end users and the contribution of the crowdsourcing mechanisms to mitigate this effect, we performed a validation using OMNET++. We define two special nodes, one single attacker, Eve, and a protector of the network named $Guardian$. The proof of concept is reduced to a single cell, where the nodes communicate over VoIP. Eve will affect communications by directing the attack against the service that supplies to the rest of nodes. Then, the $Guardian$ will perceive a fault in the service provisioning, and follow the proper procedures for their recovery.

Figure 5 highlights the behaviour of Eve (red), $Guardian$ (blue) and the $Server$ that receives the request from one of the UEs. Eve begins to act in $t = 2ms$. Then, considering that all the nodes are using the service, the communication between the nodes is affected proportionally to the number of messages that the nodes can send during the time window that the service remains inoperative. UE send messages to the $Server$ that will only be handled if the $Guardian$ is present to restore the service. It can be seen that at $8ms$ there is an interruption in the service and the $Server$ stops responding to the UE requests, because the $Guardian$ is not present. In general, only when the $Guardian$ starts operating does the $Server$ starts listening to requests.

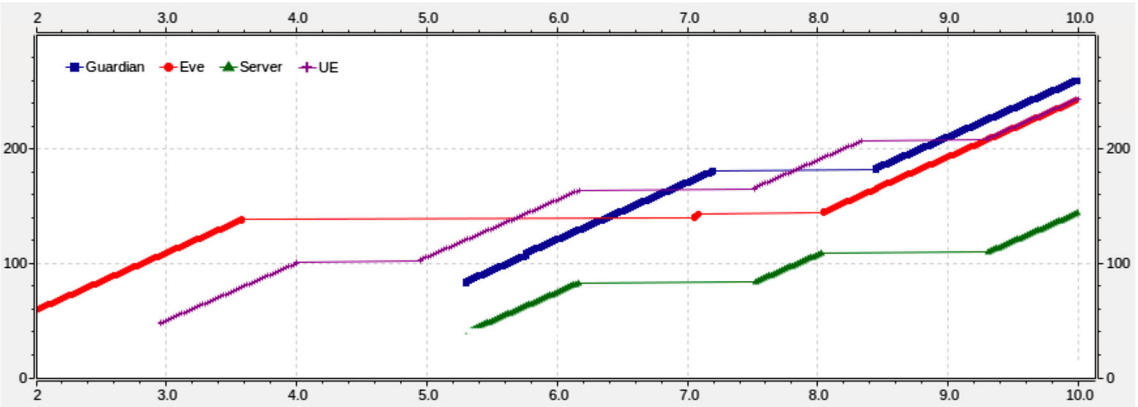


Fig. 5 Simulation results with a single cell

Therefore, if the attack depends on the strategic location of the attacker, then corrective measures can be taken from the source of the threat. If the *Guardian* can react, it could even inhibit the attacker, or store digital evidence about the attack and the context (potential digital witness in the area). An additional interesting study that we leave for future work is to analyse how these data vary with mobile nodes at different speeds, and varying the number of guardians and attackers.

Finally, it must be highlighted that IoT devices have serious limitations in computation and storage. Even worst, most of them are a security risk in themselves. However, we can use the density of IoT devices to obtain information from many sources to improve the data analysis and the extraction of conclusions. This information could be taken in two ways: a) from those IoT devices able to contribute (not all IoT devices are equally limited) or b) from those intermediary platforms able to provide data summaries relevant to the context.

7 Conclusions

Given the proliferation of technologies and devices in 5G it is unrealistic to assume that security should *only* be provided at the core of the network. Rather the opposite is true, the only way to react efficiently to new forms of threats is to do so at the edge of the communication. More specifically, crowdsourcing mechanisms can be an effective weapon against cybersecurity threats in 5G IoT. In this paper this idea has been analysed in depth to show the advantages of this cooperation in the different areas of 5G. We have also adapted an example of crowdsourcing to help improve security in 5G environments using IoT devices. The results of this paper can be adjusted to any final context where crowdsourcing will be applied. Additional challenges are, for example, to consider the privacy and trust in the different models for crowdsourcing applied to 5G IoT. Along these lines, some work has already been done on digital witnessing, but the problem must be particularised to the different contexts of the 5G infrastructure.

Finally, note that the solution proposed perfectly fits in the current LTE/4G network. However, from our point of view, the real change where collaboration will be fundamental will occur when the decoupling between software and hardware is greater. Unlike 4G, 5G has been conceived to support specific use cases in IoT, and this is a serious problem because these devices continue to be insecure. Not only that, if a security problem occurs, there are no proactive solutions that help clarify what has happened.

Acknowledgments This work has been partially funded by the Spanish Ministry of Economy and Competitiveness through the projects IoTest (TIN2015-72634-EXP /AEI) and SMOG (TIN2016-79095-C2-1-R).

References

1. Belmonte Martin A, Marinos L, Rekleitis E, Spanoudakis G, Petroulakis N (2015) Threat landscape and good practice guide for software defined networks/5g. European Union Agency for Network and Information Security (ENISA)
2. Chon KHS (2016) Cybercrime precursors: towards a model of offender resources. PhD Thesis. Australian National University
3. de Fuentes JM, González-Manzano L, Gonzalez-Tablas AI, Blasco J (2013) Wevan–a mechanism for evidence creation and verification in vanets. J Syst Archit 59(10):985–995
4. Dohler M, Nakamura T (2016) 5G mobile and wireless communications technology. Cambridge University Press, Cambridge
5. Gao H, Barbier G, Goolsby R (2011) Harnessing the crowdsourcing power of social media for disaster relief. IEEE Intell Syst 26(3):10–14
6. Hanslovan K (2017) Proud moment: Wannacry collaboration. https://medium.com/@KyleHanslovan/proud-moment-wannacry-collaboration-e1f6fafe76dc
7. Howe J (2006) The rise of crowdsourcing. Wired Mag 14(6):1–4
8. Luxembourg TCIRC (2017) Cirl misp threat sharing. https://www.circl.lu/services/misp-malware-information-sharing-platform/
9. Micro T (2016) Flocker mobile ransomware crosses to smart tv. http://blog.trendmicro.com/trendlabs-security-intelligence/flocker-ransomware-crosses-smart-tv/
10. Monahan T, Mokos JT (2013) Crowdsourcing urban surveillance: the development of homeland security markets for environmental sensor networks. Geoforum 49:279–288
11. Nieto A, Roman R, Lopez J (2016) Digital witness: safeguarding digital evidence by using secure architectures in personal devices. IEEE Netw 30(6):34–41
12. Nieto A, Rios R, Lopez J (2018) IoT-forensics meets privacy: towards cooperative digital investigations. Sensors 18(2):1–17. 492
13. Nomikos N, Nieto A, Makris P, Skoutas DN, Vouyioukas D, Rizomiliotis P, Lopez J, Skianis C (2015) Relay selection for secure 5g green communications. Telecommun Syst 59(1):169–187
14. Palattella MR, Dohler M, Grieco A, Rizzo G, Torsner J, Engel T, Ladid L (2016) Internet of things in the 5g era: enablers, architecture, and business models. IEEE J Sel Areas Commun 34(3):510–527
15. Ratasuk R, Prasad A, Li Z, Ghosh A, Uusitalo MA (2015) Recent advancements in m2m communications in 4g networks and evolution towards 5g. In: 18th international conference on intelligence in next generation networks (ICIN). IEEE, pp 52–57
16. Wagner C, Dulaunoy A, Wagener G, Iklody A (2016) Misp: the design and implementation of a collaborative threat intelligence sharing platform. In: Proceedings of the 2016 ACM on workshop on information sharing and collaborative security. ACM, pp 49–56
17. Xu Z, Zhang H, Hu C, Mei L, Xuan J, Choo KKR, Sugumaran V, Zhu Y (2016) Building knowledge base of urban emergency events based on crowdsourcing of social media. Concurr Comput: Pract Exp 28(15):4038–4052
18. Xu L, Collier R, O'Hare GMP (2017) A survey of clustering techniques in wsns and consideration of the challenges of applying such to 5g iot scenarios. IEEE Internet of Things J PP(99):1–1. https://doi.org/10.1109/JIOT.2017.2726014
19. Yang N, Wang L, Geraci G, Elkashlan M, Yuan J, Di Renzo M (2015) Safeguarding 5g wireless communication networks using physical layer security. IEEE Commun Mag 53(4):20–27