Future Generation Computer Systems 75 (2017) 46–57

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Evolving privacy: From sensors to the Internet of Things

Javier Lopez [a], Ruben Rios [a,*], Feng Bao [b], Guilin Wang [b]

[a] Network, Information and Computer Security (NICS) Lab, University of Malaga, Spain
[b] Huawei International Pte Ltd., Singapore

HIGHLIGHTS

- Analysis of existing privacy threats in scenarios involving sensing technologies.
- Evaluation of the privacy problems that may be inherited by the IoT.
- Identification of the challenges that emerge as sensors are integrated into the Internet.

ARTICLE INFO

Article history:
Received 23 November 2016
Received in revised form
24 March 2017
Accepted 29 April 2017
Available online 8 May 2017

Keywords:
Privacy
WSN
Internet of Things
Challenges

ABSTRACT

The Internet of Things (IoT) envisions a world covered with billions of smart, interacting things capable of offering all sorts of services to near and remote entities. The benefits and comfort that the IoT will bring about are undeniable, however, these may come at the cost of an unprecedented loss of privacy. In this paper we look at the privacy problems of one of the key enablers of the IoT, namely wireless sensor networks, and analyse how these problems may evolve with the development of this complex paradigm. We also identify further challenges which are not directly associated with already existing privacy risks but will certainly have a major impact in our lives if not taken into serious consideration.

1. Introduction

The Internet of Things (IoT) has been recognised as one of the major technological revolutions of this century [1,2]. Although the IoT is still in its infancy and will only unleash its full potential with the development of a completely distributed approach [3], the importance of this paradigm has already been recognised by the major international standard bodies [4], which have come into play to ensure the correct operation, interoperability and resilience of this paradigm.

Despite the complexities of the scenarios envisioned by the IoT [5], the realisation of this paradigm can be achieved with three main, non-trivial architectural components: smart things, backend servers and communications infrastructure (as depicted in Fig. 1). One of the challenges in these scenarios is to enable the connection of everyday objects to the Internet. However, the IoT is not only about connectivity, it is about the pervasive collection and sharing of data towards a common goal. Therefore, smart sensing technologies are undeniably one of the key enablers of this paradigm.

Since humans are amidst smart things, the deployment of sensing technologies by IoT systems will pose an unprecedented threat to individual privacy. Unlike current Internet scenarios where users have to take an active role (i.e., query for services) to put their privacy at stake, with the increasing number of sensing devices around us, we become targets of data collection without even noticing it and in hitherto unsuspected situations. This has led some companies to analyse the need for security and privacy in these environments [6,7] but in most cases privacy is treated in the narrow sense of data confidentiality. Surprisingly, only a few companies acknowledge the need for more advanced privacy mechanisms, even though the NGMN Alliance [8] explicitly states that no mature solution has been proposed to date.

Also some researchers have looked at privacy problems in IoT environments. Most of them consider privacy as part of a broader security analysis (e.g., [3]) and only a few papers analyse privacy as a problem in its own right. In this respect, some authors have looked at privacy in the IoT from a legal perspective [9]. Other authors have analysed the privacy impact of various enabling IoT technologies [10,11]; however their analyses are horizontal and they leave out some relevant problems inherited from sensor networks. We cover them in this paper in detail.

* Corresponding author.
E-mail addresses: jlm@lcc.uma.es (J. Lopez), ruben@lcc.uma.es (R. Rios), bao.feng@huawei.com (F. Bao), wang.guilin@huawei.com (G. Wang).

http://dx.doi.org/10.1016/j.future.2017.04.045
0167-739X/

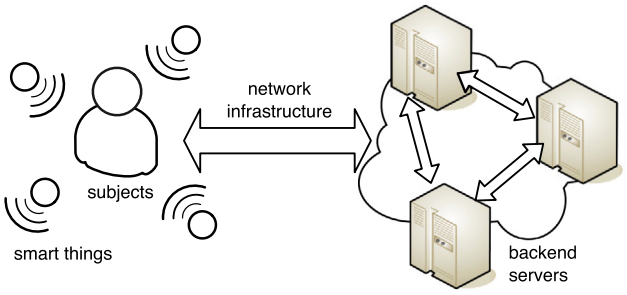


Fig. 1. Simplified IoT architecture.

These privacy problems (see Fig. 2) can be classified into two main categories according to the entity whose privacy is being threatened, namely the user or the network itself [12]:

- In *user-centric* privacy, the problem comes from the ability of sensors to detect the presence of humans or relevant assets and capture sensitive information about them. Therefore, sensor networks can be used as a mechanism to inadvertently spy on anyone or anything. Moreover, user-centric privacy cannot be easily achieved by technological means alone as the privacy perpetrator is the owner of the network and he/she may secretly use the surveillance capabilities of the network to profile and track users.
- In *network-centric* privacy, the attacker is an external entity who wants to learn information about the network itself or the elements being monitored by the network. In this case, the first line of defence is the use of confidentiality mechanisms to protect the content of data packets. However, this is usually not sufficient to provide network-centric privacy as the attacker may gain access to the cryptographic material. In addition, the attacker may be able to extract relevant information by means of traffic analysis attacks.

This classification can be broken down into several subcategories depending on the type of information or asset to be protected. A natural question at this point is whether computer-based anonymity solutions for current Internet scenarios may be suitable to tackle the aforementioned problems. After an extensive analysis [13] we concluded that most of these systems are too costly, and even when some of them are lightweight enough, they do not meet the anonymity requirements for sensor networks or they limit their functionality. However, it is worth noting that they will be indispensable for protecting the traffic to/from the outside infrastructure.

In this paper we concentrate on analysing how the privacy problems that have appeared in sensor networks, as isolated systems, will evolve when they are integrated into the Internet. We also identify new challenges that the evolution of these technologies will possibly entail. The main goal of this paper is thus to highlight privacy problems as well as potential solutions and, in this way, encourage the scientific community to continue researching and delving into the various challenges identified in this paper. This will, in turn, facilitate the development of solutions to address privacy threats thus giving rise to a more privacy-conscious IoT.

The structure of this paper is organised according to the classification in Fig. 2. First, in Section 2 we focus on problems and challenges caused by the ability of sensor networks to surreptitiously collect information about individuals. Subsequently, Section 3 and Section 4 deals with two different privacy problems that affect the network itself and the assets and entities being legitimately monitored by the network. Section 5 describes further challenges that may arise due to the integration of sensing technologies in the IoT but are not a direct evolution of problems already existing in sensor networks. Finally, Section 6 summarises the main contributions of the paper.

2. User-centric privacy

This section describes the privacy problems associated with the ability of sensing technologies to collect information about individuals within their monitoring range without them even being aware of this situation. We also briefly look at the typical approach to privacy in the Internet era, which is based on legislation and fair information practices. Finally, we present the reasons why legislation is not the way to a privacy-friendly IoT and discuss some related challenges.

2.1. Introduction

User-centric privacy concerns people being the target of data collection by ill-intentioned network operators or data-hungry businesses. In fact, Camenisch [14] describes personal information as the "new currency on the Internet" due to the change in the business model over the last few years. Now services are offered in exchange for personal information instead of money. Regardless of the claims of service providers, in many cases personal data are not only used to provide value-added services to the users but also to improve their products or are shared with third parties for different purposes, such as targeted advertisement [15,16].

With sensing technologies all around us, the opportunities for data collection reach new orders of magnitude. Prior to sensing technologies, it was relatively difficult to violate individual privacy unless a user was actively involved in Internet communications. Unfortunately, in a world covered with all types of sensors, privacy can be breached at anytime regardless of being an active user or not, of the system. Moreover, these invasions of personal privacy may appear in all sorts of everyday situations, even in the intimacy of our own home. This represents an unprecedented loss of privacy as sensing technologies will be ubiquitous. There will be sensors at the office, at the supermarket, at home and also attached to our bodies or even implanted [17]. Consequently, it is paramount to set barriers on the collection, processing, storage and dissemination of personal data.

Until recently, the most common approach to privacy protection has been through legislation. Indeed, one of the most well-known privacy definitions was given by Alan F. Westin [18], a legal scholar, who talks about privacy as the right of individuals to determine how much personal information is disclosed to other entities, and how it should be maintained and disseminated.

2.2. Privacy legislation

The aforementioned definition is probably the basis for modern information privacy law as it encapsulates important notions which were later included in some major pieces of legislation, such as the US Privacy Act of 1974, the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of 1980, and the EU Directive 95/46/EC of 1995. Some of these guidelines and directives have been recently revised or are in the process of revision and awaiting for adoption at the time of writing.

Thereafter, any collection of personal information should conform to the fair information practices (FIPs) as the basis for confidence and trust in online transactions. The FIPs establish a number of principles including user awareness, consent, access and control, purpose specification, data minimisation, and secure storage. In other words, individuals must be aware of being subject to data collection and they must explicitly allow the collection, processing, storage and dissemination of data about themselves. Also, the data collector must clearly specify the purpose of data collection and use the data for no other purposes. Moreover, the collection of personal information must be minimised and retained only for as long as is necessary to fulfil the original purpose

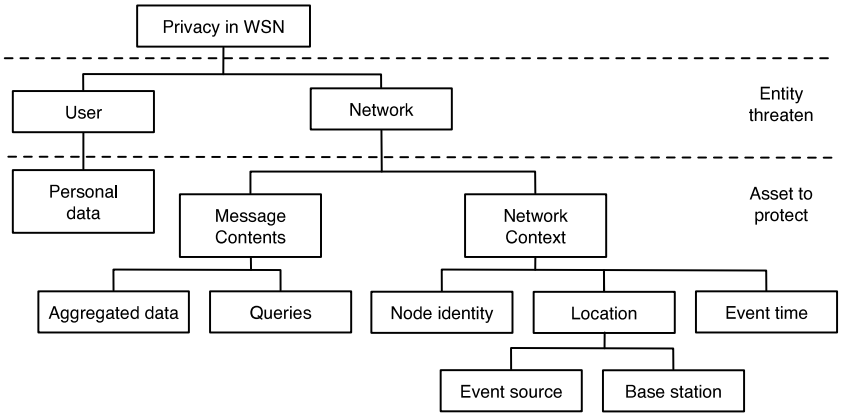


Fig. 2. Privacy problems in WSN.

specified to the user. Finally, the collected data must be secure and accessible to the user at all times, being the data collector responsible for any privacy breaches.

Unfortunately, these principles are not always met [19] and, when this happens, legislation must be in place to punish privacy invaders. To that end, periodic audits must be established as well as severe sanctions. Clearly, for the time being this is not the case and, most importantly, the problem will be aggravated with the advent of ubiquitous sensing technologies and the IoT.

Legislation is an important mechanism to prevent misuse of personal information, however, it is not the solution to the problem. In fact, legislation does not prevent privacy from being violated but is more a way to compensate the damage caused by privacy breaches. Of course legislation is aimed to dissuade powerful entities from abusing of their ability to collect personal information but it is more a patch than a solution. It is basically a reactive tool that punishes privacy perpetrators once the harm is done. Privacy is not recovered but compensated economically.

Under these circumstances, companies find themselves in the position of taking advantage of the situation and collect as much data as possible to increase their revenues and expect to get away with it, or they may consider following a privacy-by-design approach and fair information practices, possibly limiting their business model. As a result, the most prominent firms in the market seem to be following the first approach [20] basically because the revenues usually outweigh the cost in fines imposed by court. The only hope is that privacy scandals inspire action and users retaliate against this type of dishonest behaviour.

2.2.1. Challenges

Legislation on its own cannot provide privacy guarantees to individuals interacting with the Internet of Things. As sensors and computers are miniaturised and embedded inside everyday objects, thus disappearing from our vision and our consciousness, we become more vulnerable as we may not even be aware of being observed. This implies that it will be more difficult to take legal action against privacy perpetrators especially in a world covered with billions of devices, where it will not be straightforward to map devices to their owners in order to take them to court.

Interestingly, even if we save these obstacles and are able to identify that our personal information has been obtained without our consent, there is nothing we can do to recover our privacy. Moreover, legislation is slow. Legislation has always been behind technology and the distance will continue to grow as the IoT matures and acquires the ability to collect more detailed information and develops new ways of deriving knowledge from the collected data thanks to advanced data mining algorithms.

On the other hand, businesses can decide to follow fair information practices, however, this is not trivial and there are several factors to take into consideration. Service providers cannot constantly prompt users with consent requests because this would make the IoT a cumbersome and impractical paradigm. Users overwhelmed with requests would either ignore them or be reluctant to use the technology as it becomes extremely annoying. Also, it is important to rethink the way in which consent, privacy policies, and so on, are presented to the users. Not only is important to avoid the use of extensive policy documents in favour of more intuitive and eye-catching ways of providing this information but also it is instrumental to consider that devices in the IoT will be varied and not many of them will have human-friendly interfaces to interact with users.

In this respect, the solution to enable a non-intrusive IoT seems to be related to the implementation of mechanisms for the automatic negotiation of privacy preferences. These mechanisms would allow users to seamlessly interact with systems that are respectful with their personal data. The challenge here is providing suitable tools for configuring privacy preferences in an informed way, letting the users learn about the risks of sharing too much and at the same time finding a balance to be able to use services.

Also in relation to this, it would be necessary for businesses to take these privacy preferences into consideration in order to change the traditional opt-in/opt-out approach, where the user either accepts all the conditions stated in the privacy policy or the service is not provided. In contrast, a more flexible approach is recommended, where the provision of services is more granular and based on the amount of information the user is willing to provide. The more information provided, the more accurate or feature-rich the service could be.

3. Content-oriented privacy

The data collected and transmitted by the network may contain private information about individuals, businesses and valuable assets. As such, protecting these data from eavesdroppers and attackers enables content-oriented privacy in WSNs. Although the typical approach to data protection has been through authentication and encryption, these mechanisms alone cannot ensure content-oriented privacy in some specific circumstances. Next we cover two situations where content-oriented privacy is not sufficiently covered with these basic but still necessary mechanisms. These are during data-aggregation and when users query the network for data.

3.1. Aggregated data privacy

Data-aggregation is the process of combining information from different data sources as messages flow towards the base station.

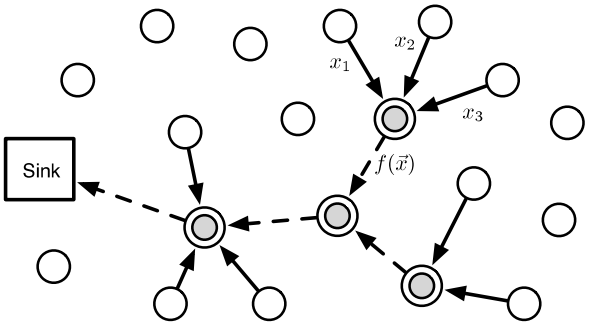


Fig. 3. Data aggregation in WSN.

Some typical data-aggregation operators are the sum, average, maximum, and minimum. This process can be seen in Fig. 3, where data sources pass event data to aggregator nodes along the communication path. The main benefit of these protocols is that they significantly reduce the communication and energy overhead of sensor nodes and at the same time allow the base station to reduce the computational burden due to the processing of a large number of messages. Consequently, data-aggregation is a very important process for the durability and efficiency of sensor networks.

3.1.1. Solutions

Since data-aggregation requires the processing of data on several intermediate nodes, there is an obvious content-oriented privacy risk in the case these nodes are compromised by an attacker. The trivial solution to prevent intermediate nodes from breaching content-oriented privacy is to apply end-to-end encryption to each transmitted message. Although this prevents intermediary nodes from gaining access to the contents of messages, it also precludes the application of data-aggregation mechanisms. As a result, the research community has strived to develop algorithms capable of aggregating data while keeping the contents of messages safe from curious intermediaries.

Different authors have approached privacy-preserving data-aggregation from various angles resulting in solutions with diverse properties and different levels of accuracy, overhead, flexibility, etc. A typical approach is to use homomorphic encryption as it naturally enables intermediate nodes to perform some basic operations over encrypted data. In this respect we have two groups of solutions based on whether symmetric-key homomorphism [21,22] or public-key homomorphisms [23,24] are used. The main difference between them is that in the symmetric case, encryption and decryption are done with the same key and thus is more prone to key compromise attacks. Another set of solutions are capable of providing content privacy during aggregation by slicing the data into pieces [25,26] and sending them to different aggregators, which aggregate the contributions and then forward them to the base station. The main limitation of this approach is on the increased number of collisions and network overhead. Finally, some authors trade accuracy for privacy and tackle the problem by means of data perturbation mechanisms based on the generalisation of data before sending it [27] or the addition of noise to readings [28,29].

3.1.2. Challenges

These solutions will become more necessary with the advent of the IoT and will be essential in scenarios like smart metering [30], where embedded devices used for collecting utility consumption (i.e., smart meters) may use adjacent meters to relay their own readings to the utility company. In such a scenario, a curious neighbour could learn the utility consumption of another neighbour if the attacker is used as a relay.

There are several challenges to overcome for the success of privacy-preserving data aggregation in the IoT. First, most existing solutions assume particular network topologies, organised in clusters with static sensor devices. However, the mobility and dynamism of the foreseen scenarios, where sensors are attached to objects or carried by individuals, demand for solutions that consider constantly changing topologies with both static and mobile data aggregators.

A major related challenge is the distribution of keys and trust. Ordinary sensor networks usually consider an initialisation phase for the distribution of secrets, which can be later used for the purpose of private data aggregation but this would be infeasible in highly dynamic scenarios with countless security domains like those envisioned by the Internet of Things. Consequently, shifting to public-key cryptography seems absolutely necessary but this transition will be extremely difficult due to the heterogeneity and hardware limitations of the devices involved in this new paradigm.

There is also a lot of room for innovation in cryptography. Devices will continue to miniaturise and extremely constrained devices will coexist with more powerful ones. Thus, it is imperative to advance in cryptographic mechanisms making them suitable for tiny devices without compromising security or usability. More precisely there is a need for exceptionally efficient fully homomorphic operators. At the time of writing, there are some crypto-systems capable of performing some basic operations efficiently (e.g., addition) but fully homomorphic cryptosystems are still very costly and much research needs to be done before these schemes are really convenient for tiny things with embedded micro-controllers.

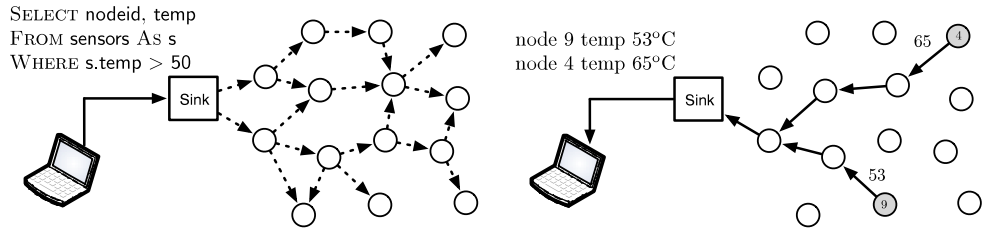
Finally, it is mandatory to consider active attacks, where the adversary not only wants to observe the data of other users but also may take advantage of privacy mechanisms to maliciously modify aggregated values without being detected. Consequently, it is paramount to find solutions capable of revoking the privacy of malicious contributors or aggregators. However, there must be legal and technological bounds to limit the revocation of privacy to situations where the identification of evildoers is critical and the revocation must be realised only by trustworthy parties or by the set of entities affected by the attack. Clearly, finding such a balance between privacy and integrity will not be an easy task especially considering that these systems will be highly distributed and possibly anarchic.

3.2. Query privacy

Sensor networks usually follow an event-driven data reporting method meaning that they only transmit data upon the detection of an event of interest in their vicinity. The popularity of this data reporting method lies in the ability of the network to provide phenomena information in real time while keeping the energy budget low. However, there may be occasions in which we are interested in learning about a specific phenomenon at a particular time. In these cases the network must turn to a query-driven approach, in which the user queries the network for the readings of a particular set of sensor nodes or asks for nodes satisfying a particular condition (see Fig. 4). For example, an oil company may be interested in the readings of a particular region of an underwater sensor network.

3.2.1. Solutions

In the aforementioned example there is a serious organisational privacy risk if an attacker is capable of learning which sensors are being queried by the oil company as this may denote interest for petroleum exploration in a particular area. Obviously, the company may wish to keep their activities and interests secret from competitors and other third parties for the safety of their own



(a) Query is broadcast to the network.

(b) Nodes' replies are returned to the user.

Fig. 4. Query-driven WSNs.

business. The goal of query privacy is precisely to reduce the risk of exposing sensitive information to attackers when issuing queries to a sensor network.

The trivial solution to the problem is to make all sensor nodes reply to queries even if the user is not interested in them. After receiving the readings, the base station (or the user) keeps the relevant data and discards the rest. This approach is very simple and provides perfect privacy but it is also extremely inefficient, especially when the network is densely populated. Thus, several authors have proposed solutions in an attempt to find the right balance between privacy and network overhead. For example, the authors in [31] try to reduce the overhead by using data-aggregation when responding to queries. This is possible since they focus on a particular type of query, namely MAX queries, for finding the maximum value of a particular feature (e.g., the maximum temperature). A more general approach is presented in [32], where the idea is to hide the interests of the user in a particular area by issuing additional bogus queries together with the actual query. Another approach to the problem when issuing queries to a specific node is to guide the query on a particular path in such a way that any of the nodes in the path are potentially the node of interest to the user [33]. However, this requires additional knowledge about the topology of the network. To overcome this problem, the scheme proposed in [34] leverages data replication at a number of random locations in the network thus unlinking the data from its source. When the user sends a query, it is forwarded to several random destinations hoping to hit one of the replicas. Finally, some authors [35] have recently explored how much communication overhead is necessary to achieve a certain level of privacy when issuing queries to a sensor network.

3.2.2. Challenges

As the number of sensing devices grows in the Internet of Things, the goal of achieving perfect query privacy becomes more unattainable since the overhead grows exponentially. Therefore, one substantial challenge for the future will be to find solutions capable of achieving perfect privacy without incurring much overhead or at least finding an appropriate balance between both worlds. In this respect, it is important to quantify and explore the limits of privacy and communication overhead as this will help reveal how far can technology be pushed to ensure the desired level of privacy.

An important difference between current sensor networks and the ones considered in future scenarios for the IoT lies in the security domains of the networks. In traditional sensor networks both the client and the owner of the network are the same entity and third parties are not authorised to query the network. However, this will notably change over the coming years and sensor networks will be offered as a service to other parties. Consequently, the network owner and the client do not necessarily belong to the same domain. In this setting, clients may be reluctant to disclose their interests to network operators in order to prevent user profiling. The similarities between the described problem and private information retrieval for databases [36], where a user wants to retrieve information from a database without disclosing the items retrieved, are evident and thus they will unfold and mature in parallel.

In addition, so far the query privacy problem has been addressed from a narrow perspective, that is, a user will query only its own network. But with the advent of the IoT, clients will be able to query a number of networks from different providers from remote locations. This opens the door to linkability issues like those already existing in the current Internet. An external attacker may be able to learn information from the networks to which the queries of a user are addressed. Combining this information he may later be able to infer new knowledge and build user profiles. Moreover, as IoT systems are expected to collaborate in order to provide advanced new services and attackers may learn from the relationships between service providers.

There are also other data associated with the process of querying which needs to be protected. In particular, the number of queries being issued as well as the rate at which queries are transmitted reveal the level of interest of the requester has in a particular set of elements. Constantly querying the same sensors reveals a great interest in a particular area. Furthermore, the order and the relationship between queries reveal sensitive information. Given a sequence of queries, the attacker (e.g., the service provider) should not be able to learn of the intentions of the client. Clearly, hiding all these data will be a major challenge for the future.

4. Context-oriented privacy

During the normal operation of the network, the mere presence of messages in the network reveals a lot of information even if secure encryption algorithms are used to protect their contents. The reason for such a data leakage is that an attacker may learn information not only from the contents of the messages but also from the features of the communications, including the size and number of messages being transmitted, the time and rate at which messages are being sent, the frequency spectrum used by the nodes, the source and destination of transmissions, etcetera [37]. Although these data are apparently innocuous, they can be used to infer information about the type of sensors being used, the owner of the network, the type and precision of the data being collected, the topology of the network, and so on. Some of these features are extremely difficult or impossible to hide depending on the hardware platform but other features can be easily changed although they have an impact on the efficiency and durability of the network. Next we analyse two context-oriented privacy problems in detail.

4.1. Temporal privacy

The occurrence of an event is always associated with the time at which the event takes place and without this information event data is mostly meaningless. For example, knowing that the pressure of a nuclear centrifuge has passed a certain threshold is useless if we do not know when to activate the corresponding

release valve. Therefore, immediately after detecting a special event, the sensor node collects information and generates an event message that it transmits to the base station. If the source node is not in the neighbourhood of the base station, the message traverses several nodes until it eventually reaches its destination. Whenever a message is received by a relay node, the recipient processes and forwards it to the next communication hop as soon as possible. In this way, sensor networks achieve real-time monitoring capabilities.

4.1.1. Solutions

Due to the need for data in real time, an attacker can estimate with reasonable accuracy the time at which the event was detected based on publicly available parameters: the time of arrival of the message, the distance (counted as the number of hops) from the data source, which can usually be obtained from packet headers, and the routing protocol in use. This provides the attacker with the ability to predict future behaviours of the phenomenon being monitored by merely observing the temporal pattern of packets arriving at the base station. In a military scenario this information is extremely valuable for the enemy as they can preempt the movement of troops and craft more intelligent attack plans remotely.

The trivial solution to this problem would be to switch to a time-driven data reporting model, where sensor nodes transmit data at regular intervals defined by the network administrator. Again, there are some downsides to the trivial solution which are due to the duration of the interval: if it is set too long, it limits the real-time capabilities of the network but if, on the contrary, it is set too short, it considerably reduces the lifetime of the sensor nodes. Therefore, the few existing articles addressing this problem [38,39] have turned to introducing random delays as the messages flow to the base station.[1] This solution is still incompatible with real-time applications and requires the use of buffering at intermediate nodes but is more energy efficient since messages are only transmitted when sensor nodes detect relevant data. Buffering is not a trivial task and needs to be handled with care for two main reasons, which are the tight memory space of sensor nodes and the uneven distribution of traffic in sensor networks. Therefore, they propose a mechanism to adjust the introduced delay based on the amount of received messages.

Recently, some effort has been made towards enabling real time monitoring while preserving temporal privacy [40]. The proposed solution is based on the introduction of Laplacian delays to perturb the transmission time and ordering of messages. The features of the Laplacian distribution enables the data recipient to aggregate the data from multiple sources without much error. However, it is unclear whether the adversary can perform similarly and find out the original sending times.

4.1.2. Challenges

The main challenge in this area for the years to come will be to reach a solution capable of finding the correct balance between perturbation, data utility and energy consumption. Temporal privacy can only be satisfied by introducing significant delays to message transmissions or by introducing fake traffic in order to hide real transmissions but this is at odds with real-time monitoring capabilities and the energy preservation principle of sensor networks and the Internet of Things.

Although buffering can increase temporal privacy, this technique presents several functional impediments besides the memory requirements in hardware constrained devices like sensor nodes. So far, this technique can only be applied to delay-tolerant applications unless the buffering delay is significantly reduced, which allows attackers to gain a great advantage over the protection mechanism. The solution may be somehow similar to the evolution from mixnets to onion routing but the problem here has different nuances such as temporal delays in mixes when introduced to prevent correlations between messages and not necessarily to provide temporal privacy. When onion routers were first introduced, the idea was to allow internet communications in real-time, which was not possible with mixes. Compared to mixes, which introduce large delays until a sufficiently large pool of messages is available, onion routers rely on the multiplexing of messages in a single channel. Onion routers does not necessarily provide temporal privacy. In most cases, the attacker gains temporal information from the time at which messages arrive regardless of the data source.

Moreover, the use of buffering mechanisms may be in conflict with other security mechanisms used by the network. Introducing large delays to messages before forwarding them may appear to a distributed intrusion detection system [41] like some kind of denial of service attack. There is extensive literature on detecting and defeating packet dropping (e.g., selective forwarding) attacks but little or no work has been done on the protection of temporal privacy and denial of service attacks simultaneously. This will doubtlessly be a challenging area of future research.

4.2. Identity privacy

Even if the payload of messages is properly protected from eavesdropping by secure confidentiality mechanisms, the attacker can still learn information from the packet headers as these are usually in clear text to enable routing operations. Among other relevant information, packet headers contain the source and destination address of the nodes involved in the communication (see Fig. 5). Therefore, after observing the transmissions of the network for a while,[2] the attacker may be able to map identifiers to nodes and nodes to geographical locations in the field. As a result, the attacker obtains a map of the network which allows him or her to easily link event messages to the area where they were generated.

4.2.1. Solutions

Nodes must change their identifiers periodically to prevent exposing their identities to external observers. Instead of using their true identifiers nodes use pseudonyms. Persistent pseudonyms are useless because the attacker can eventually map these pseudonyms to actual nodes as if the pseudonyms were the original identifiers. Therefore, pseudonyms are only effective if they are periodically updated.

Some of the solutions to provide node anonymity are based on the generation and distribution of pseudonyms from a large pool. In [43] the base station generates a network-wide pool and distributes random subranges of the pool to the nodes. The base station keeps the correspondence between the true identity of the node and the assigned subranges. In addition, neighbouring nodes exchange pseudonym information to enable routing and hop re-encryption since nodes select a random pseudonym for each transmitted packet. The main problem of this approach is on the memory requirements to store pseudonyms. A similar approach is devised in [44], where the base station assigns labels to each network link. These labels are used as identifiers when a node has

[1] The actual timestamp of the message is encrypted within the payload.

[2] The attacker may even trigger the transmission of messages. For example, he or she may light a burner near a node in a forest fire detection scenario.

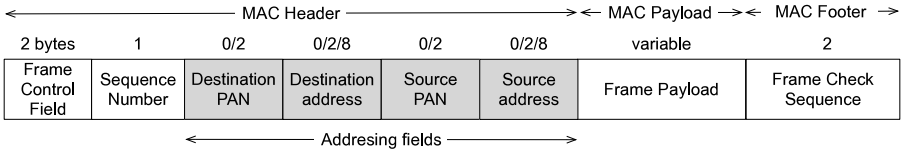


Fig. 5. General IEEE 802.15.4 MAC Frame format [42].

to send a packet to another node. In this case, the main limitation is that the link labels are not sufficiently dynamic and they are only changed after a new topology discovery.

Cryptographic mechanisms were devised to overcome the limitations of the previous solutions. These schemes turn to keyed hash functions to generate pseudonyms that are unlinkable to previously used ones [43]. In this way, they are capable of reducing the memory overhead imposed by pool-based solutions at the cost of more computations. They assumed that secrets cannot be compromised but as this is a strong assumption, the authors in [45] proposed the use of keyed chains in the regular order (the node rehashes the pseudonym to generate a fresh one) or in reverse order (the nodes first create the hash chain and then use elements in reverse order) for enhanced protection. More recent schemes [46,47] not only update the pseudonyms but also the secret keys used for the hashing process.

4.2.2. Challenges

First, pool-based solutions present serious scalability issues. The distribution and management of a complete pool of pseudonyms for the IoT is clearly impractical. One reason is that most of the elements of the IoT will have too constrained a memory to hold a sufficient number of pseudonyms and it will be infeasible to update the pseudonyms regularly enough in a centralised way. Moreover, node capture will become easier thus exposing stored pseudonyms.

Crypto-based solutions solve most of the problems caused by node compromise thanks to the use of hash chains and key updates but they also demonstrate some limitations. Basically, these and pool-based solutions assume static network deployments where devices only communicate with nearby devices. However, in an IoT scenario, devices may be dynamic and spontaneous communications with unknown devices may be necessary at some point. Therefore, considering mobility will be essential in the development of new pseudonym solutions for the Internet of Things.

Existing solutions concentrate on node identifiers at the link layer since WSNs are considered isolated systems, where nodes only communicate with the base station or nearby devices. However, due to the integration of sensor networks into the Internet, sensor nodes will also communicate with remote devices and thus it will be necessary to consider the obfuscation of identifiers at the routing layer.

Also, as sensors and things will be carried and worn by individuals, the identifiers of the devices will reveal personal information about their owners. Since hardware identifiers are unique, they can be easily linked to people. Also, as the number of devices we carry will continue to grow, the re-identification process will be more robust because each of the features (i.e., identifiers) is partially identifying and when combined together, the chances for error are significantly reduced.

Furthermore, identifiers not only help to re-identifying individuals, but they also reveal personal information about them. Hardware identifiers usually reveal information about the manufacturer and the type of device. As a result, an attacker may be able to infer personal information from the devices we own. For example, the attacker can learn that we have a heart problem from the identifier of our pacemaker, he may also learn that someone has a good economic situation because he wears an expensive smart watch, or he may learn someone is a policeman because he has a service weapon. Similar problems have been observed in the past with technologies like RFID [48], however, this problem is even more acute in IoT scenarios as attackers will be able to get this information also remotely.

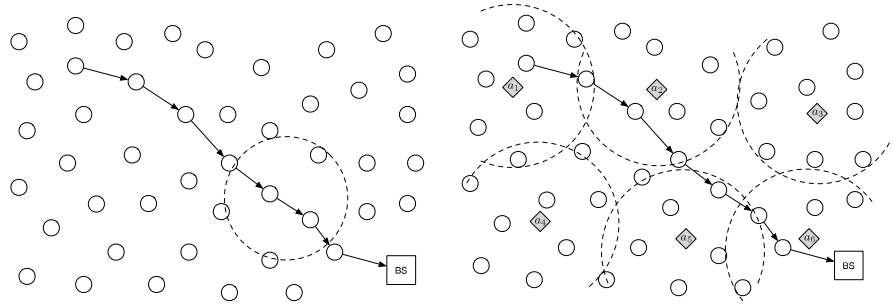
4.3. Location privacy

Despite the efforts to hide the identities of the nodes, the attacker can still learn location information by observing the communication patterns in the network. The wireless nature of the communications and the urgent need of sensor nodes to preserve their limited energy budget exposes the location of relevant nodes. More precisely, single-path routing protocols are very energy efficient because they use the minimum number of relays and as such they tend to use the same communication path for every message, thus extremely simplifying traffic analysis. Location privacy refers to the ability to keep secret the location of nodes with a particularly interesting role, namely data sources and the base station. The location of data sources is relevant because they are close to a special event (e.g., an endangered animal in habitat monitoring applications) while the importance of the base station lies in that it is the device in charge of receiving and processing all the information collected by the nodes, and thus the attacker can cause much harm by destroying or compromising this precious device.

4.3.1. Solutions

A local attacker is a passive, external adversary with a local hearing range, similar to that of an ordinary sensor node (see Fig. 6(a)). This type of adversary moves in the network field following messages to reach either data sources or the base station. In order to reach a data source, the adversary uses a directional antenna to determine the angle of arrival of messages and move in that direction to find the data sender. By repeatedly performing this operation on the various sensor nodes that make up the communication path, the attacker eventually reaches the original data sender. The attacker is also capable of reaching the base station by acting similarly but now he looks at the transmission times between neighbours and their transmission rates. As nodes closer to the base station receive and forward a higher number of messages, the attack strategy is to move towards nodes with higher transmission rates. Countermeasures against local adversaries are mainly focused on the randomisation of routing paths for source [49,50] and sink [51,52] protection as this prevents traceback attacks and balances the number of transmissions in the network. Some authors have also turned to the injection of fake traffic to mislead the adversary from their target [53,54]. More advanced schemes have considered hiding the transmission of data from the attacker by sending them within apparently innocuous messages [55] or by re-routing the packets to circumvent the area under the control of the adversary [56].

Adversaries can achieve a larger hearing range by deploying several antennas in the field. The attacker who monitors all the communications in the network it is known as a global adversary (see Fig. 6(b)). Based on the communication patterns observed by



(a) Local adversary. (b) Global adversary.

Fig. 6. Location privacy problem.

the antennas, a global adversary can estimate the location of data sources and the base station. Data sources are detected because they are the first to transmit data and the base station can be spotted because it is located in the area with highest transmission rates. To prevent global adversaries the trivial solution is to make every sensor transmit at a particular rate regardless of the presence of events [57]. However, this approach either introduces significant delivery delays or is too costly in terms of energy consumption. Therefore, the research community has struggled to find the correct balance between both. Some solutions send messages following a particular probability distribution in such a way that event messages can be preempted without altering the properties of the original distribution [58,59], while other schemes have tried to minimise fake traffic by removing it at various network nodes [60] or by reducing the area to which messages are delivered [61].

Active adversaries are not limited to eavesdropping the communication channel but are also capable of disturbing the network operation by creating, modifying or blocking messages, and tampering with devices. In fact, we are unaware of any research that deals with active adversaries manipulating the communications even though this is not necessarily a very strong adversary. Notwithstanding, some papers have considered the threats of attackers tampering with sensor nodes to compromise location privacy. In [62], the authors propose that upon the occurrence of an event of interest, the sensing node encrypts the collected data with a secret key shared with the base station. Then these encrypted data are sent to a different node, which stores it temporarily until the base station requests it. In this way, if the attacker compromises a storage device he is unable to decrypt the data because the original key is not known to this node. Also, it is not possible for the attacker to learn the original data source. In another paper [63], the authors make the observation that an active adversary can easily reach the base station if he learns the routing tables of a few sensor nodes. To reduce this threat they present a routing table perturbation scheme that re-arranges the elements of the routing table in such a way that it reduces the chances of the attacker while still allowing packets to reach the base station.

4.3.2. Challenges

Despite the large body of research on location privacy (see [64] for a complete analysis) there are still many challenges to overcome. First, most of these solutions have been designed with a single goal in mind which is either to protect data sources or the base station and with a particular type of adversary in mind. However, when these systems are an integral part of the IoT we will need solutions capable of protecting both data sources and the base station simultaneously. Also, it is paramount to consider adversaries capable of disrupting the network operation for their own benefit and not only consider passive attackers who simply observe and analyse the communications.

Furthermore, some of the proposed solutions will not be applicable when moving towards the IoT for a number of reasons. First, these solutions make assumptions about the system model that may not always be realistic such as sensor networks compromising thousands of devices. Sensor networks may be much smaller (e.g., a home automation network) and may be small enough for an adversary to control all the communications with a single antenna. Practically speaking, there are situations in which local adversaries resemble a global adversary. Notwithstanding, as IoT systems may interact with remote services and devices, there is no adversary powerful enough to control all possible communication flows. Furthermore, some approaches which were innovative and efficient, like context-aware privacy solutions, may be impractical in some IoT scenarios like Smart Cities where the network will be unable to faithfully recognise the adversary and use his location to adapt the routing paths.

Additionally, as the number of devices grow it will be easier for the attacker to compromise objects and use them as elements of an adversarial network to observe the communications of legitimate nodes. This problem is aggravated by the fact that it will be easier to compromise and take control of devices as things will be reachable from remote locations through the Internet. Therefore, the attacker will have the opportunity to cover larger and geographically disperse locations to eavesdrop on devices without having to be physically present in those regions. In this sense, the attacker becomes very powerful but can hardly cover the whole Internet of Things although he might be able to control complete subsystems and occasionally learn the relationships among them and eavesdrop on their communications. Moreover, the attacker can continue to compromise devices based on the information so far collected in order to close the circle on specific target networks thus gradually increasing his ability to monitor all the communications of a particular system.

A typical approach to protect location privacy, especially from global adversaries, is to inject fake traffic in the network. However, as the network density increases in IoT scenarios, this approach becomes more disruptive. Interferences grow, the signal to noise ratio lowers, packet collisions and retransmissions become more frequent and thus the timeliness, reliability and throughput of the channel drops precipitously. Consequently, the provision of location privacy based on the injection of fake traffic needs to be carefully redesigned to prevent these problems. A promising area of research in this respect is cognitive radio networks [65], which enables opportunistic spectrum access based on its utilisation. With this type of technology it will be possible to improve network efficiency but the injection of fake traffic also poses impediments on the durability of the network as it implies the rapid depletion of batteries. Therefore, coming up with new approaches capable of providing similar levels of protection without incurring so much overhead will be of tremendous interest in the future.

Dealing with active adversaries will be a challenging and promising area of research. So far, little work has been done to

address this type of attacker, possibly due to the difficulties of dealing with active attacks with the extreme hardware limitations of sensor nodes. The open nature of wireless communications not only enables eavesdropping but also injecting, modifying, blocking or replaying packets, which have already allowed a variety of attacks in computer networks including replay attacks [66], congestion attacks [67], and so on. These well-known attacks are even more plausible in sensor networks since the attacker is very powerful compared to hardware constrained sensor nodes.

Moreover, active adversaries may have access to the internal memory of some of the devices we own or collect information about us. These objects will store much relevant information for the sake of configuration, error detection and mitigation, etc. This information includes the performance of the object, user preferences, and all sorts of user-related data. Consider, for example, a smart pen which may not only reveal information about the whereabouts of its owner but may also indicate persons to whom drugs have been prescribed, recipients and number of cheques written by the user, and even biometric information. This is extremely sensitive and private information which is safe while stored in the device but becomes a problem as soon as a third party gains access to the device. Whenever a personal device is borrowed, sold or sent for repair, the information stored in the device is subject to be exposed. This already happens with our hard drives and smart phones but the problem will be exacerbated in the IoT since we now know what sorts of data are contained in our devices (i.e., pictures, documents, etc.) but this may not be so clear for smart things given their ability to collect fine-grained information at any time.

5. Further identified challenges

Despite the many challenges that have been presented in previous sections, here we identify a number of additional challenges which are not directly related to already existing problems in wireless sensor networks but are more associated with the features and peculiarities of the sensors and the Internet of Things. As this is a particularly dynamic and evolving paradigm, new challenges will doubtlessly appear in the near future.

First, it is important to consider the Internet of Things as a whole and not as isolated systems which are used only in particular scenarios. The benefits of this new paradigm will come with the seamless interconnection and interaction between these systems of systems. Unleashing the full potential of this paradigm requires sharing confidential data between service providers. However, service providers may be reluctant to share their confidential databases but still wish to obtain the benefits of running data mining algorithms on the union of their databases. Privacy-preserving data mining will be a relevant area of research to enable knowledge sharing at the backbone of the IoT without exposing individual records.

Similarly, users may wish to share information with service providers or store their data in the Cloud but only if the data are encrypted. Therefore, the service provider must be able to perform operations, such as queries over encrypted data and return the results to the user, which is the only entity capable of retrieving the actual results. In exchange, service providers should also be able to extract information from the data even if encrypted. Developing data mining algorithms over encrypted data will be another challenging area of research for future IoT scenarios.

So far, the user has been considered as a passive element of the system who has little or no responsibility with respect to protecting his own privacy. With the advent of the IoT, the user will own smart objects and will need to configure them as well as interact with them. How the user configures his own devices may not only affect his own privacy but also the privacy of relatives, friends or colleagues. Therefore, raising user awareness and promoting the privacy sensitive behaviours will be a major challenge to deal with.

Also, it is important to consider that when combining data from different sources this can lead to a privacy breach. Usually, when privacy mechanisms are in place data are obfuscated before being shared with third parties. The problem arises when data from different sources are shared and the obfuscation mechanisms return incongruent results. For example, if an individual shares an obfuscated location as being in Lapland but the built-in sensors of his car states that the outside temperature is in the range of 30 to 40 degrees Celsius, these two sources of data are clearly contradictory. Similarly, the combination of data from various individuals can lead to privacy leaks especially when the attacker has access to external knowledge such as whether these individuals share a flat or work at the same office.

Another relevant area of research related to the user is the way they interact with smart objects. Interactions with things may drastically change in the future from keyboards and touch screens to more privacy invasive mechanisms. Examples of these technologies already exist and include products from large multinationals like Apple's Siri, Amazon's Alexa or Google Now, all of which are capable of recognising voice commands. This technology brings with it serious privacy concerns as the environment is constantly monitored waiting for a voice command and when detected it is sent to the company's servers for processing. Companies respond to these concerns by claiming that voice recordings are only transmitted when the user activates the system with a command. However, these claims cannot always be trusted [19].

These concerns are expected to be aggravated with the development of new interfaces for communicating with things. Especially invasive are brain–computer interaction technologies such as those devised by Emotiv [68], which just released headsets for monitoring the electrical activity of the brain and translating these signals into meaningful data ranging from basic commands to a user's mood, stress levels or mental disorders. Clearly, this may have a tremendous impact to individual privacy as not only the things we say or do may be recorded but also the things we think of are subject to analysis. Therefore, the challenge with these sorts of invasive technologies is to make devices powerful enough to process the commands and signals within the devices without resorting to external servers.

Finally, as the IoT evolves, sensitised objects will also interact with other objects or people and not only with a base station. The interactions among objects may lead to the creation of augmented relationship graphs, such as those present in online social networks. This poses an unprecedented privacy threat as an avid adversary may not only learn about the objects we own but also with whom they interact. As a result, an attacker looking at the pattern of communication between our own devices and the devices of other people may be able to infer information such as family members, friends, user interests, professional activity, and so forth.

6. Conclusion

Privacy preservation will be one of the major challenges in the development of the Internet of Things. Billions of sensor-enabled devices will be deployed for collecting fine-grained information from the environment and will share them with other devices and backend servers. Amidst them, there will be individuals as well as relevant assets and businesses thus leading to an unprecedented loss of privacy unless these issues are properly addressed from the inception of this new paradigm.

Table 1
Summary of privacy problems.

	Problems	Solutions	Challenges	Research
User privacy	Surveillance networks	Legislation and audits Fair Information practices	User awareness Quicker and endured legislation Seamless user interaction	Automatic negotiation and configuration Service flexibility
Content privacy	Internal eavesdroppers during aggregation	End-to-end encryption Homomorphic encryption Data slicing & perturbation	Dynamic topologies Lightweight homomorphisms Privacy revocation	Trust Advances in crypto
	Infer query contents from respondents	Flooding Bogus queries Data replication	Reduce overhead Sensors-as-a-Service User–server linkability	Private information retrieval Anonymous communications
Context privacy	Predict future behaviour from temporal patterns	Time-driven reporting Buffering	Real-time capabilities Conflicts w/ other mechanisms Node capture	Channel multiplexing Intrusion detection systems Tamper-resistant pseudonyms
	Link messages to data sources	Pools of pseudonyms Cryptographic pseudonyms	Dynamic topologies Network-layer pseudonyms Identification & inventory attacks	Agnostic identifiers Network-wide pseudonyms Selective response to queries
	Location leakage	Random routing Fake traffic	Energy consumption Holistic privacy Active and internal attackers	Cognitive radios Memory obfuscation
Further	Data sharing Data combination	Computation over encrypted data Privacy-aware data mining	Data sharing at backend Multi-source data combination Invasive interfaces and display Social smart things	Privacy-preserving data mining over encrypted data User awareness Context-aware data presentation

Therefore, this paper has delved into the main privacy problems arising from one of the core technologies of the IoT, namely sensor networks. Different categories of problems are presented and the most prominent countermeasures are analysed in order to gain insight into the features and limitations of these solutions. We have also tried to envision how these problems will evolve with the integration of sensing technologies as part of the Internet and recognised new challenges as well as areas that will demand future research. Moreover, we have identified additional problems that are not directly related to existing ones but will doubtlessly affect individual privacy in the future. Table 1 presents a summary of current problems and solutions, future challenges and promising areas of research.

Finally, we want to stress that as a complex and rapidly evolving paradigm, the Internet of Things will pose many technological and legal challenges which can only be overcome with sufficient anticipation and collaboration between all stakeholders. This entails the respect for fundamental human rights, like individual privacy. Only then will the full potential of the Internet of Things be unleashed.

Acknowledgements

The work of the first two authors has been partially funded by the Spanish Ministry of Economy and Competitiveness through PERSIST (TIN2013- 41739-R) and SMOG (TIN2016-79095-C2-1-R).

References

[1] C. Links, The Internet of things will change our world, ERCIM News (101) (2015) 3. Keynote. URL https://ercim-news.ercim.eu/images/stories/EN101/EN101-web.pdf.
[2] H. Green, How The Internet Of Things Will Change (And Improve) Our Everyday Lives, https://www.forbes.com/sites/ibm/2016/10/04/how-the-internet-of-things-will-change-and-improve-our-everyday-lives/ (Accessed: 03/2017) (Oct 2016).
[3] R. Roman, J. Zhou, J. Lopez, On the features and challenges of security and privacy in distributed internet of things, Comput. Netw. 57 (10) (2013) 2266–2279. http://dx.doi.org/10.1016/j.comnet.2012.12.018.
[4] IEEE Standards Association, IoT Architecture - Internet of Things (IoT) Architecture, https://standards.ieee.org/develop/wg/IoT_Architecture.html (Accessed: 02/2017) (2016).
[5] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of Things (IoT): A vision, architectural elements, and future directions, Future Gener. Comput. Syst. 29 (7) (2013) 1645–1660. http://dx.doi.org/10.1016/j.future.2013.01.010.
[6] Huawei Technologies Co., Ltd., 5G Security: Forward Thinking, http://www.huawei.com/minisite/5g/img/5G_Security_Whitepaper_en.pdf (Accessed: 02/2017) (2015).
[7] Ericsson AB, 5G Security - Scenarios and Solutions, https://www.ericsson.com/res/docs/whitepapers/wp-5g-security.pdf (Accessed: 02/2017) (2015).
[8] Next Generation Mobile Networks, NGMN 5G White Paper, https://www.ngmn.org/uploads/media/NGMN_5G_White_Paper_V1_0.pdf (Accessed: 02/2017) (2015).
[9] X. Caron, R. Bosua, S.B. Maynard, A. Ahmad, The internet of things (iot) and its impact on individual privacy: An australian perspective, Comput. Law Secur. Rev. 32 (1) (2016) 4–15. http://dx.doi.org/10.1016/j.clsr.2015.12.001, URL http://www.sciencedirect.com/science/article/pii/S0267364915001661.
[10] J.H. Ziegeldorf, O.G. Morchon, K. Wehrle, Privacy in the internet of things: threats andchallenges, Secur. Commun. Netw. 7 (12) (2014) 2728–2742. http://dx.doi.org/10.1002/sec.795.
[11] P. Porambage, M. Ylianttila, C. Schmitt, P. Kumar, A. Gurtov, A.V. Vasilakos, The quest for privacy in the internet of things, IEEE Cloud Comput. 3 (2) (2016) 36–45. http://dx.doi.org/10.1109/MCC.2016.28.
[12] R. Rios, J. Lopez, Analysis of location privacy solutions in wireless sensor networks, IET Commun. 5 (2011) 2518–2532. http://dx.doi.org/10.1049/iet-com.2010.0825.
[13] R. Rios, J. Lopez, (Un)suitability of anonymous communication systems to WSN, IEEE Syst. J. 7 (2) (2013) 298–310. http://dx.doi.org/10.1109/JSYST.2012.2221956.
[14] J. Camenisch, Information privacy?!, Comput. Netw. 56 (2012) 3834–3848. http://dx.doi.org/10.1016/j.comnet.2012.10.012.
[15] J. Temperton, AVG can sell your browsing and search history to advertisers, http://www.wired.co.uk/news/archive/2015-09/17/avg-privacy-policy-browser-search-data (Accessed: 02/2017) (Sept 2015).
[16] J. Parsons, Popular ID app could sell YOUR personal data to third-parties, without you even knowing it, http://www.mirror.co.uk/news/technology-science/technology/popular-id-app-could-sell-6205624 (Accessed: 02/2017) (Aug 2015).
[17] M. Behfar, E. Moradi, T. Bjrninen, L. Sydnheimo, L. Ukkonen, Design and technical evaluation of an implantable passive sensor for minimally invasive wireless intracranial pressure monitoring, in: World Congress on Medical Physics and Biomedical Engineering, Vol. 51, Springer, 2015, pp. 1301–1304. http://dx.doi.org/10.1007/978-3-319-19387-8_316.
[18] A.F. Westin, Privacy and Freedom, first ed., New York Atheneum, 1967.
[19] S. Landau, What was samsung thinking? IEEE Secur. Privacy 13 (3) (2015) 3–4. http://dx.doi.org/10.1109/MSP.2015.63.
[20] C.D. Marsan, 15 worst internet privacy scandals of all time, http://www.networkworld.com/article/2185187/security/15-worst-internet-privacy-scandals-of-all-time.html (Accessed: 02/2017) (2012).
[21] C. Castelluccia, A.C.-F. Chan, E. Mykletun, G. Tsudik, Efficient and provably secure aggregation of encrypted data in wireless sensor networks, ACM Trans. Sensor Netw. 5 (3) (2009) 20:1–20:36. http://dx.doi.org/10.1145/1525856.1525858.

[22] S. Othman, A. Bahattab, A. Trad, H. Youssef, Confidentiality and integrity for data aggregation in wsn using homomorphic encryption, Wirel. Pers. Commun. 80 (2) (2015) 867–889. http://dx.doi.org/10.1007/s11277-014-2061-z.
[23] C.-M. Chen, Y.-H. Lin, Y.-C. Lin, H.-M. Sun, RCDA: Recoverable concealed data aggregation for data integrity in wireless sensor networks, IEEE Trans. Parallel Distrib. Syst. 23 (4) (2012) 727–734. http://dx.doi.org/10.1109/TPDS.2011.219.
[24] Y.-H. Lin, S.-Y. Chang, H.-M. Sun, CDAMA: Concealed data aggregation scheme for multiple applications in wireless sensor networks, IEEE Trans. Knowl. Data Eng. 25 (7) (2013) 1471–1483. http://dx.doi.org/10.1109/TKDE.2012.94.
[25] W. He, X. Liu, H. Nguyen, K. Nahrstedt, T. Abdelzaher, PDA: Privacy-preserving data aggregation in wireless sensor networks, in: 26th IEEE International Conference on Computer Communications, 2007, pp. 2045–2053. http://dx.doi.org/10.1109/INFCOM.2007.237.
[26] G. Yang, S. Li, X. Xu, H. Dai, Z. Yang, Precision-enhanced and encryption-mixed privacy-preserving data aggregation in wireless sensor networks, Int. J. Distrib. Sens. Netw. 2013 (427275) (2013) 12. http://dx.doi.org/10.1155/2013/427275.
[27] W. Zhang, C. Wang, T. Feng, GP2S: Generic privacy-preservation solutions for approximate aggregation of sensor data, in: IEEE International Conference on Pervasive Computing and Communications, (PerCom 2008), IEEE Computer Society, 2008, pp. 179–184. http://dx.doi.org/10.1109/PERCOM.2008.60.
[28] M.M. Groat, W. Hey, S. Forrest, KIPDA: k-Indistinguishable privacy-preserving data aggregation in wireless sensor networks, in: IEEE INFOCOM 2011, IEEE, 2011, pp. 2024–2032.
[29] S. Ozdemir, M. Peng, Y. Xiao, PRDA: polynomial regression-based privacy-preserving data aggregation for wireless sensor networks, Wirel. Commun. Mob. Comput. 15 (4) (2015) 615–628. http://dx.doi.org/10.1002/wcm.2369.
[30] C.-I. Fan, S.-Y. Huang, Y.-L. Lai, Privacy-enhanced data aggregation scheme against internal attackers in smart grid, IEEE Trans. Ind. Inf. 10 (1) (2014) 666–675. http://dx.doi.org/10.1109/TII.2013.2277938.
[31] R. Di Pietro, A. Viejo, Location privacy and resilience in wireless sensor networks querying, Comput. Commun. 34 (3) (2011) 515–523. http://dx.doi.org/10.1016/j.comcom.2010.05.014.
[32] B. Carbunar, Y. Yu, W. Shi, M. Pearce, V. Vasudevan, Query privacy in wireless sensor networks, ACM Trans. Sensor Netw. 6 (2) (2010) 14:1–14:34. http://dx.doi.org/10.1145/1689239.1689244.
[33] E. De Cristofaro, X. Ding, G. Tsudik, Privacy-preserving querying in sensor networks, in: 18th International Conference on Computer Communications and Networks, ICCCN '09, IEEE Computer Society, San Francisco, CA, 2009, pp. 1–6. http://dx.doi.org/10.1109/ICCCN.2009.5235352.
[34] T. Dimitriou, A. Sabouri, Privacy preservation schemes for querying wireless sensor networks, in: IEEE International Conference on Pervasive Computing and Communications Workshops, 2011, pp. 178–183. http://dx.doi.org/10.1109/PERCOMW.2011.5766864.
[35] K. Hayawi, A. Mortezaei, M.V. Tripunitara, The limits of the trade-off between query-anonymity and communication-cost in wireless sensor networks, in: 5th ACM Conference on Data and Application Security and Privacy, CODASPY'15, ACM, 2015, pp. 337–348. http://dx.doi.org/10.1145/2699026.2699113.
[36] S. Yekhanin, Private information retrieval, Commun. ACM 53 (4) (2010) 68–73. http://dx.doi.org/10.1145/1721654.1721674.
[37] S. Pai, S. Bermudez, S. Wicker, M. Meingast, T. Roosta, S. Sastry, D. Mulligan, Transactional confidentiality in sensor networks, IEEE Secur. Privacy 6 (4) (2008) 28–35. http://dx.doi.org/10.1109/MSP.2008.107.
[38] P. Kamat, W. Xu, W. Trappe, Y. Zhang, Temporal privacy in wireless sensor networks, in: Proceedings of the 27th International Conference on Distributed Computing Systems, (ICDCS'07), IEEE Computer Society, 2007, p. 23. http://dx.doi.org/10.1109/ICDCS.2007.146.
[39] P. Kamat, W. Xu, W. Trappe, Y. Zhang, Temporal privacy in wireless sensor networks: Theory and practice, ACM Trans. Sensor Netw. 5 (4) (2009) 28:1–28:24. http://dx.doi.org/10.1145/1614379.1614380.
[40] X. Yang, X. Ren, S. Yang, J. McCann, A novel temporal perturbation based privacy-preserving scheme for real-time monitoring systems, Comput. Netw. 88 (2015) 72–88. http://dx.doi.org/10.1016/j.comnet.2015.06.007.
[41] R. Mitchell, I.-R. Chen, A survey of intrusion detection in wireless network applications, Comput. Commun. 42 (0) (2014) 1–23. http://dx.doi.org/10.1016/j.comcom.2014.01.012.
[42] The Institute of Electrical and Electronics Engineers (IEEE), IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements. Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs), http://standards.ieee.org/getieee802/download/802.15.4-2006.pdf (2006).
[43] S. Misra, G. Xue, Efficient anonymity schemes for clustered wireless sensor networks, Int. J. Sensor Netw. 1 (1) (2006) 50–63. http://dx.doi.org/10.1504/IJSNET.2006.010834.
[44] A.A. Nezhad, A. Miri, D. Makrakis, Location privacy and anonymity preserving routing for wireless sensor networks, Comput. Netw. 52 (18) (2008) 3433–3452. http://dx.doi.org/10.1016/j.comnet.2008.09.005.
[45] Y. Ouyang, Z. Le, Y. Xu, N. Triandopoulos, S. Zhang, J. Ford, F. Makedon, Providing anonymity in wireless sensor networks, in: IEEE International Conference on Pervasive Services, 2007, pp. 145–148. http://dx.doi.org/10.1109/PERSER.2007.4283904.
[46] J.-R. Jiang, J.-P. Sheu, C. Tu, J.-W. Wu, An anonymous path routing (APR) protocol for wireless sensor networks, J. Inf. Sci. Eng. 27 (2) (2011) 657–680. URL http://www.iis.sinica.edu.tw/page/jise/2011/201103_16.html.
[47] J. Chen, X. Du, B. Fang, An efficient anonymous communication protocol for wireless sensor networks, Wirel. Commun. Mob. Comput. 12 (14) (2012) 1302–1312. http://dx.doi.org/10.1002/wcm.1205.
[48] A. Juels, RFID security and privacy: A research survey, IEEE J. Sel. Areas Commun. 24 (2) (2006) 381–394. http://dx.doi.org/10.1109/JSAC.2005.861395.
[49] P. Kamat, Y. Zhang, W. Trappe, C. Ozturk, Enhancing source-location privacy in sensor network routing, in: 25th IEEE International Conference on Distributed Computing Systems, ICDCS 2005, 2005, pp. 599–608. http://dx.doi.org/10.1109/ICDCS.2005.31.
[50] H. Wang, B. Sheng, Q. Li, Privacy-aware routing in sensor networks, Comput. Netw. 53 (9) (2009) 1512–1529. http://dx.doi.org/10.1016/j.comnet.2009.02.002.
[51] J. Deng, R. Han, S. Mishra, Decorrelating wireless sensor network traffic to inhibit traffic analysis attacks, Pervasive Mob. Comput. 2 (2) (2006) 159–186. http://dx.doi.org/10.1016/j.pmcj.2005.12.003.
[52] Y. Jian, S. Chen, Z. Zhang, L. Zhang, A novel scheme for protecting receiver's location privacy in wireless sensor networks, IEEE Trans. Wireless Commun. 7 (10) (2008) 3769–3779. http://dx.doi.org/10.1109/T-WC.2008.070182.
[53] A. Jhumka, M. Leeke, S. Shrestha, On the use of fake sources for source location privacy: Trade-offs between energy and privacy, Comput. J. 54 (6) (2011) 860–874. http://dx.doi.org/10.1093/comjnl/bxr010.
[54] L. Yao, L. Kang, P. Shang, G. Wu, Protecting the sink location privacy in wireless sensor networks, Pers. Ubiquitous Comput. (2012) 1–11. http://dx.doi.org/10.1007/s00779-012-0539-9.
[55] M. Shao, W. Hu, S. Zhu, G. Cao, S. Krishnamurthy, T. La Porta, Cross-layer enhanced source location privacy in sensor networks, in: IEEE Conference on Sensor, Mesh, and Ad Hoc Communications and Networks, IEEE Communications Society, (SECON'09), 2009, pp. 1–9. http://dx.doi.org/10.1109/SAHCN.2009.5168923.
[56] R. Rios, J. Lopez, Exploiting context-awareness to enhance source-location privacy in wireless sensor networks, Comput. J. 54 (10) (2011) 1603–1615. http://dx.doi.org/10.1093/comjnl/BXR055.
[57] K. Mehta, D. Liu, M. Wright, Location privacy in sensor networks against a global eavesdropper, in: IEEE International Conference on Network Protocols, (ICNP 2007), IEEE, 2007, pp. 314–323. http://dx.doi.org/10.1109/ICNP.2007.4375862.
[58] M. Shao, Y. Yang, S. Zhu, G. Cao, Towards statistically strong source anonymity for sensor networks, in: The 27th Conference on Computer Communications IEEE INFOCOM 2008, 2008, pp. 466–474. http://dx.doi.org/10.1109/INFOCOM.2008.19.
[59] B. Alomair, A. Clark, J. Cuellar, R. Poovendran, Towards a statistical framework for source anonymity in sensor networks, IEEE Trans. Mob. Comput. 12 (2) (2012) 248–260. http://dx.doi.org/10.1109/TMC.2011.267.
[60] Y. Yang, M. Shao, S. Zhu, B. Urgaonkar, G. Cao, Towards event source unobservability with minimum network traffic in sensor networks, in: ACM Conference on Wireless Network Security, (WiSec'08), ACM, 2008, pp. 77–88. http://dx.doi.org/10.1145/1352533.1352547.
[61] K. Mehta, D. Liu, M. Wright, Protecting location privacy in sensor networks against a global eavesdropper, IEEE Trans. Mob. Comput. 11 (2) (2012) 320–336. http://dx.doi.org/10.1109/TMC.2011.32.
[62] M. Shao, S. Zhu, W. Zhang, G. Cao, Y. Yang, pDCS: Security and privacy support for data-centric sensor networks, IEEE Trans. Mob. Comput. 8 (8) (2009) 1023–1038. http://dx.doi.org/10.1109/TMC.2008.168.
[63] R. Rios, J. Cuellar, J. Lopez, Probabilistic receiver-location privacy protection in wireless sensor networks, Inform. Sci. 321 (2015) 205–223. http://dx.doi.org/10.1016/j.ins.2015.01.016.
[64] R. Rios, J. Lopez, J. Cuellar, Location privacy in WSNs: Solutions, challenges, and future trends, in: Foundations of Security Analysis and Design (FOSAD) VII, Vol. 8604, Springer, 2014, pp. 244–282. http://dx.doi.org/10.1007/978-3-319-10082-1_9.
[65] G.P. Joshi, S.Y. Nam, S.W. Kim, Cognitive radio wireless sensor networks: applications, challenges and research trends, Sensors 13 (9) (2013) 11196–11228. http://dx.doi.org/10.3390/s130911196.
[66] R. Pries, W. Yu, X. Fu, W. Zhao, A new replay attack against anonymous communication networks, in: IEEE International Conference on Communications, ICC'08, 2008, pp. 1578–1582. http://dx.doi.org/10.1109/ICC.2008.305.
[67] N.S. Evans, R. Dingledine, C. Grothoff, A practical congestion attack on tor using long paths, in: Proceedings of the 18th Conference on USENIX Security Symposium, SSYM'09, USENIX Association, Berkeley, CA, USA, 2009, pp. 33–50. URL http://dl.acm.org/citation.cfm?id=1855768.1855771.
[68] Emotiv, Inc., Wearables for your brain, https://www.emotiv.com/ (Accessed 02/2017) (2014).

Javier Lopez is Full Professor at the University of Malaga. His activities are mainly focused on network security, critical information infrastructures protection and security services, leading a number of national and international research projects in those areas, including projects in FP5, FP6 and FP7 European Programmes. Prof. Lopez is the Co-Editor in Chief of the International Journal of Information Security (IJIS) and Spanish representative in the IFIP Technical Committee 11 on Security and Protection in Information Systems. Besides, he is a member of the Editorial Board of the journals Computer Communications, Computers & Security, International Journal on Critical Infrastructure Protection and International Journal of Communication Systems, among others. He is also the Chair

of the ERCIM (European Research Consortium for Informatics and Mathematics) Working Group on Security and Trust Management.

Ruben Rios is a postdoctoral researcher at the University of Malaga. He obtained the B.Sc. from the University of Skövde (Sweden) in 2007 and later the M.S.Eng. and the Ph.D. degrees in Computer Science from the University of Malaga (Spain) in 2008 and 2014, respectively. He has been involved in several national and European projects. His research interests are centred on the notions of privacy, anonymity, and information disclosure, with special interest on its application to Wireless Sensor Networks and the Internet of Things.

Feng Bao is currently the Director of the Security Lab at Huawei. He received his B.S. in mathematics and M.S. in Computer Science from Beijing University, and his Ph.D. in Computer Science from Gunma University, Japan. He was a researcher with Chinese Academy of Science and a Visiting Scientist with Hamburg University. From 1996 to 2012, he was with the Institute for Infocomm Research, A*STAR of Singapore, and took the position of the Principal Scientist and the Head of the Cryptography and Security Dept. His research interests are mainly in cryptography and cyber security. He has published over 200 papers in the international conferences and journals, which have over 5000 citations. He has 16 patents and has been involved in the management of dozens of industry projects and international collaborations. He is a member of Asiacrypt Steering Committee and the Editorial Member of 2 international journals. He has chaired over 20 international conferences in security.

Guilin Wang received the Ph.D. degree in computer science from the Institute of Software, Chinese Academy of Sciences, Beijing, China, in 2001. He is currently a Senior Researcher with Huawei International Pte Ltd., Singapore. He is also currently a Senior Lecturer with the School of Computer Science and Software Engineering, University of Wollongong, Wollongong, Australia. Before this, he was a Lecturer with the University of Birmingham, Birmingham, UK, a Research Scientist with the Institute for Infocomm Research, Singapore, and an Assistant Professor with the Chinese Academy of Sciences. He has authored or coauthored more than 80 research publications in the areas of applied cryptography and telecommunication security. His main research interests include the analysis, design, and applications of digital signatures and security protocols.

Dr. Wang has served as a Program Cochair for six international security conferences, a Committee Member for more than 60 international conferences or workshops, and a Reviewer for over 20 international journals.