§§

FP7-PEOPLE-2012-IAPP

mesh-wise

Self-organising MESH Networking with Heterogeneous Wireless Access

D2.1: Wireless environment sensing: gathering & storing datasets of network primitives

Report

Contractual date of delivery to EC: Month 18
Actual date of delivery to EC:
Available online as of:
Lead beneficiary: ULUND
Nature: PUBLIC
Version: 1.0

Project Name: Self-organising MESH Networking with Heterogeneous Wireless Access
Acronym: MESH-WISE

Start date of project: 01/03/2013 **Duration:** 48 Months
Project no.: 324515

Project funded by the
European Commission under the
People: Marie Curie Industry-Academia
Partnerships and Pathways (IAPP)
Programme of the 7th Framework
FP7-PEOPLE-2012-IAPP

MARIE CURIE ACTIONS
SEVENTH FRAMEWORK PROGRAMME

Document Properties

Document ID	PEOPLE-2012-IAPP-324515-MESH-WISE-D2.1
Document Title	*Wireless environment sensing: gathering & storing datasets of network primitives, Report.*
Lead Beneficiary	Lund University
Editor(s)	Bjorn Landfeldt, Lund University
Work Package No.	2
Work Package Title	*Distributed resource management and self-organisation*
Nature	Report
Number of Pages	45
Dissemination Level	**PU**
Revision History	Version 1
Contributors	ULUND: Björn Landfeldt, Yuan Li Forthnet: George Vasilakis LiU: Vangelis Angelakis FORTH: Elias Tragos, Alexandros Fragkiadakis MobiMESH: Stefano Napoli, Alberto Pollastro, Biagio Passaro

Contents

1 Executive summary

In order for wireless mesh networks to be able to self-configure to adapt to changing operational conditions, it is necessary for the nodes to be able to sense the environment in order to determine the operational state of the system. The state is then used to compare against potential optimization outcomes.

In the MESH-WISE project we consider both nodes that participate in network access infrastructure as well as wireless sensor nodes which form part of a future Internet of things infrastructure scenario. We therefore focus on two aspects of the sensing, first, channel state sensing for determining configuration actions which will improve network capacity and lower delays and second, sensing of the environment for data management in sensor networks. This work also includes security aspects of data management in these networks.

We have made good progress in these two areas and produced a number of tangible outcomes in the form of publications. Furthermore, implementations of some of the results have been made in a mesh management framework at MobiMESH.

2 Sensing of the wireless channel state

One of the fundamental primitives of 802.11-based WLAN standards is the sensing of the channel state before transmission. The sensing is used to inform transmitting nodes about the occupancy of the medium so an informed decision can be made whether or not to access the channel.

The fundamental scheme known as Carrier Sense Multiple Access (CSMA) was first introduced in the 1970s as an improvement over the then existing pure random access method called ALOHA. In 1975, Kleinrock and Tobagi [1] published their seminal work on the performance of the CSMA scheme under varying system loads. However, the modelling is very intricate and extending it to cover a full implementation of a 802.11 protocol leads to models that are difficult to work with. Instead, in 2000 Bianchi [2] presented an alternative model, which approximated the system by considering full load, i.e. all nodes always have non-empty send buffers. This model have been the most used ever since because of its relative simplicity.

However, in our work in MESH-WISE we have investigated the effects of channel sensing and discovered that the simplistic view taken in CSMA is not suitable for modern WLAN standards [3, APPENDIX A]. Our findings show that the increasing data rates in modern WLAN standards coupled with a trend towards smaller frames in mobile systems lead to CSMA being inefficient and sometimes worse performing than the ALOHA scheme. In short, sending a frame is so fast that it takes longer to wait to sense the channel and one of two problems may occur. First, valuable transmission opportunities may be lost while sensing and second, the sensed information is outdated during the transmission of a frame.

Our findings are therefore that the sensing has to be done on higher quality information than previously used and active sharing of deterministic information becomes an exciting alternative to pure random access. Our work is now focussing on the effectiveness of different cooperative schemes where information sharing sits at the core of the chan-

nel access mechanism. We have thus shifted the nature of the sensed information and found that this can be done without requiring significantly more complex sensing or signalling.

3 Sensing for data management in wireless sensor networks

We divide the work in this area into two separate categories, efficient information sensing and secure information sensing.

3.1 Efficient information sensing

In Wireless Sensor Networks (WSN), most of a sensor's energy is consumed for channel sensing and data transmission. Due to the broadcast nature of the wireless medium, a sensor consumes energy for sensing every packet transmitted by its one-hop neighbors. Likewise, a sensor consumes energy for the transmission of raw monitored data (or relaying of peers' data). In order to minimize the energy consumption due to transmit and carrier sense, efficient data collection is of paramount significance.

We propose a novel data collection scheme based on compressed sensing and matrix completion. In a nutshell, this technique takes advantage of intra-temporal correlation of sensor readings and the inter-spatial correlation of the data gathered by different sensors and forwarded to a sink node [4, APPENDIX B]. If the sensed data is sparse, using compressed sensing in a sensor results in using fewer samples for encoding data, and thus fewer packet transmissions are needed for the data to be reported. The use of matrix completion technique in the sink node enables reconstructing the reported compressed data even in the presence of packet loss as a common issue in random access wireless networks.

Our findings [4, APPENDIX B] show that the proposed technique performs substantially well (with less than 10% error) under relatively high packet loss rates (as high as 40%) and very high compression rates (as high as 75%). Also, the use of this technique leads to substantial reduction of energy consumption.

3.2 Secure information sensing

With the introduction of SmartCity applications realized by WSNs, the security issues and the appropriate countermeasures becomes highly crucial for these network to succeed. Furthermore, the increasing demand for spectrum triggered by the growth of applications highlights the use of cognitive radio as a potential solution for efficient spectrum sharing, which in turn triggers new types of security threats. We identified the various security and privacy threats common to both WSNs and cognitive WSNs and also those threats unique to the latter type of WSNs [6, APPENDIX D]. We further classified the security attacks with respect to the architectural layers of WSN. Countermeasures and the open challenges are specified, which can be used as a reference for future research [6, APPENDIX D].

Energy efficient data collection is embraced as a technique to extend the lifetime of WSNs, however, it can also be used as an incentive for malicious nodes to efficiently collect data, compromise privacy, and plan more serious attacks. In [5, APPENDIX C], we showed how malicious nodes can use compressed sensing and matrix completion technique [4, APPENDIX B] to detect some application features (e.g., periodicity) and thereby detect the nature of the application. Our findings reveal that malicious nodes can successfully detect the periodic components of the captured wireless traffic for high compression ratios.

4 PHY/MAC sensing for routing optimization

Considering the backbone network component of a wireless mesh network, it can be easily seen that the overall performance can be greatly improved if the routing techniques could gather and employ information from the PHY and the MAC layers and employ them to perfect the routing metric.

Two of the major issues that shall be kept in account when considering routing in a wireless mesh backbone scenario are:

- the physical rate of the link: since IEEE 802.11 interfaces employ rate adaptation algorithms to adapt the rate to the environment conditions; therefore the metrics that employ the nominal link rate are not effective on such networks, and the sensing of the instant link rate is needed;

- the intra flow interference: in meshed networks the shortest path may cross two consecutive links employing the same frequency, which would lead to dramatic performance losses; such interference shall therefore be detected and avoided through proper metrics.

We have investigated these two dimensions and implemented the core parts of a sensing framework in the MobiMesh architecture as detailed below:

4.1 Physical link rate detection

In wired networks, the transmission rate is constant and it is the same for the entire physical transmission range. As opposed, in IEEE 802.11 wireless net- works is possible to employ different rates to transmit. The reason of multi-rate capability is directly related on wireless communication characteristics. There is a direct relationship between the rate of communication and the quality of the channel required to support that communication reliably. Since distance is one of the important factors that determines wireless channel quality, there is an inherent trade-off between high transmission rate and transmission range, this occurs for the reason that low rates use stronger modulations to channel degradations so low rates has longer range than high rates. Wireless channels are unpredictable, can be very instable and vary quickly, then transmission rate should dynamically changes for adapt to the environment conditions. Therefore, different rates are chosen according to signal strength received.

There are several rate control algorithms which perform rate adaptation, most important are ONOE, ARF and SampleRate.

4.1.1 Link quality metrics

It is possible to collect and calculate link quality parameters and characteristics at the MAC and PHY level. These particular parameters referred to medium are managed by the wireless driver in order to correctly handle the wireless connection. There are multiple metrics based on the link quality, several metrics are employed internally by driver whereas other can be calculated. The most important metrics are: average medium busy time, average medium busy transmit time, average medium busy time, receive time, MAC layer delay, link transmission rate, link frame size. In the following two very interesting metrics related to the quality of the link will be explained. These metrics are complex to calculate and could be employed in the future by ad-hoc routing protocols in order to improve performance.

4.1.1.1 Busy time

A node is defined to be busy if it is transmitting or receiving. A node is consid- ered to be transmitting not only if it is emitting power through its antenna, but also if it is performing tasks related to frame transmission which may include interframe space, backoff time, etc. A method has been defined in order to obtain the average busy time. Every time a packet is sent with or without success, the sender node is busy for a period of time. With some calculations based on the various IEEE 802.11 standards, it is possible to calculate how long the sender is busy for each transmitted frame. Similarly, every time a packet is received, it is possible to calculate how long it has kept the receiver busy. This method of getting the busy transmit and busy receive time of a node requires precise technical details about each sent or received frame; then, it is possible to compute the busy time.

4.1.1.2 Bandwidth availability

A list of all neighboring nodes is kept in memory. For each of them, the rate of the last frame is kept in memory, as well as other PHY characteristics. The last rate used to a destination is reported as the current rate of the link. The available bandwidth to a destination depends on the rate and PHY used to that destination. It depends on the availability of the medium and on the frame size as well. The current rate and PHY of a link is known already. The medium availability is known through the computed percentage busy time described previously, the percentage of idle time is equal to 100% - percentage busy time. The frame size of future transmissions cannot be known in advance. There- fore, is possible estimate the available bandwidth of a link selecting a frame size. IEEE 802.11 vary size from 132 bytes the short size frames to 2346 bytes the long size frame. Hence, the available bandwidth is calculated from divide size of the packet by time spent to send the packet that includes transmission time, waiting time and time for acknowlegment.

4.1.2 Radio link metrics

To be as much as possible aware on the radio link conditions, is it possible to outline several important parameters which are characteristics in particular of wireless links; these parameters can be used to take accurate routing decisions. The information related to radio conditions can be gathered by wireless driver that works at the PHY and MAC level. In fact, wireless driver employs measures of the received signal strength for some functions such as decide weather the channel is free or busy. In the following, some radio metrics will be presented.

4.1.2.1 Signal strength

The signal strength is the measure of how strong a received signal is. Accord- ing to this parameter, the wireless driver can determine the channel status or the quality of a link, and then to decide how reliable is. In addition, it could be a usefully parameter in order to compare the signal received between differ- ent nodes and perform roaming tasks when needed. Information about signal strength belongs to physical layer. The IEEE 802.11 standards have defined the Receive Signal Strength Indicator (RSSI) that is a numeric value with range of 0-255 which represent the measured signal power by the wireless NIC. The value of RSSI is no standard and each vendor employs its own measured mechanism to its devices, therefore by now, is not appropriated to use as a parameter in routing metrics.

4.1.2.2 Bit rate

The transmission bit rate parameter permit to determine the link transmission speed. The IEEE 802.11 standards permit multiple bit rates, these rates can be applied frame by frame. The standard does not specify how to choose the physical transmission rate, there are several algorithms that set the transmission rate. Rate control algorithms choose transmission rate depending on the channel quality. Using the transmission rate and the frame size is possible to calculate the transmission time for a frame. Transmission rate as well as transmission time are interesting parameters to be applied as a metric in routing protocols because they can lead to select best routes available.

4.1.2.3 Bandwidth

The bandwidth parameter denote the link capacity. Bandwidth measures the amount of data that can travel through a link. Usually is expressed in bits per second (bps). Bandwidth measurement for a wireless link is a complex process. This value can provide important information in order to avoid bottleneck nodes, allowing the choice of high throughput nodes in route selection. Furthermore, the wireless channel is a shared access medium, hence the bandwidth varies with depending on the number of hosts that contend for the channel. Another effect that affect bandwidth is observed in multi-hop networks with a single radio interface where the bandwidth is halved on every hop. The are particular definitions of bandwidth. The available bandwidth is defined as the available capacity and is different of bandwidth that is referred to the maximum capacity.

The estimated bandwidth is the expected capacity that will can be used. Bandwidth is a very useful parameter in order to improve route selection.

4.1.3 Link rate retrieving

The rate selection algorithms implemented by the IEEE 802.11 drivers collect data evaluating the information introduced in the previous sections in order to select the best transmission rate to be used when transmitting data to a specific destination. They also continuously analyze and monitor the channel to adapt the transmission rate to the changing conditions of the environment.

Therefore in order to make the routing decision aware of the radio link quality, the best indicator is the rate selected by the driver itself through its rate selection algorithm; it is in fact a value selected among a standardized set (the defined IEEE 802.11 transmission rates) that summarizes all the values presented in the previous sections in a single, "environment estimation" parameter.

The fact that the selected value is chosen from a standardized set is very important because it will let us to use the selected rate for a link as an indicator of the link quality independently from the rate selection algorithm itself; therefore we can decouple the radio aware routing algorithm from the rate selection algorithm, and thus swap the latter without changes to the former.

4.2 Intra flow Interference

Various problems arise when equipping wireless mesh nodes with multiple antennas. Existing routing protocols can still be used and will provide connectivity in WMNs, but no optimal throughput can be expected due to the characteristics of the wireless medium. In this section we will talk about problems in WMNs when equipping mesh nodes with multiple wireless interfaces.

Two types of collision can be observed in wireless networks. Both of them are already foreseen in the standardization of the IEEE 802.11 standards. The first collision type is direct collision where two wireless devices, tuned to the same channel, within range of each other try to transmit at the same time. The mechanisms to react on this type of collision are based on the CSMA/CA model implemented by the IEEE 802.11 standard. The hidden node problem is the second kind of collision foreseen in the IEEE 802.11 MAC layer. The RTS/CTS mechanisms to prevent this collisions are implemented to handle this situation. Those mechanisms can be activated when needed and are not obligatory. It becomes quite clear, that in a dense area, like a WMN, with many nodes using the same channel, those collisions happen even more frequently. This will clearly limit capacity and throughput in those networks. One suggested solution to this is the usage of wireless nodes this multiple wireless interfaces tuned to different channels. This will decrease the traffic on each channel and hence produce less collisions.

Various sources can create interference in wireless networks. But not only undesired effects in the environment can cause interference in WLANs. Interference can be caused by other nodes in the coverage area of a node, when using the same or overlapping channels. When data is transmitted from one node to another, various nodes can partici-

pate in the transmission. If nodes, sensing each other, participating in this transmission use overlapping channels for this transmission they create interference along this way, as those can not send while another node is sending on the same channel. This effect can even be observed at a node passing on information on a channel that is overlapping with the one used for receiving this data. This type of interference is called *intra-flow interference*. Interference can also be caused by nodes not transmitting the same data flow. If they are within sensing range of each other and use overlapping channels, they cannot send or receive at the same time. This type of interference is called *inter-flow interference*.

As seen in table 2.1 on page 6 in the IEEE 802.11g standard up to 14 different channels are defined. As the frequencies of adjacent channels are overlapping those 14 channels can never be fully interference free used. In fact only a maximum of 3 non overlapping channels can be used at the same time. Even in the IEEE 802.11a standard, defined with a maximum of 27 non overlapping channels, some problems can be observed. It has been noted by [7] that at single node equipped with multiple wireless interfaces, interference between adjacent non overlapping channels can arise. This means that the number of channels that can be used without creating interference for one node is smaller than the total number of available channels. It has been proven experimentally that by increasing the distance between interfaces the interference can be diminished [8]. This means that even though many channels are defined in the 802.11 standards, channel selection has to be done carefully in order to avoid high interference.

Summarizing, it can be said, that various problems arise in WMNs. This problems are often connected with the usage of wireless links. Therefore recent research points to equipping wireless nodes with multiple wireless interfaces. By tuning each wireless interface to a different, non overlapping channel, problems like interference and collisions can be mitigated. Two aspects have to be considered. First, this channel assignment can not be done on a random base, as network fragmentation or bad routes can be caused. Furthermore, the used routing protocol has to be aware of the different used channels and try to balance the traffic in a WMN on a link and channel basis. In a WMN with both, a good channel assignment, and channel aware routing protocol collisions can be reduced significantly and throughput and capacity of the WMN increased.

As stated above, the routing protocol decisions must be related to the information about the radio channel assignment in order to make multi-radio devices effective in increasing the network performances. Therefore we'll design and implement an intra-flow interference identification algorithm in order to be able to detect and possibly avoid intra-flow interference; also, we'll define a routing metric that will take such interference into account while taking routing decisions in order to minimize it and completely avoid it wherever possible.

5 Conclusions

We have made good progress with the work on sensing and information management/storage in the project. Certain practical implications will need to be revisited as

technical solutions are derived in the later part of the work as necessary. Apart from publications and seminars where we have reported our results, we have had ongoing work to implement parts in the Mobimesh management framework, which was also demonstrated during the July project outreach in Heraklion, Greece. We are therefore confident in moving forward towards work on effective management and configuration solutions in the project.

6 References

[1] L. Kleinrock and F. Tobagi, "Packet Switching in Radio Channels: Part I -- Carrier sense multiple-access modes and their throughput-delay characteristics", IEEE Trans. Communications Vol 23 issue 12, 1975.

[2] G. Bianchi, "Performance analysis of the IEEE 802.11 distributed coordination function", IEEE JSAC, vol. 18 issue 3, 2000, pp. 535-547.

[3] E. Fitzgerald and B. Landfeldt, "The Failure of CSMA in Emerging Wireless Network Scenarios", Submitted to IFIP Wireless Days 2014

[4] A. Fragkiadakis, I. Askoxylakis, E. Tragos, "Joint compressed-sensing and matrix-completion for efficient data collection in WSNs", in proc. IEEE CAMAD, Berlin, Germany, Sep 2013.

[5] A. Fragkiadakis and I. Askoxylakis, "Malicious traffic analysis in wireless sensor networks using advanced signal processing techniques", in proc. IEEE D-SPAN, Madrid, Spain, June 2013.

[6] A. Fragkiadakis, V. Angelakis and E. Z. Tragos, "Securing Cognitive Wireless Sensor Networks: A Survey", International Journal of Distributed Sensor Networks, vol. 2014, Article ID 393248, March 2014.

[7] Richard Draves, Jitendra Padhye, and Brian Zill, editors. Proceedings of the 10th annual international conference on Mobile computing and networking, Philadelphia, Pennsylvania, USA, 2004. ACM. Routing in Multi-Radio, Multi-Hop wireless Mesh Networks, pages 114-128.

[8] Ashish Raniwala and Tzi cker Chiueh. Architecture and algorithms for an ieee 802.11-based multi-channel wireless mesh network. Proceedings of IEEE International Conference on Computer Communications, 2005.

Appendices

E. Fitzgerald and B. Landfeldt, "The Failure of CSMA in Emerging Wireless Network Scenarios", Submitted to IFIP Wireless Days 2014

A. Fragkiadakis, I. Askoxylakis, E. Tragos, "Joint compressed-sensing and matrix-completion for efficient data collection in WSNs", in proc. IEEE CAMAD, Berlin, Germany, Sep 2013.

A. Fragkiadakis and I. Askoxylakis, "Malicious traffic analysis in wireless sensor networks using advanced signal processing techniques", in proc. IEEE D-SPAN, Madrid, Spain, June 2013.

A. Fragkiadakis, V. Angelakis and E. Z. Tragos, "Securing Cognitive Wireless Sensor Networks: A Survey", International Journal of Distributed Sensor Networks, vol. 2014, Article ID 393248, March 2014.

Appendix A

The Failure of CSMA in Emerging Wireless Network Scenarios

The Failure of CSMA in Emerging Wireless Network Scenarios

Emma Fitzgerald*, Bjorn Landfeldt†
School of Electrical and Information Technology
Lund University
SE-221 00 Lund
Sweden
Email: *Emma.Fitzgerald@eit.lth.se, †Bjorn.Landfeldt@eit.lth.se

***Abstract*—The current family of 802.11 protocols are based on the Carrier Sense Multiple Access (CSMA) mechanism which is a simple and robust means of sharing a channel. However, two current trends in wireless networks point towards a situation where CSMA fails to perform better than pure random access solutions such as ALOHA. The first trend is the ever increasing raw data rate in each generation of 802.11 which is set to continue with the current 802.11ax standardisation. The second is the move towards smaller frames as end users increasingly use mobile devices instead of desktop computers. We show that as the ratio of propagation delay to packet transmission time increases, the probability of sensing incorrect information about the channel state increases correspondingly, to the point where ALOHA outperforms CSMA. This leads to a need to develop new wireless MAC protocols with an increased focus on information sharing and co-ordination between nodes.**

***Index Terms*—CSMA, 802.11, 802.11ax, wireless LAN, MAC**

I. Introduction

Carrier Sense Multiple Access (CSMA) has been in use in wireless LANs for more than two decades. It provides a simple but effective means of negotiating medium access between multiple nodes without requiring a centralised controller or extensive configuration. However, the landscape for unlicensed spectrum wireless networks appears very different today than when CSMA was first developed and these changes can potentially have a large impact on the effectiveness of carrier sensing, the central mechanism in CSMA.

There are two main changes occurring in wireless LANs that affect the performance of CSMA. The first is increased raw data rates, leading to shorter frame transmission times. The second change we are seeing is an increased number of short packets, which incur higher proportional overhead. The trend is toward mobile devices and current studies show that the average frame size is very small in these networks.

Carrier-sensing is vulnerable to collisions whenever a node senses the channel state within one propagation delay of the beginning of another node's transmission. This becomes increasingly likely as data rates increase and packet sizes decrease, since the proportion of transmission time represented by periods vulnerable to incorrect sensing (and thus collision) increases. In this paper we will explore these trends and provide analysis, based on the model of CSMA developed in [1], demonstrating that we are now reaching the limits of the usefulness of CSMA and thus require a new approach to MAC protocols for wireless LANs.

Data rates are increasing with improved physical layer technologies. Table I shows the advancements in 802.11 raw data rates over time. Further, the new 802.11ax standard aims to achieve at least a four times increase in data rate [2]. An examination of the protocol overheads, however, reveals that many are not dependent on the data rate and thus are more detrimental to efficiency at higher data rates.

Inter-frame spaces, time spent transmitting acknowledgements and management traffic, and headers all detract from the channel capacity available to transmit data from higher layer applications [3]–[5]. In addition to this, the contention window mechanism — employed when a node wishes to transmit but cannot because the channel is already busy — also affects the maximum achievable throughput [5]–[7]. A poorly chosen contention window can result in either idle time, when all nodes are waiting for their randomly selected transmission slots and no node is actually transmitting yet, or collision, if two or more nodes choose the same slot.

However slot times, which are the basis for inter-frame spacing and backoff times, are based not on data transmission times but rather on the propagation delay [8]. This means that as data rates go up, a higher proportion of the channel time is devoted to these overheads rather than to transmitting useful data. Some mechanisms have been developed to mitigate this problem, in particular frame aggregation [9]–[12], so that more data is sent in between each instance of header, acknowledgement, inter-frame spacing and backoff. Nonetheless, trends in the traffic patterns in wireless LANs and in how these networks are used show that simply moving to larger and larger frames is not a comprehensive answer to the problems of inefficiencies in CSMA protocols.

A recent study of packet sizes in 802.11 networks in Boulder, Colorado shows a large proportion of small packets being transmitted [13]. In both residential and managed enterprise environments, packets of less than 300 bytes predominated. Moreover, usage patterns in wireless LANs are changing, with increases in uplink traffic from many different nodes; real-time, delay-sensitive traffic; and low-frequency sensor traffic such as needed for smart homes and the Internet of Things [14]–[18]. These traffic types are not well suited to frame

Standard	Year	Max data rate (Mb/s)	Frequency (GHz)
802.11	1997	2	2.4
802.11a	1999	54	5
802.11b	1999	11	2.4
802.11g	2003	54	2.4
802.11n	2009	150	2.4, 5
802.11ac	2013	866.7	5

TABLE I
DATA RATES OF 802.11 STANDARDS [8]

aggregation.

As our results will show, CSMA is inherently unsuited to networks in which packet transmission times are short, as is the case with high data rates and small packets. Instead, a new class of MAC protocols is needed in order to improve the reliability of the information nodes have about the channel state and when they should transmit. This can be achieved through greater co-ordination and information sharing between nodes. However, care must be taken to not unduly increase overhead or introduce incompatibility with existing protocols.

The rest of this paper is organised as follows. Section II discusses related work. Section III then gives an overview of the model presented in [1] and Section IV describes our implementation of this model and results for small packet transmission times. In Section V, we analyse the utility of channel sensing as a function of propagation delay relative to packet transmission time. Section VI outlines an approach to moving beyond the limitations of CSMA and finally Section VII concludes this paper.

II. RELATED WORK

There is a large body of existing work addressing various aspects of CSMA performance under many different conditions and assumptions. Bianchi's model [19] has been particularly influential, with numerous further developments following on from it [20]–[24]. There are some limitations of the Bianchi model that make it unsuitable for our purposes, however. The Bianchi model captures the behaviour of CSMA when the network is at saturation, that is, when every node always has a packet queued to send. This makes certain simplifications possible. In particular, there is no notion of packet transmission time, since the packet arrival rate does not need to be considered. Collisions are also only modelled when nodes choose the same backoff counter value, not when nodes sense the channel during one propagation delay after the beginning of a packet. This makes sense under saturation conditions where no packet will arrive during this vulnerable period as all nodes already have a packet waiting at all times. There have been some extensions of this work to non-saturated conditions (e.g. [20], [24], [25]), however one or more of these limitations still remain in each case.

We wish to study the combined effect of increasing data rates and short packets and as such, we need to explicitly model packet transmission time. Collisions due to sensing during a vulnerable period are also a significant factor under these circumstances, as our results will demonstrate, so they cannot be neglected. Further, we would like to examine network behaviour not just under saturation conditions but also under lighter loads, and in particular how quickly the channel reaches saturation under increasing loads.

In order to investigate the effects of high data rates, small packets and non-saturation conditions, we instead take as our starting point the model developed by Kleinrock and Tobagi [1]. This model incorporates explicit modelling of packet transmission time relative to the propagation delay and varying offered load. While it focuses on p-persistent CSMA and its variants, rather than 802.11, its results are nonetheless applicable to any CSMA protocol, particularly for the aspects we wish to consider. Section III will give a more detailed explanation of this model.

A number of simplifying assumptions are made in the model in order to make the analysis tractable. In particular a common packet size and propagation delay across all nodes is used, and the network consists of an infinite number of nodes collectively forming a Poisson-distributed packet arrival process. These assumptions will of course not be true in any realistic network, however they are reasonable for examining the theoretical throughput achievable in CSMA. In particular, realistic traffic models following the bursty, self-similar traffic patterns characteristic of internet traffic [26]–[29] are likely to exacerbate the problem of collisions due to channel sensing during vulnerable periods rather than mitigate it, so the Poisson model represents a best performance bound for this work. Analysis using a finite number of nodes is developed in [30], however this leads to a significantly more complex model. In addition, an infinite population model is a good approximation for a large number of nodes and we are particularly interested in high-density networks such as those targeted by 802.11ax.

III. KLEINROCK AND TOBAGI CSMA ANALYSIS

Kleinrock and Tobagi developed a model in [1] for analysing the throughput and delay characteristics of a number of CSMA variations, along with ALOHA and slotted ALOHA [31]. The CSMA protocols considered primarily differ in their persistence scheme. In this paper, we will focus on p-persistent CSMA as it is the most similar to the 802.11 protocols in widespread use today, however [1] also provides results for non-persistent and 1-persistent CSMA, in both slotted and unslotted variants.

We will first introduce some notation used in [1], which is necessary in order to understand and discuss the analysis based on this model. Kleinrock and Tobagi characterise MAC protocols in terms of throughput, denoted by S. In this model, all packets are considered to be of the same length and as such, time is normalised to the packet transmission time T. S is then the number of packets transmitted per packet transmission time, with $S \in [0, 1]$. If packets were able to be perfectly scheduled with no collisions and no idle time between transmissions (which is not actually achievable with the protocols considered), S would thus be equal to 1. We also have the offered load, G ($G \geq S$), which is the number

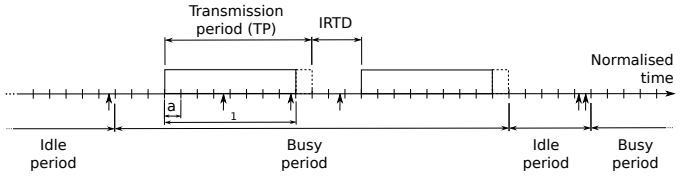


Fig. 1. p-persistent CSMA cycle as described in [1]. Vertical arrows indicate packet arrivals.

of packets, including retransmissions of previously collided packets, that nodes collectively attempt to transmit on the channel per packet transmission time.

A particularly important parameter for our work is a, the ratio of the propagation delay to the packet transmission time. Since in this model time is normalised to the packet transmission time, a is then simply the propagation delay expressed in units of T. Lastly we have p, the persistence parameter. A node which senses the channel busy will first wait until the end of the current transmission, and then attempt to transmit with probability p, or wait one slot time (equal to a) with probability $1-p$. This is then repeated for every slot until the node transmits its packet, either successfully or unsuccessfully (i.e. resulting in a collision).

The p-persistent CSMA protocol as described in [1] follows a cycle consisting of an idle period followed by a busy period (see Figure 1). During an idle period, no packets are transmitted on the channel and no nodes have packets queued to send. An idle period ends when a packet arrives at a node ready to be transmitted. The system then enters a busy period. Note that during a busy period, the channel itself is not constantly busy, that is, a signal is not present on the channel the entire time. This is because some of the time is spent with nodes waiting to transmit, according to the persistence scheme.

The node (or potentially more than one node, each with its own packet to transmit) where this packet is queued then follows the p-persistence protocol to determine a slot in which to start the actual transmission of the packet. This transmission is referred to as a transmission period (TP) and ends one propagation delay (a) after the node has completed transmitting the packet. The transmission can either be successful, if no other node attempts to transmit at the same time, or result in a collision, if two or more nodes transmit at once. In the latter case, the colliding packets are then rescheduled for retransmission.

If any packets arrive (at any node) during the TP, the nodes with packets queued perform the p-persistence scheme to determine, at each slot, whether they will attempt to transmit. The system then experiences an initial random transmission delay (IRTD) of zero or more slot times, during which the channel is idle. It is possible for more packets to arrive during this time, in which case these nodes will also use the persistence scheme to decide when to attempt transmission. Once at least one node begins a new transmission in a slot, a new TP occurs (which, again, may be successful or result in collision). This process continues until such time as there are no nodes with packets queued for transmission at the end of a TP. The system then enters the next idle period — and thus the start of the next cycle — one propagation delay after the end of the last TP.

T	Packet transmission time for a single packet, normalised to 1
S	Throughput; the number of packets transmitted per T seconds
G	Offered load; number packets to transmit per T seconds
TP	Transmission period (see Figure 1)
p	Persistence parameter; the probability a node will attempt to transmit in any given slot
a	Ratio of propagation delay to packet transmission time
$\bar{B}$	Duration of a busy period (see Figure 1)
$\bar{I}$	Duration of an idle period (see Figure 1)
IRTD	Initial random transmission delay (see Figure 1)
$\bar{m}$	Average number of TPs in a busy period
$\bar{t}$	Average number of slots in an IRTD

TABLE II
NOTATION USED IN THIS PAPER AND IN [1]

The average length of a busy period is denoted by $\bar{B}$ and the average length of an idle period by $\bar{I}$. The total average length of a cycle is then $\bar{B}+\bar{I}$. The average number of slots in an IRTD is denoted $\bar{t}$. Expressions for these values are derived in [1]. Lastly, we will denote average number of TPs in a busy period by $\bar{m}$ (not used in [1]). A summary of notation can be seen in Table III.

IV. Large a analysis

In [1], only results for relatively small values of a are presented, as these were values that were reasonable for the data rates and traffic patterns in use at the time of publication. We developed a sofware implementation of the model from [1] and now present analysis for larger values of a.

Figures 2 and 3 show throughput vs offered load for the various MAC protocols included in the analysis — ALOHA, slotted ALOHA, non-persistent CSMA; slotted non-persistent CSMA, 1-persistent CSMA, slotted 1-persistent CSMA and p-persistent CSMA (here with $p=0.1$) — with decreasing a values. As can be seen in the figures, as a grows larger, throughput decreases dramatically, eventually to the point that the CSMA protocols perform worse than slotted ALOHA — that is, we eventually gain nothing by sensing the channel and can do no better than pure random access.

To understand why this is the case, it is helpful to consider the probability that there will be a collision when a node attempts to transmit a packet. As discussed in [1], the probability of a successful transmission is given by $\frac{S}{G}$ and hence the collision probability is $1-\frac{S}{G}$. Figures 4 and 5 show the collision probability as a function of offered load for the same values of a as in Figures 2 and 3, again with $p=0.1$.

We see that the probability that a packet will encounter a collision using CSMA increases as a increases, eventually becoming greater than that for slotted ALOHA. More time is thus wasted transmitting interfering packets that do not result in data being received successfully, reducing the channel utilisation.

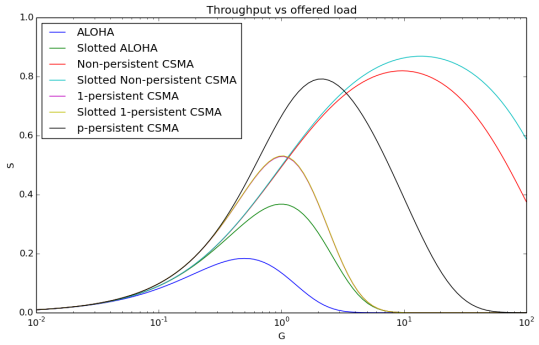


Fig. 2. Throughput vs offered load for various wireless MAC protocols, $a = 0.01$

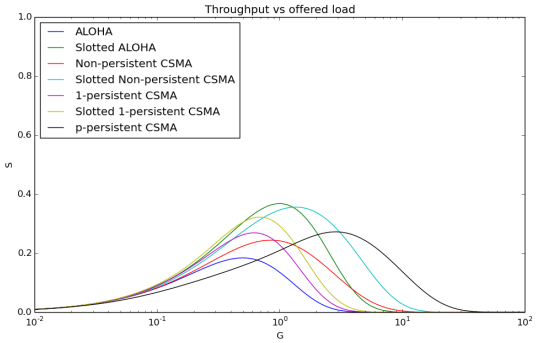


Fig. 3. Throughput vs offered load for various wireless MAC protocols, $a = 0.5$

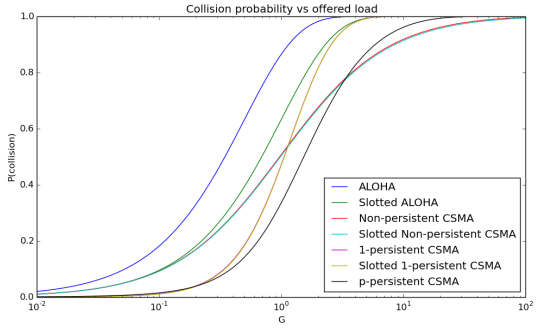


Fig. 4. Collision probability for various wireless MAC protocols, $a = 0.01$

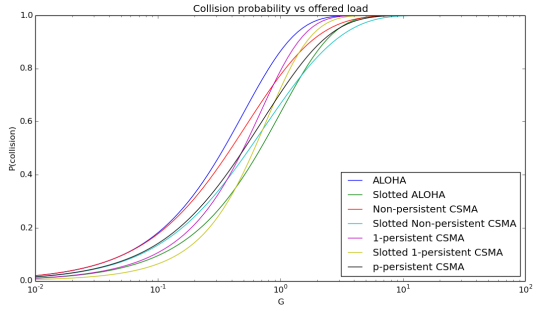


Fig. 5. Collision probability for various wireless MAC protocols, $a = 0.5$

A. Discussion

That the collision probability increases as a increases is a direct consequence of the reason for encountering collisions

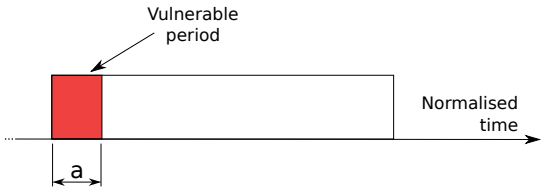


Fig. 6. Period during a transmission that is vulnerable to collision

in CSMA. We first need to distinguish between the two types of collisions possible using CSMA protocols. The first occurs when two nodes are in a backoff state after sensing that the channel is busy, and then choose to retry transmission at the same time. This type of collision can be a large source of overhead if many nodes are waiting to transmit and we are using a small p value (or small contention window size in 802.11). However, the rate of these collisions does not depend on a; it is instead a function of p (or contention window size). Hence these collisions do not account for the rise in collision probability with increasing a.

The second type of collision occurs when a node senses the channel within one propagation delay of another node starting a transmission (see Figure 6). During this vulnerable period, the signal from the transmitting node has not yet reached the sensing node and thus goes undetected. The sensing node sees the channel as free even though it is actually busy. These vulnerable periods occur only at the beginning of packet transmissions and as a increases, they account for a higher proportion of the time the channel is busy. Thus the likelihood of sensing the channel during a vulnerable period increases, resulting in an increased collision probability. In Section V we will explore this further and derive expressions for the probability of obtaining incorrect information when sensing the channel.

Although the Kleinrock and Tobagi model deals with p-persistent CSMA, the problems discussed in the preceding sections apply just as much, if not more, to actual CSMA protocols in use today such as the 802.11 family of protocols. Figure 7 shows the maximum throughput of p-persistent CSMA, according to the model in [1], for a variety of network diameters, packet sizes and data rates. Each of these parameters contribute to the value of a in a real network: the data rate and packet size together determine the time taken to transmit a packet, while the network diameter determines the maximum propagation delay between any pair of nodes. Today, with 802.11ac, a data rate of 500Mb/s is achievable and as can be seen in the figure, the maximum achievable throughput is poor — even below slotted ALOHA — at small packet sizes.

V. Utility of Channel Sensing

The primary aim of any MAC protocol is to attempt to separate transmissions in time such that a node will, ideally, only transmit when no other node is transmitting. Each node, when it has a packet queued to send, attempts to determine when the channel is free for transmission and we can characterise

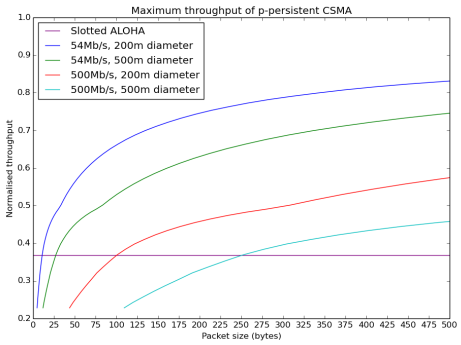


Fig. 7. Maximum throughput of p-persistent CSMA for different data rates, network diameters and packet sizes

MAC protocols in terms of the accuracy with which nodes are able to do this. There are two possible types of errors a node can make when attempting to determine when to transmit. It can either incorrectly perceive the channel to be available when it is not, leading to a collision as two nodes attempt to transmit at once, or else it can incorrectly perceive the channel as busy when it is in fact available, leading to wasted time as the channel lies idle even though there are nodes with packets queued for transmission. In ALOHA, only the first type of error is possible since nodes never check whether the channel is busy but simply assume it to be available at any time, and only discover in retrospect (due to lack of acknowledgement) that this was not the case.

The goal of CSMA is to use channel sensing to gather more information about the channel state before transmitting. However, the information gathered is not perfect — it does not exactly match the true channel state at any given time. Sensing will lag behind the true channel state by the amount of time it takes a signal to propagate from a transmitting node to a sensing node. The network diameter, that is, the maximum distance between any two nodes, gives an upper bound on the propagation delay. In [1], all pairs of nodes are considered to have the same propagation delay. This simplifies the analysis and will result in conservative estimates of the information gain from performing channel sensing.

We can consider CSMA in terms of two random variables: the true channel state and the state as sensed by a node. To determine the accuracy — and hence usefulness — of the information obtained through channel sensing, we can take the correlation between the sensed channel state and the true channel state. Throughout this section, we will discuss p-persistent CSMA, however, 1-persistent CSMA and non-persistent CSMA are special cases of this protocol for $p = 1$ and $p = 0$ respectively.

Given random variables X and Y with expected values μ_X and μ_Y, and standard deviations σ_X and σ_Y respectively, the correlation of X and Y is defined as

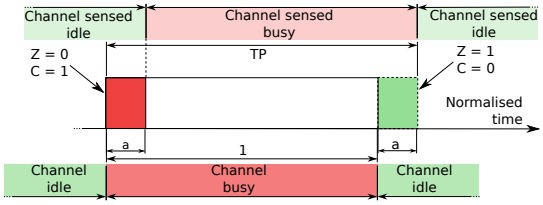


Fig. 8. Sensed and true channel states

$$\text{corr}(X, Y) = \frac{E\left[(X - \mu_X)(Y - \mu_Y)\right]}{\sigma_X \sigma_Y}$$

Let the true channel state be denoted C and the channel state as sensed by a node be denoted Z. Each of these variables can take two possible values: busy or idle. C will be busy whenever any node in the network is transmitting, even if this transmission has not yet reached any other node, and idle otherwise. Z is node-dependent and will be busy whenever the signal received at a node is above the SINR threshold for the channel to be considered busy, and idle otherwise. Here we will neglect effects such as channel noise, multipath propagation, etc. and assume an ideal channel. Let 1 represent a busy state and 0 represent an idle state (for either variable). Since Z is actually the same process as C, just one propagation delay behind, we have $Z(t) = C(t - a)$, and in steady state, then, $\mu_Z = \mu_C = \mu$ and $\sigma_Z = \sigma_C = \sigma$.

We can take the correlation of C and Z.

$$\text{corr}(C, Z) = \frac{\sum_{c\in\{0,1\}, z\in\{0,1\}} (c - \mu)(z - \mu) P(C = c, Z = z)}{\sigma^2} \tag{1}$$

This is equivalent to the autocorrelation of C with a time delay equal to the propagation delay, however when deriving the probabilities to satisfy Equation 1 it is helpful to consider Z and C separately.

In order to derive an expression for $\text{corr}(C, Z)$, we need to find the following:

- μ
- σ
- $P(C = 1, Z = 1)$: the probability that the channel is busy and is sensed as busy
- $P(C = 0, Z = 1)$: the probability that the channel is idle but is sensed as busy
- $P(C = 1|Z = 0)$: the probability that the channel is busy but is sensed as idle
- $P(C = 0, Z = 0)$: the probability that the channel is idle and is sensed as idle

To determine these values, we can consider the cycle of busy and idle periods that the channel goes through under p-persistent CSMA, depicted in Figure 1. (See Section III for a more detailed explanation of this protocol.) A busy period consists of m transmission periods (TPs), each of which may result in either a successful packet transmission or a collision. The average times spent in busy and idle periods are derived

in [1] and denoted by $\bar{B}$ and $\bar{I}$ respectively. Note that as with all other time expressions, these are normalised to the packet transmission time.

$$\bar{B} = a\bar{t}' + \frac{a\bar{t}\,(1-\pi_0) + 1 + a}{\pi_0} \tag{2}$$

$$\bar{I} = \frac{a}{1-e^{-g}} \tag{3}$$

The probability that the number of TPs in a busy period is equal to m is $\pi_0\,(1-\pi_0)^{m-1}$, for $m \in \mathbb{Z}_{>0}$ [1], and so we can find $\bar{m}$ by taking the average over this distribution.

$$\bar{m} = \sum_{m=1}^{\infty} m\pi_0\,(1-\pi_0)^{m-1} \tag{4}$$

As a busy period must have at least one TP, m is always at least 1.

This is an arithmetico-geometric series and so we can compute this sum:

$$\begin{aligned}\bar{m} &= \pi_0\left(\frac{1}{1-(1-\pi_0)}\right) + \frac{(1-\pi_0)\times 1}{(1-(1-\pi_0))^2} \\ &= \pi_0\left(\frac{\pi_0 + 1 - \pi_0}{{\pi_0}^2}\right) \\ &= \pi_0\left(\frac{1}{{\pi_0}^2}\right) \\ &= \frac{1}{\pi_0}.\end{aligned} \tag{5}$$

When sensing the channel, the probability that it is sensed busy or idle will be equal to the probability of the channel actually being busy or idle, since the sensed channel state is simply the channel state one propagation delay earlier. Thus if we sensed the channel constantly, the proportions of time we would sense busy and idle states is equal to the proportions of time the channel actually spends busy and idle. We therefore have

$$P(Z=1) = P(C=1)$$

and

$$P(Z=0) = P(C=0).$$

The channel is in a busy state only during a TP (excluding the final propagation delay after transmission ends), with $\bar{m}$ TPs per cycle on average. Hence the proportion of time the channel is busy (or, equivalently, the probability that the channel is busy in steady state) is

$$P(C=1) = \frac{\bar{m}}{\bar{B}+\bar{I}}. \tag{6}$$

The probability that the channel is idle is then

$$\begin{aligned}P(C=0) &= 1 - P(C=1) \\ &= 1 - \frac{\bar{m}}{\bar{B}+\bar{I}}.\end{aligned} \tag{7}$$

Next we will derive the conditional probabilities for the channel state given a particular sensed state (see Figure 8). First consider the case that the channel is sensed busy, i.e. $Z=1$. The channel is sensed busy during a TP after the initial propagation delay. The duration of a TP is $1+a$ and since we are subtracting one propagation delay from the beginning, we are left with a duration of 1. Of this time, the channel is only actually busy during the transmission itself, whereas during the propagation delay (of length a) at the end, the channel is actually idle. Hence we have

$$P(C=1|Z=1) = 1-a \tag{8}$$

and

$$P(C=0|Z=1) = a. \tag{9}$$

To determine the channel state probabilities conditioned on the channel being sensed idle, we must first determine the total time the channel could be sensed as idle. This can either occur within one propagation delay of the beginning of a TP, or whilst the channel is idle and it has been longer than a propagation delay since the end of a TP. The first case occurs on average $\bar{m}$ times per cycle, and is of length a each time, giving a total time of $a\bar{m}$. The second case can occur either during an idle period, of length $\bar{I}$ (note that an idle period does not begin until one propagation delay after the last TP of a busy period), or during a busy period while nodes waiting to transmit are in backoff. The average length of the backoff time is $a\bar{t}$ ($\bar{t}$ slots of length a each) and this occurs $\bar{m}-1$ times per cycle (between each pair of consecutive TPs). Hence the total time a constantly sensing node would see the channel as idle per cycle is

$$\text{Sensed idle time} = \bar{I} + (\bar{m}-1)a\bar{t} + a\bar{m}. \tag{10}$$

Of this time, the channel is actually busy during the vulnerable periods ($a\bar{m}$) and idle otherwise. Hence

$$P(C=1|Z=0) = \frac{a\bar{m}}{\bar{I}+(\bar{m}-1)a\bar{t}+a\bar{m}} \tag{11}$$

and

$$P(C=0|Z=0) = \frac{\bar{I}+(\bar{m}-1)a\bar{t}}{\bar{I}+(\bar{m}-1)a\bar{t}+a\bar{m}}. \tag{12}$$

We can now determine the joint probability distribution of C and Z. The joint probabilities are:

$$\begin{aligned}P(C=0,Z=0) &= P(C=0|Z=0)P(Z=0) \\ &= \frac{\bar{I}+(\bar{m}-1)a\bar{t}}{\bar{I}+(\bar{m}-1)a\bar{t}+a\bar{m}}\left(1-\frac{\bar{m}}{\bar{B}+\bar{I}}\right)\end{aligned} \tag{13}$$

$$\begin{aligned}P(C=1,Z=0) &= P(C=1|Z=0)P(Z=0) \\ &= \frac{a\bar{m}}{\bar{I}+(\bar{m}-1)a\bar{t}+a\bar{m}}\left(1-\frac{\bar{m}}{\bar{B}+\bar{I}}\right)\end{aligned} \tag{14}$$

$$\begin{aligned}P(C=0,Z=1) &= P(C=0|Z=1)P(Z=1) \\ &= a\frac{\bar{m}}{\bar{B}+\bar{I}}\end{aligned} \tag{15}$$

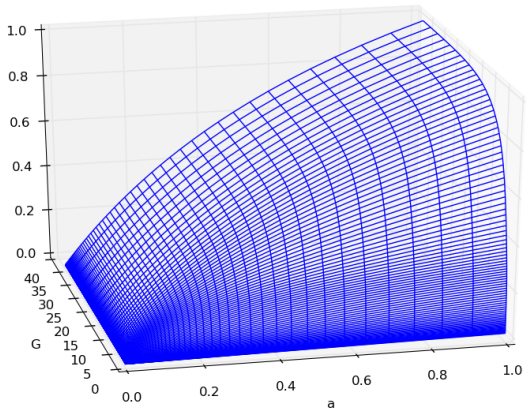


Fig. 9. Probability of obtaining incorrect information from channel sensing

$$P(C=1,Z=1) = P(C=1|Z=1)P(Z=1) = (1-a)\frac{\bar{m}}{\bar{B}+\bar{I}}. \quad (16)$$

Channel sensing will provide a node with incorrect information about the channel state whenever $Z \neq C$, which occurs with probability $P(C=0,Z=1)+P(C=1,Z=0)$. Figure 9 shows this probability as a function of the propagation delay and offered load, for $p=0.1$. At low offered loads, the probability of obtaining incorrect information from channel sensing remains low even with a high propagation delay, since the channel is idle almost all the time. When a is small, the probability of incorrect information from sensing also remains low regardless of offered load since sensing provides accurate information nearly all the time. However, once we have even a moderate offered load, the chances of sensing an incorrect channel state increase with the propagation delay. Note that at high offered loads, the channel state is not actually busy all the time, since the slot time is equal to a and the channel will be idle for some number of slots (depending on the persistence value) between transmissions.

To find the correlation between sensed channel state and true channel state, we also need expressions for μ and σ.

$$\begin{aligned}\mu &= E[C] \\ &= 0 \times P(C=0) + 1 \times P(C=1) \\ &= P(C=1) \\ &= \frac{\bar{m}}{\bar{B}+\bar{I}} \end{aligned} \quad (17)$$

$$\begin{aligned}\sigma &= \sqrt{E[C^2]-(E[C])^2} \\ &= \sqrt{E[C]-(E[C])^2} \quad \text{(since the range of C is } \{0, 1\}) \\ &= \sqrt{\mu(1-\mu)} \\ &= \sqrt{\left(\frac{\bar{m}}{\bar{B}+\bar{I}}\right)\left(1-\frac{\bar{m}}{\bar{B}+\bar{I}}\right)} \end{aligned} \quad (18)$$

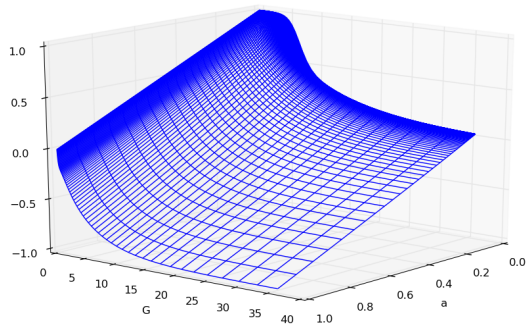


Fig. 10. Correlation between true and sensed channel state

The correlation of C and Z is then given by

$$\begin{aligned}\text{corr}(C,Z) = \frac{\sum_{c\in\{0,1\},z\in\{0,1\}}(c-\mu)(z-\mu)P(C=c,Z=z)}{\sigma^2} \\ = \frac{\begin{array}{l}(0-\mu)\,(0-\mu)\,P(C=0,Z=0) \\ +\,(0-\mu)\,(1-\mu)\,P(C=1,Z=0) \\ +\,(1-\mu)\,(0-\mu)\,P(C=0,Z=1) \\ +\,(1-\mu)\,(1-\mu)\,P(C=1,Z=1)\end{array}}{\sigma^2}\end{aligned} \quad (19)$$

where the individual terms are as given in Equations 13–18.

A plot of $\text{corr}(C,Z)$ as a function of propagation delay and offered load is shown in Figure 10. We can consider this as a measure of the utility of performing channel sensing. For small a, channel sensing is of high utility (although this decreases as the offered load increases, forcing the channel into a saturated state). As the packet transmission time decreases relative to the propagation delay, i.e. a increases, we are looking further back into the past when performing channel sensing, relative to the timescale at which data is being transmitted. Channel sensing then becomes of no or even negative utility — nodes begin obtaining and acting on incorrect information and would instead achieve better performance by transmitting based solely on random chance as in ALOHA.

VI. Beyond CSMA

As we have shown above, the main problem when a becomes large is that, in effect, all information obtained through channel sensing is old and not reliable. The main challenge is thus to improve the reliability of the information used for the access mechanism (minimise the likelihood of obtaining incorrect information).

Increasing the reliability can be achieved in two different ways: through sampling and prediction using signal processing and machine learning strategies or by increasing coordination and information exchange among the nodes. The effectiveness of each strategy will depend on the randomness of the frame generation process: a highly regular process will lend itself to learning strategies as they impose no overhead and no coordination. As the randomness increases coordination becomes more effective but it comes at a price of overhead and lost flexibility.

A main consideration is that both these classes of strategies can be implemented using legacy CSMA underneath, i.e. any MAC standard becomes backwards compatible. It is also a way of continuing the use of the simplistic CSMA mechanism by improving the information quality so it remains effective.

VII. Conclusion

In this paper we have investigated the effects of increasing data rates and small packet sizes on the performance of CSMA. We have analysed the utility of performing channel sensing in terms of the probability of obtaining incorrect information about the channel state and shown that this probability increases dramatically as the propagation delay approaches the packet transmission time.

With the continued push for higher raw data rates in 802.11 and changing traffic patterns towards a greater proportion of real-time and uplink traffic, we are reaching the limits of carrier sensing as a means for medium access control in wireless LANs. We are approaching a situation in which in some cases CSMA will perform no better than pure random access as in slotted ALOHA. We thus need a new approach to wireless MAC protocols, towards greater co-ordination and information exchange between nodes that will enable us to predict the channel state rather than using retroactive information as with channel sensing.

References

[1] L. Kleinrock and F. A. Tobagi, "Packet switching in radio channels: Part i–carrier sense multiple-access modes and their throughput-delay characteristics," *Communications, IEEE Transactions on*, vol. 23, no. 12, pp. 1400–1416, 1975.

[2] "802.11ax proposed project authorization request," https://mentor.ieee.org/802.11/dcn/14/11-14-0165-01-0hew-802-11-hew-sg-proposed-par.docx, accessed 2014-06-18.

[3] Y. Xiao and J. Rosdahl, "Throughput and delay limits of ieee 802.11," *Communications Letters, IEEE*, vol. 6, no. 8, pp. 355–357, 2002.

[4] J. Jun, P. Peddabachagari, and M. Sichitiu, "Theoretical maximum throughput of ieee 802.11 and its applications," in *Network Computing and Applications, 2003. NCA 2003. Second IEEE International Symposium on*. IEEE, 2003, pp. 249–256.

[5] F. Cali, M. Conti, and E. Gregori, "Ieee 802.11 wireless lan: capacity analysis and protocol enhancement," in *INFOCOM'98. Seventeenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, vol. 1. IEEE, 1998, pp. 142–149.

[6] F. Calì, M. Conti, and E. Gregori, "Dynamic tuning of the ieee 802.11 protocol to achieve a theoretical throughput limit," *IEEE/ACM Transactions on Networking (ToN)*, vol. 8, no. 6, pp. 785–799, 2000.

[7] Y. Tay and K. C. Chua, "A capacity analysis for the ieee 802.11 mac protocol," *Wireless networks*, vol. 7, no. 2, pp. 159–171, 2001.

[8] I. S. Association *et al.*, "802.11-2012-ieee standard for information technology–telecommunications and information exchange between systems local and metropolitan area networks–specific requirements part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications," 2012.

[9] D. Skordoulis, Q. Ni, H.-H. Chen, A. P. Stephens, C. Liu, and A. Jamalipour, "Ieee 802.11 n mac frame aggregation mechanisms for next-generation high-throughput wlans," *Wireless Communications, IEEE*, vol. 15, no. 1, pp. 40–47, 2008.

[10] Y. Xiao, "Ieee 802.11 n: enhancements for higher throughput in wireless lans," *Wireless Communications, IEEE*, vol. 12, no. 6, pp. 82–91, 2005.

[11] Y. Kim, S. Choi, K. Jang, and H. Hwang, "Throughput enhancement of ieee 802.11 wlan via frame aggregation," in *Vehicular technology conference, 2004. VTC2004-Fall. 2004 IEEE 60th*, vol. 4. IEEE, 2004, pp. 3030–3034.

[12] Y. Xiao, "Packing mechanisms for the ieee 802.11 n wireless lans," in *Global Telecommunications Conference, 2004. GLOBECOM'04. IEEE*, vol. 5. IEEE, 2004, pp. 3275–3279.

[13] "Packet measurements around Boulder, CO," https://mentor.ieee.org/802.11/dcn/14/11-14-0546-01-00ax-packet-traffic-measurements-around-boulder-colorado.ppt, accessed 2014-06-26.

[14] T. Henderson, D. Kotz, and I. Abyzov, "The changing usage of a mature campus-wide wireless network," *Computer Networks*, vol. 52, no. 14, pp. 2690–2712, 2008.

[15] M. Afanasyev, T. Chen, G. M. Voelker, and A. C. Snoeren, "Usage patterns in an urban wifi network," *Networking, IEEE/ACM Transactions on*, vol. 18, no. 5, pp. 1359–1372, 2010.

[16] E. Halepovic, C. Williamson, and M. Ghaderi, "Wireless data traffic: a decade of change," *Network, IEEE*, vol. 23, no. 2, pp. 20–26, 2009.

[17] M. Starsinic, "System architecture challenges in the home m2m network," in *Applications and Technology Conference (LISAT), 2010 Long Island Systems*. IEEE, 2010, pp. 1–7.

[18] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[19] G. Bianchi, "Performance analysis of the ieee 802.11 distributed coordination function," *Selected Areas in Communications, IEEE Journal on*, vol. 18, no. 3, pp. 535–547, 2000.

[20] D. Malone, K. Duffy, and D. Leith, "Modeling the 802.11 distributed coordination function in nonsaturated heterogeneous conditions," *Networking, IEEE/ACM Transactions on*, vol. 15, no. 1, pp. 159–172, 2007.

[21] P. Chatzimisios, V. Vitsas, and A. C. Boucouvalas, "Throughput and delay analysis of ieee 802.11 protocol," in *Networked Appliances, 2002. Liverpool. Proceedings. 2002 IEEE 5th International Workshop on*. IEEE, 2002, pp. 168–174.

[22] J. W. Robinson and T. S. Randhawa, "Saturation throughput analysis of ieee 802.11 e enhanced distributed coordination function," *Selected Areas in Communications, IEEE Journal on*, vol. 22, no. 5, pp. 917–928, 2004.

[23] H. Wu, Y. Peng, K. Long, S. Cheng, and J. Ma, "Performance of reliable transport protocol over ieee 802.11 wireless lan: analysis and enhancement," in *INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, vol. 2. IEEE, 2002, pp. 599–607.

[24] N. T. Dao and R. A. Malaney, "A new markov model for non-saturated 802.11 networks," in *Consumer Communications and Networking Conference, 2008. CCNC 2008. 5th IEEE*. IEEE, 2008, pp. 420–424.

[25] K. Duffy, D. Malone, and D. J. Leith, "Modeling the 802.11 distributed coordination function in non-saturated conditions," *IEEE Communications Letters*, vol. 9, no. 8, pp. 715–717, 2005.

[26] W. E. Leland, M. S. Taqqu, W. Willinger, and D. V. Wilson, "On the self-similar nature of ethernet traffic," in *ACM SIGCOMM Computer Communication Review*, vol. 23, no. 4. ACM, 1993, pp. 183–193.

[27] V. Paxson and S. Floyd, "Wide area traffic: the failure of poisson modeling," *IEEE/ACM Transactions on Networking (ToN)*, vol. 3, no. 3, pp. 226–244, 1995.

[28] M. E. Crovella and A. Bestavros, "Self-similarity in world wide web traffic: evidence and possible causes," *Networking, IEEE/ACM Transactions on*, vol. 5, no. 6, pp. 835–846, 1997.

[29] O. Tickoo and B. Sikdar, "On the impact of ieee 802.11 mac on traffic characteristics," *Selected Areas in Communications, IEEE Journal on*, vol. 21, no. 2, pp. 189–203, 2003.

[30] H. Takagi and L. Kleinrock, "Throughput analysis for persistent csma systems," *Communications, IEEE Transactions on*, vol. 33, no. 7, pp. 627–638, 1985.

[31] N. Abramson, "The aloha system: another alternative for computer communications," in *Proceedings of the November 17-19, 1970, fall joint computer conference*. ACM, 1970, pp. 281–285.

Appendix B

Joint compressed-sensing and matrix-completion for efficient data collection in WSNs

Joint compressed-sensing and matrix-completion for efficient data collection in WSNs

Alexandros Fragkiadakis, Ioannis Askoxylakis, Elias Tragos
Institute of Computer Science
Foundation for Research and Technology-Hellas (FORTH)
P.O. Box 1385, GR 711 10, Heraklion, Crete, Greece
email: {alfrag, asko, etragos}@ics.forth.gr

***Abstract*—Wireless sensor networks have gained considerable interest in the last few years, serving a large number of applications. Data collection efficiency is of paramount importance as sensors are severe resource-constrained devices. Furthermore, current protocol inefficiencies lead to significant packet loss. In this work, we minimize the necessary information sensors transmit by applying the compressed sensing principles. Moreover, missing information due to packet loss is efficiently recovered using the matrix completion theory. The performance evaluation shows that when these advanced signal processing techniques are jointly used, the reconstruction error is small for high compression ratios, and fairly high packet loss. At the same time, the total energy consumption of the network substantially decreases.**

***Index Terms*—wireless sensor networks, compressed sensing, matrix completion, reconstruction error, performance evaluation, energy consumption.**

I. Introduction

Wireless sensor networks (WSNs) have gained considerable interest in the last few years mainly due to the advances of the technology regarding the electromechanical systems (EMS). EMS technology has enabled the design of off-the-shelf miniature sensors with enhanced processing capabilities and memory. This, along with the deployment and standardization of energy-efficient network protocols like the IEEE 802.15.4, 6LowPan, etc., have given a considerable boost to WSN deployment for a large number of applications.

WNSs consist of tens or hundreds of miniature sensors that sense information from the surrounding environment. Typical WSN applications involve the measurement of the ambient temperature, light, humidity, barometric pressure, acceleration, velocity, acoustics, magnetic field, etc., [1]. As sensors are severe resource-constrained devices in terms of memory, processing, and energy, they usually do not perform any sophisticated computations on the sensed information; rather, they transmit it to a more powerful device, called as sink, for further processing. There are several data delivery models used for information flow between the sensors and the sink: (i) periodic-based where sensors periodically send their sensed data to the sink, (ii) event-driven, where data are transmitted to the sink only after an event has taken place (e.g. fire), (iii) query-driven, where the sink requests data from the sensors, and (iv) hybrid model that combines mechanisms from a subset of the previous models. The choice of the suitable model depends on the application served by the WSN.

Nowadays, WSNs are used for a large number of purposes like environmental monitoring [2], critical infrastructure protection [3], emergency response and disaster relief [4], life-logging [5], health monitoring [6], surveillance [7], water-use efficiency [8], earthquake localization [9], structural damage detection [10]. One of the most important advantages of WSNs is that they can be easily deployed in large and harsh environments and operate unattended.

Unlike traditional wireless networks, WSNs have several limitations because of the resource-constrained nature of the sensors, and the low bandwidth characteristic of the communication protocols used (e.g. IEEE 802.15.4). For these reasons, the design of energy-efficient mechanisms is of paramount importance as they can substantially prolong WSNs lifetime. There has been considerable interest in the design of energy-efficient mechanisms for data collection. Data collection is referred to the process where the sink collects the sensed data using one of the delivery models referred previously. Data collection mainly involves packet transmissions from the sensors to the sink, and as shown in the literature ([11]), most of the sensors' energy is consumed for the listen and transmit operations. For transmission, a sensor has to first sense the channel (in case a carrier-sense protocol is used) using its RF (radio-frequency) circuit, and if it is free, to transmit its packet. If it is not free, it enters a back-off stage. If transmission attempts result to collisions, packet re-transmission takes place. For the listen operations, every sensor spends energy to decode and further accept or reject a transmitted packet. Due to the broadcast nature of the wireless medium, a sensor consumes energy for every packet transmitted by its one-hop neighbors, even if this sensor is not addressed as the receiver of the transmitted information.

In order to minimize the transmit and listen operations' overhead, several techniques like source coding, lossy compression, in-network aggregation etc., have been proposed in the literature. In this work, we use the relatively new theory of compressed sensing (CS) [12]; compressing the sensed data in each sensor prior to transmission to the sink. Taking advantage of the intra-temporal correlation of sensor measurements, we

show that with CS, the reconstruction (de-compression) error at the sink is small, while energy spending substantially decreases.

A significant flaw of WSNs is the high packet loss experienced due to the bandwidth limitations and the resource-constrained nature of the sensors. In this paper, by taking advantage of the inter-spatial correlation of the sensed data, we show that information recovery is possible with high performance, in case of packet loss, using the matrix completion principles [13].

Our main contributions are as follows:

- we use compressed sensing to compress the sensed data at each sensor prior to transmission to the sink,
- we utilize the matrix completion principles in order to recover the missing information due to packet loss,
- we evaluate the above techniques in a simulated environment showing that the reconstruction error is low, while a significant amount of energy is saved.

The rest of this work is organized as follows. Section II and Section III give the background on compressed sensing and matrix completion, respectively. Section IV describes how compressed sensing and matrix completion are used jointly. In Section V we describe the simulation testbed and present performance evaluation results. Related work is described in Section VI. Finally, conclusions appear in Section VII.

II. Compressed sensing for the intra-temporal correlation

The recently introduced theory of CS exploits the structure of a signal in order to enable a significant reduction in the sampling and computation costs. In the context of a WSN, suppose that $\mathbf{x} \in \mathbb{R}^N$ is a signal referred to the sensed data of an individual sensor. CS theory proves that if $\mathbf{x}$ is sparse in some domain, it can be reconstructed exactly with high probability from M randomized linear projections of signal $\mathbf{x}$ into a measurement matrix $\mathbf{\Phi} \in \mathbb{R}^{M \times N}$, where $M \ll N$. A signal is called sparse if most of its elements are zero in a specific transform basis. The discrete signal $\mathbf{x} \in \mathbb{R}^N$ can be expressed in terms of a sparsifying basis (dictionary) $\mathbf{\Psi}$ of $N \times 1$ vectors $\{\psi_{i=1}^N\}$ such that:

$$\mathbf{x} = \mathbf{\Psi}\mathbf{b} \tag{1}$$

where $\mathbf{b} \in \mathbb{R}^N$ is a sparse vector with S non-zero components ($\|\mathbf{b}\|_0 = S$). The general measurement model is expressed as follows:

$$\mathbf{y} = \mathbf{\Phi}\mathbf{x} = \mathbf{\Phi}\mathbf{\Psi}\mathbf{b} = \mathbf{\Theta}\mathbf{b} \tag{2}$$

where $\mathbf{\Theta} = \mathbf{\Psi}\mathbf{\Phi}$. Essentially, each sensor instead of transmitting a signal $\mathbf{x} \in \mathbb{R}^N$, it performs CS and finally transmits a smaller signal $\mathbf{y} \in \mathbb{R}^M$.

The original vector $\mathbf{b}$ and consequently the sparse signal $\mathbf{x}$, is estimated by solving the following ℓ_0-norm constrained optimization problem:

$$\hat{\mathbf{b}} = \arg\min \|\mathbf{b}\|_0 \quad s.t. \quad \mathbf{y} = \mathbf{\Theta}\mathbf{b} \tag{3}$$

where the $\|\mathbf{b}\|_0$ norm counts the number of non-zero components of $\mathbf{b}$. As solving (3) is both numerically unstable and NP-complete, reconstruction is performed following the norm convex relaxation problem:

$$\hat{\mathbf{b}} = \arg\min \|\mathbf{b}\|_1 \quad s.t. \quad \mathbf{y} = \mathbf{\Theta}\mathbf{b}. \tag{4}$$

The ℓ_1 norm ($\|\mathbf{b}\|_1 := \sum_i |b_i|$) can exactly recover the S-sparse signal with high probability using only $M \geq CS\log(N/S)$ measurements ($C \in R^+$) [12]. Finally, the reconstructed signal is given by $\hat{\mathbf{x}} = \mathbf{\Psi}\hat{\mathbf{b}}$.

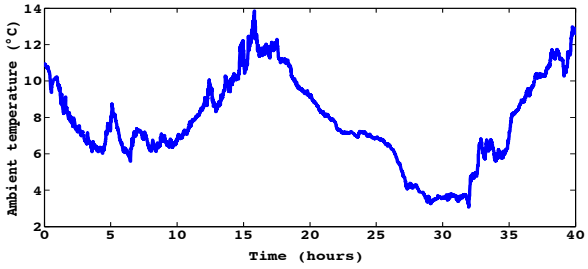


Figure 1: Ambient temperature measured by a single sensor

Figure 1 shows the ambient temperature measured by a sensor (with a period of 30 seconds) of the WSN described in [14]. Although the temperature may change during the day, there are however time periods where it does not significantly change. This reveals the intra-temporal correlation of the data sensed at each individual sensor. We exploit this property and use CS to compress the original sensed data of equally-sized blocks of size N. Later in the evaluation, we select $N = 100$ that corresponds to a time period of 50 minutes.

III. Matrix completion for the inter-spatial correlation

Bandwidth limitations and the resource-constrained nature of the sensors often cause high packet loss during the operation of a WSN. Packets are mainly lost due to collisions in the wireless medium, buffer overflows, protocol inefficiencies (e.g MAC, routing), etc. We attempt to recover the information carried by the lost packets using a new signal processing theory called as matrix completion (MC). Assume that there is a WSN consisting of S_i sensors where $i \in [1, k]$. All sensors report their measurements to a sink every δ_t seconds, transmitting a single packet for each measurement they perform. Each transmitted packet carries a packet id (assigned by its originating sensor) that is incremented for every new packet. The sink creates a table accumulating the measurements sent by the sensors (Table I). The table boxes that contain the symbol (?) denote the information carried by the packets that were lost in the WSN.

TABLE I: Measurement collection at the sink with missing information

packet id	Sensor id			
	S_1	S_2	...	S_k
1	10.22	**?**	...	11.22
2	10.33	9.12	...	11.45
3	1.23	**?**	...	11.56
4	**?**	9.54	...	**?**
5	**?**	9.12	...	11.12
...	...	...	...	...

Actually, the sink does not receive the ambient temperatures measured at the sensors ($\mathbf{x} \in \mathbb{R}^N$), but it receives their compressed versions ($\mathbf{y} \in \mathbb{R}^M$). Therefore, each column of Table I contains the compressed values (according to CS principles) transmitted by the corresponding sensor. The problem now is to recover the missed values of the matrix (Table I) by using the present ones. MC theory proves that if this matrix (denoted by $M \in \mathbb{R}^{n \times k}$) has a low rank (defined as the maximum number of independent columns or rows), it can be recovered with high probability. More interestingly, one can recover M from $s \geq Cd^{6/5}rlog(d)$ random measurements, where C is a positive constant, $d = max(n, k)$ and r is the rank of the matrix.

Suppose $M \in \mathbb{R}^{n \times k}$ is the unknown matrix we want to recover. As packet loss occurs in the network, the only information available about M is a set of entries $M \in \mathbb{R}^{i \times j}$, $(i, j) \in \Omega$, where Ω is the full set of entries $n \times k$. At the sink, the available information can be summarized using $P_\Omega(M)$, where the sampling operator (due to packet loss) is defined by:

$$[P_\Omega(X)]_{ij} = \begin{cases} X_{ij}, & \text{if } (i,j) \in \Omega \\ 0, & \text{otherwise} \end{cases} \quad (5)$$

We will try to recover matrix M using information $P_\Omega(M)$. If $M \in \mathbb{R}^{n \times k}$ is a low rank matrix, one could recover it by solving [13]:

$$\begin{array}{ll} \text{minimize} & \text{rank(X)} \\ \text{subject to} & P_\Omega(X) = P_\Omega(M) \end{array} \quad (6)$$

However, (6) is both unstable and NP-hard, hence it cannot be easily used in practice. A widely used alternative is the convex relaxation:

$$\begin{array}{ll} \text{minimize} & \| X \|_* \\ \text{subject to} & P_\Omega(X) = P_\Omega(M) \end{array} \quad (7)$$

where $\| X \|_*$ denotes the Frobenius norm of X.

IV. Joint compressed sensing and matrix completion

Figure 2 depicts how CS and MC are used jointly. Each sensor, splits its sensed data into equally-sized blocks of length N. Then, for each block, using CS with a compression ratio equal to $100 \times \frac{N-M}{N}$, it produces a compressed signal y of length M (using (2)) that is smaller than its uncompressed version x. Signal y is transmitted to the sink using a total number of M packets. In this paper, we use a Gaussian distribution for matrix $\mathbf{\Phi}$, and FFT as the basis for matrix $\mathbf{\Psi}$. Several works have shown that these matrices have the necessary properties (incoherence) in order to achieve high performance in terms of the reconstruction error.

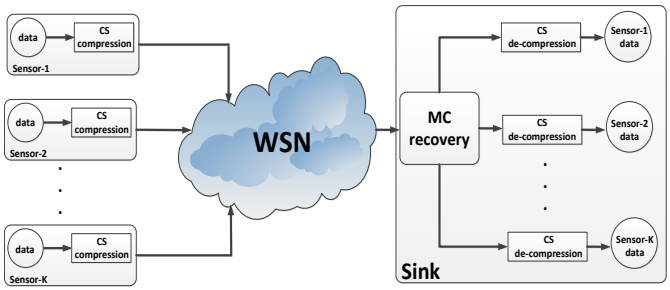


Figure 2: Joint use of compressed sensing and matrix completion techniques

The sink receives and stores the packets transmitted by the sensors in its memory, and creates a table similar to Table I. As WSNs are lossy networks, the created table has a number of missing entries, depending on the packet loss. The missing entries are recovered applying MC using (7). For MC recovery, we use the Singular Value Thresholding (SVT) algorithm [15]. After table recovery, de-compression takes place for the data of each individual sensor using CS through (4). For CS reconstruction, a variety of algorithms based on linear programming, convex relaxation, and greedy strategies have been proposed to solve (4). Here, we use the Orthogonal Matching Pursuit (OMP) strategy [16] as it is computationally very efficient.

V. Wireless sensor network testbed and performance evaluation

For the network testbed we use 32 Z1 sensors [17], and a single sink, in a simulated environment shown in Figure 3. Sensors run the Contiki operating system [18], controlled by Cooja, Contiki's simulator/emulator. The sensors are pre-loaded with ambient temperature measurements provided by [14]. During simulations, sensors compress the temperature measurements with CS using one out of three possible compression ratios (25%, 50%, and 75%). The compressed measurements are transmitted to the sink using a suitable protocol over UDP. We vary the transmitted packet rate so as to create an average packet loss in WSN that varies from 10% to 80%, with a step of 10%. We repeat each experiment 50 times.

Figure 4 shows the MC recovery error (MC_{err}) for different compression ratios and average packet loss. MC_{err} is defined as $MC_{err} = \frac{||M-X||_2}{||M||_2}$, where X is the recovered matrix, and M the matrix if there were no packet loss. The vertical lines on this figure show the 95% confidence interval. Observe

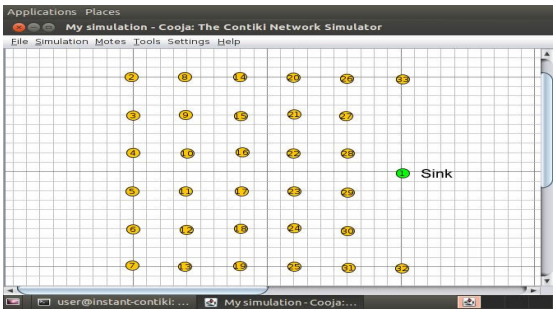
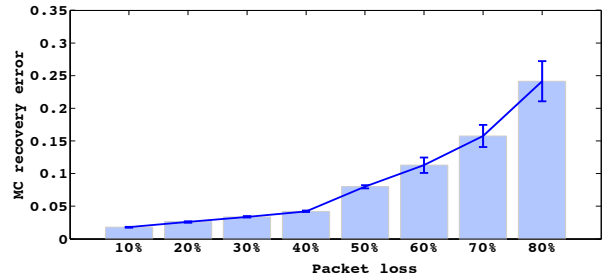


Figure 3: Simulated wireless sensor network testbed

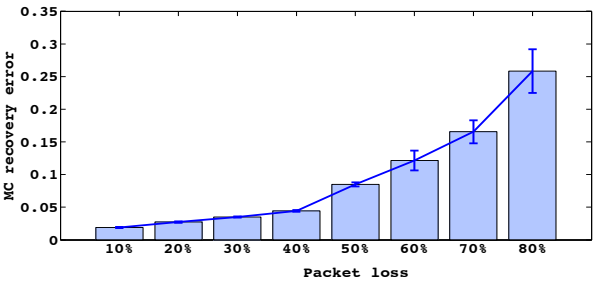
that as the packet loss increases, MC_{err} increases as less information is available for a successful recover. Furthermore, as the CS compression ratio increases, MC_{err} increases for the same average packet loss. This happens because a higher compression ratio results in a smaller matrix at the sink. The size of the matrix directly affects its rank that it further affects MC performance. The smaller the matrix, the less the correlated information, hence the higher its rank.

Next, we investigate CS reconstruction error (CS_{err}), defined as $CS_{err} = \frac{||x-\hat{x}||_2}{||x||_2}$. CS reconstruction (or decompression) takes place after MC recovery (Figure 2). Figure 5 shows the cumulative density function (CDF) of CS_{err} for different compression ratios and packet loss. As the compression ratio increases, CS_{err} increases. Moreover, for the same compression ratio, CS_{err} increases as the packet loss increases. This is because MC recovery (due to the smaller matrix size) has a lower performance that directly affects CS performance. However, observe that even for a relatively high packet loss (40%) CS_{err} is less than 0.1 for the majority of the sensors (about 80%). This means that signal fidelity can reach 90% in such lossy environments when CS and MC are used. For an even higher packet loss and compression ratio, performance deteriorates. Nevertheless, the tolerance for a specific CS_{err} depends on the application that uses the sensed data. Figures such as Figure 4 can assist a network operator to choose the suitable compression ratio that better fits specific application requirements.

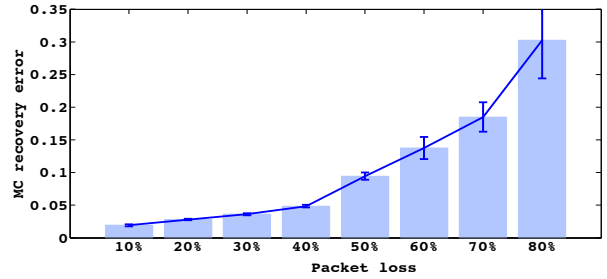
Next, we measure the power consumption of the WSN for a 3 hours period. We vary the compression ratio, while the transmission packet rate has been selected so as to have a 40% average packet loss in WSN. The power consumption is measured using powertrace [19], a built-in power measurement module of Contiki. Figure 6 shows the total power consumption of WSN when no CS is used, and for CS with the various compression ratios. The error bars show the 95% confidence intervals. Observe that as the compression ratio increases, network's power consumption significantly decreases. This is because less packets are transmitted into the network, hence less power is consumed.



(a) Compression ratio: 25%



(b) Compression ratio: 50%



(c) Compression ratio: 75%

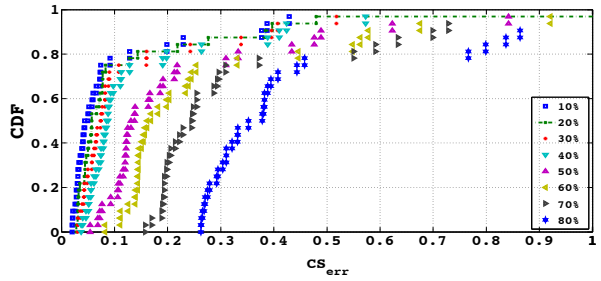
Figure 4: MC recovery error for different compression ratios and packet loss

VI. Related work

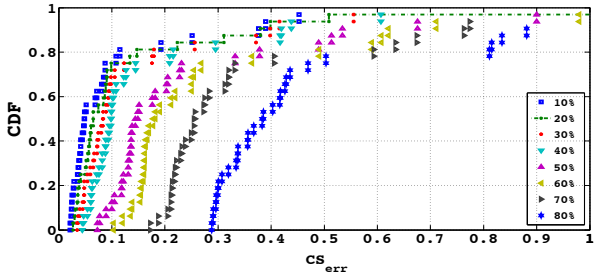
Several contributions exist in the literature involving compressed sensing, and matrix completion techniques. CS has been used for data compression or event detection in several works ([20], [21], [22], [23]. However, these contributions do not consider the significant packet loss that can occur in lossy networks such as WSNs. Regarding MC, works ([24], [25]) study the efficiency in data collection. All the above contributions use either MC or CS. On the contrary, we use these techniques jointly and show how missing information is recovered using MC, and how energy consumption reduces by applying CS.

VII. Conclusions

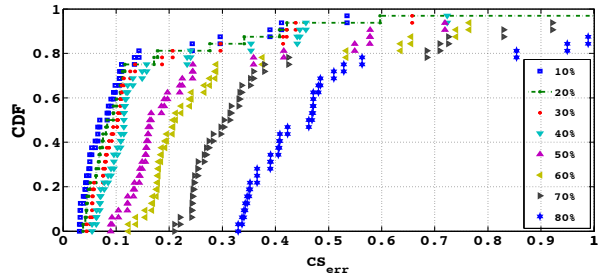
In this work, we used the matrix completion theory to recover missing information due to packet loss. Furthermore, we deployed the compressed sensing theory in order to reduce the communication overhead within the sensor network. The



(a) Compression ratio: 25%



(b) Compression ratio: 50%



(c) Compression ratio: 75%

Figure 5: CS reconstruction error for different compression ratios and packet loss

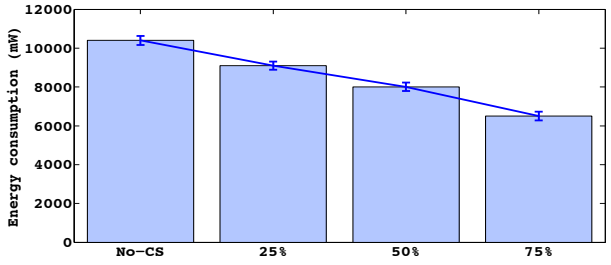


Figure 6: WSN total power consumption

evaluation results show that compressed sensing jointly with matrix completion, give a small reconstruction error for fairly high compression ratios and for a significant packet loss. Missing information is sufficiently recovered, and the total energy consumption of the sensors substantially reduces.

REFERENCES

[1] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Computer Networks, Elsevier*, vol. 52, pp. 2292–2330, 2008.

[2] G. Barrenetxea, F. Ingelrest, G. Schaefer, M. Vetterli, O. Couach, and M. Parlange, "SensorScope: Out-of-the-Box Environmental Monitoring," in *Proc. of IPSN*, 2008.

[3] L. Buttyan, D. Gessner, A. Hessler, and P. Langendoerfer, "Application of wireless sensor networks in critical infrastructure protection - challenges and design options," *IEEE Wireless Communications*, vol. 17, pp. 44–49, 2010.

[4] E. Cayirci and T. Coplu, "Sendrom: sensor networks for disaster relief operations management," *Wireless Networks*, vol. 13, pp. 409–423, 2007.

[5] M. Yasutoshi, K. Akiko, and M. Takashi, "Wireless wearable vibration sensor for touch-based life log system," in *Proc. of INSS*, 2012.

[6] A. Milenkovic, C. Otto, and E. Jovanov, "Wireless sensor networks for personal health monitoring: Issues and an implementation," *Computer Communications*, vol. 29, pp. 2521–2533, 2006.

[7] T. He, "Vigilnet: An integrated sensor network system for energy-efficient surveillance," *ACM Transactions on Sensor Networks*, vol. 2, pp. 1–38, 2006.

[8] J. McCulloch, P. McCarthy, S. Guru, W. Peng, D. Hugo, and A. Terhorst, "Wireless sensor network deployment for water use efficiency in irrigation," in *Proc. of REALWSN*, 2008.

[9] G. Werner-Allen, P. Swieskowski, and M. Welsh, "Real-time volcanic earthquake localization," in *Proc. of SenSys*, 2007.

[10] K. Chintalapudi, J. Paek, O. Gnawali, T. Fu, K. Dantu, J. Caffrey, R. Covindan, and E. Johnson, "Structural Damage Detection and Localization Using NETSHM," in *Proc. of IPSN*, 2006.

[11] A. Fragkiadakis, I. Askoxylakis, and E. Tragos, "Secure and energy-efficient life-logging in wireless pervasive environments," in *Proc. of the 1st International Conference on Human Aspects of Information Security, Privacy and Trust*, 2013.

[12] E. Candes and M. Wakin, "An introduction to compressive sampling," *IEEE Signal Processing Magazine*, vol. 25, no. 2, pp. 21–30, 2008.

[13] E. Candes and Y. Plan, "Matrix completion with noise," *Proceedings of the IEEE*, vol. 98, no. 6, pp. 925–936, 2010.

[14] "Sensorscope: Sensor networks for environmental monitoring, http://lcav.epfl.ch/sensorscope-en."

[15] J. Cai, E. Candes, and Z. Shen, "A singular value thresholding algorithm for matrix completion," *SIAM Journal on Optimization*, vol. 20, pp. 1956–1982, 2010.

[16] J. Tropp and A. Gilbert, "Signal recovery from random measurements via orthogonal matching pursuit," *IEEE Transactions on Information Theory*, vol. 53, pp. 4655–4666, 2007.

[17] "Zolertia z1 platform, http://www.zolertia.com/products/z1."

[18] "The open source os for the internet of things, http://www.contiki-os.org."

[19] A. Dunkels, J. Eriksson, N. Finne, and N. Tsiftes, "Powertrace: Network-level power profiling for low power wireless networks," Tech. Rep.

[20] A. Fragkiadakis and I. Askoxylakis, "Malicious traffic analysis in wireless sensor networks using advanced signal processing techniques," in *Proc. of the 14th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMom)*, 2013.

[21] A. Fragkiadakis, S. Nikitaki, and P. Tsakalides, "Physical-layer Intrusion Detection for Wireless Networks using Compressed Sensing," in *Proc. of WiMob*, 2012.

[22] C. Chou, R. Rana, and W. Hu, "Energy efficient information collection in wireless sensor networks using adaptive compressive sensing," in *Proc. of LCN*, 2009, pp. 443–450.

[23] R. Masiero, G. Quer, D. Munaretto, M. Rossi, J. Widmer, and M. Zorzi, "Data acquisition through joint compressive sensing and principal component analysis," in *Proc. of Globecom*, 2009, pp. 1–6.

[24] J. Cheng, Q. Ye, H. Jiang, D. Wang, and C. Wang, "Stcdg: An efficient data gathering algorithm based on matrix completion for wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 12, pp. 850–861, 2013.

[25] G. Tsagkatakis and P. Tsakalides, "Dictionary based reconstruction and classification of randomly sampled sensor network data," in *Proc. of SAM*, 2012, pp. 117–120.

Appendix C

Malicious traffic analysis in wireless sensor networks using advanced signal processing techniques

Malicious traffic analysis in wireless sensor networks using advanced signal processing techniques

Alexandros Fragkiadakis, Ioannis Askoxylakis
Institute of Computer Science
Foundation for Research and Technology-Hellas (FORTH)
P.O. Box 1385, GR 711 10, Heraklion, Crete, Greece
email: {alfrag,asko}@ics.forth.gr

***Abstract*—The recent advances in micro-sensor hardware technologies, along with the invention of energy-efficient protocols, have enabled a world-wide spread in wireless sensor networks deployment. These networks are used for a large number of purposes, while having small maintenance and deployment costs. However, as these are usually unattended networks, several security threats have emerged. In this work, we show how an adversary can overhear the encrypted wireless transmissions, and detect the periodic components of the wireless traffic that can further reveal the application used in the sensor network. Traffic analysis is performed in a very energy-efficient way using the compressed sensing principles. Furthermore, the periodic components are detected using the Lomb-Scargle periodogram technique.**

***Index Terms*—compressed sensing, malicious traffic analysis, signal processing, energy-efficiency, wireless sensor networks, Lomb-Scargle periodogram, Contiki**

I. Introduction

The recent advances in micro-electro-mechanical systems and low power and highly integrated digital electronics, have enabled the development of low-cost micro-sensors. These devices are used for measuring a number of physical attributes such as temperature, light, humidity, barometric pressure, acceleration, velocity, acoustics, magnetic field, etc [1]. The sensors are not used in isolation but are grouped into the so-called motes. Motes are integrated devices (e.g. [2]) that contain CPU and memory functionalities under a common board. The advances in sensor operating systems (e.g. Contiki, TinyOS) along with the standardization of new protocols (e.g IEEE 802.15.4, Zigbee) and the adoption of already existing networking protocols (IPv4/IPv6), have made feasible the deployment of wireless sensor networks (WSNs).

Nowadays, WSNs are used for a large number of purposes such as for environmental monitoring [3], critical infrastructure protection [4], emergency response and disaster relief [5], life-logging [6], health monitoring [7], surveillance [8], water-use efficiency [9], earthquake localization [10], structural damage detection [11], etc. Their main advantage is that they are easily deployed in large and harsh areas. Information is sensed and collected by (often) battery-operated motes, and transmitted through a multi-hop routing scheme to a central server, known as sink, for further processing. The sink is a node with enhanced hardware capabilities that performs the more complex tasks required, as motes themselves are severe-constrained devices in terms of processing, storage, computation, and power.

As WSNs become worldwide, their security issues have become a major concern. WSNs face a number of security threats at different layers such as: (i) jamming (interference) attacks at the physical layer, (ii) guaranteed time slot attacks at the medium access layer, (iii) sinkhole, wormhole and other routing attacks at the network layer. A number of counter-measures have been introduced for thwarting these attacks, mainly focusing on intrusion detection, and cryptographic schemes [12].

Except the aforementioned attacks that are successfully detected and mitigated using intrusion detection schemes, another type of attack, the *malicious traffic analysis attack*, cannot be detected and easily mitigated. In this attack, an adversary has the role of a passive listener that collects information from the network, and tries to detect and identify different periodic components in the captured network traffic. Essentially, the ultimate scope of the adversary is to detect information such as the type of applications that execute in the WSN, the paths related to the routing algorithm, etc. Such an information disclosure can severely violate the privacy and security of information-sensitive applications, like those used in wireless body area sensor networks [13]. In this work, we show how an adversary by using advanced signal processing techniques, can effectively detect the periodic components in the network traffic in a very energy-efficient way. Traffic analysis is performed using the Lomb-Scargle periodogram (LSP) technique, while power consumption reduces through the use of the compressed sensing (CS) principles.

Related work focuses on the study of traffic analysis that reveals periodic patterns of the captured traffic. As the authors in [14] show, signal processing techniques can be very effective in traffic analysis. We complement this work by con-

sidering an adversary that by using CS, significantly reduces the power consumption required for traffic analysis. Other contributions like [13], [15], [16], propose countermeasures against malicious traffic analysis. On the contrary, we work on the attacker side and show how it can perform energy-efficient malicious traffic analysis.

The rest of this work is organized as follows. Section II describes signal processing techniques appropriate for traffic analysis. In Section III we give the background on CS theory. Section IV presents the adversary model, while the performance evaluation is shown in Section V. Finally, conclusions appear in Section VI.

II. Traffic analysis using signal processing techniques

Very often in communication networks, when information has to be protected by eavesdroppers, security primitives like encryption, authentication, and data integrity are used. A second level of protection usually follows with intrusion detection schemes. This is more imperative in WSNs, due to the broadcast nature of the wireless medium. However, regardless the strength of the security algorithm, and the effectiveness of the intrusion detection system, an adversary can still overhear the wireless channel and identify different periodic components by observing the encrypted traffic. These observations will allow him later to infer regarding the applications used or the routing algorithm decisions taken.

The key idea for identifying periodic components in an encrypted traffic is to convert packet traces into signals, and then process these signals using appropriate signal processing techniques [14]. This will allow the identification of prominent recurring frequencies and time-periods. A common spectral processing technique used for periodic component identification is the standard Discrete Fourier Transform (DFT). DFT computes the spectral power densities and requires the encoded signal to be uniformly sampled. Supposing there is a uniformly sampled signal $x(n)$ with N samples, DFT gives a N-point discrete spectrum $X_N(k)$, where

$$X_N(k) = \sum_{n=0}^{N-1} x(n) * e^{-j2\pi kn/N} = DFT[x(n)] \quad (1)$$

$X_N(k)$ can be computed using the Fast Fourier Transform (FFT), and the resulted peaks in the spectrum correspond to the periodic components in the observed traffic. However, the resulted spectrum can contain many harmonically related peaks and furthermore, it does not provide a good unbiased estimate in the presence of noise [13]. Another technique available, the Welch Averaged Periodogram [17] (WAP) can give more reliable results, as periodograms' main characteristic is that they can perform well in the presence of noise or interference [14]. WAP utilizes averaging in order to reduce noise influence, and is generated by averaging the K separate spectra $X_N^{(r)}$, computes over K different segments of data, each of length L ($\leq N$)

$$P_x(k) = \frac{1}{KU} \sum_{r=0}^{K-1} |X_L^{(r)}(k)|^2 \quad (2)$$

where $X_L^{(r)}(k) = DFT[w(n)x_r(n)]$ and $U = \frac{1}{L}\sum_{n=0}^{L-1} w^2(n)$, where the windowed data $x_r(n)$ is the r^{th} windowed segment of $x(n)$, $w(n)$ is a windowing function that reduces the artifacts caused by the abrupt changes at the end-points of the window, and U is the normalized window power. The peaks given by P_x are real values that correspond to frequencies of event times of arrival.

As mentioned before, WAP can be efficiently used in order to detect periodic events in the presence of noise or interference. The authors in [13] use WAP for the detection of periodic events in a simulated single-hop wireless body area sensor network using the packet time arrivals. However, as packet arrivals in communication networks are inherently unevenly spaced, they result in a signal encoding that is also unevenly spaced. The FFT and WAP methods perform well only when the packet arrivals are evenly spaced. In order to overcome this limitation and perform efficient traffic analysis, a method called as the Lomb-Scargle periodogram (LSP) can be used. LSP is a spectral analysis technique designed for data that are unevenly spaced. Compared to the WAP and FFT techniques, although LSP requires more computational power, it has the added advantage that the input data are sparse, hence they consume less memory [14].

The LSP technique estimates a power spectrum of N points of data for arbitrary angular frequencies. The power density for an angular frequency ω is given by:

$$P_N(\omega) = \frac{1}{2\sigma^2}\{\frac{[\sum_n (h_n - \bar{h})\cos\omega(t_n - \tau)]^2}{\sum_n \cos^2\omega(t_n - \tau)} + \frac{[\sum_n (h_n - \bar{h})\sin\omega(t_n - \tau)]^2}{\sum_n \sin^2\omega(t_n - \tau)}\} \quad (3)$$

where

$$\bar{h} = \frac{1}{N}\sum_{n=0}^{N-1} h_n$$

$$\sigma = \frac{1}{N-1}\sum_{n=0}^{N-1}(h_n - \bar{h})$$

$$\tau = \frac{1}{2\omega}\tan^{-1}(\frac{\sum_n \sin 2\omega t_n}{\sum_n \cos 2\omega t_n})$$

The samples h_n, $n \in [0, N-1]$, are the N unevenly spaced samples of the observed signal at times t_n.

In Section IV we show how the LSP technique is used to

reveal the packet flows traversing a simulated WSN. As we are primarily concerned with energy-efficient traffic analysis, the LSP method is used jointly with CS for reducing the number of data required to detect the network flows. In the next section we describe the background on CS theory.

III. Compressed sensing background

The recently proposed theory of compressed sensing (CS) ([18]) unifies compression and encryption in order to minimize the overhead for data acquisition and sampling in a WSN. CS exploits the signal structure in order to enable a significant reduction in the sampling and computation costs at a central unit. The key principles in the development of CS theory are *sparsity* and *incoherence*. A signal $\mathbf{x} \in \mathbb{R}^N$ is called sparse if most of its elements are zero in a specific transformation basis. Incoherence satisfies the fact that the sampling/sensing waveforms have an extremely dense representation in the basis. Assuming signal $\mathbf{x} \in \mathbb{R}^N$ is sparse in a basis $\mathbf{\Psi}$, it can be written as $\mathbf{x} = \mathbf{\Psi b}$, where $\mathbf{b} \in \mathbb{R}^N$ is a sparse vector with S non-zero components ($\|\mathbf{b}\|_0 = S$). CS theory proves that an S-sparse signal $\mathbf{x}$ can be reconstructed exactly with high probability from M randomized linear projections of the signal $\mathbf{x}$ into a measurement matrix $\mathbf{\Phi} \in \mathbb{R}^{M \times N}$. The general measurement model is expressed as follows:

$$\mathbf{y} = \mathbf{\Phi x} = \mathbf{\Phi \Psi b} = \mathbf{\Theta b} \tag{4}$$

where $\mathbf{\Theta} = \mathbf{\Psi \Phi}$.

The original vector $\mathbf{b}$ and consequently the sparse signal $\mathbf{x}$, is estimated by solving the following ℓ_0-norm constrained optimization problem:

$$\hat{\mathbf{b}} = \arg\min \|\mathbf{b}\|_0 \quad s.t. \quad \mathbf{y} = \mathbf{\Theta b} \tag{5}$$

where the $\|\mathbf{b}\|_0$ norm counts the number of non-zero components of $\mathbf{b}$. Note that the formulation of the optimization problem in (5) uses an l_0 norm that measures signal sparsity instead than the traditionally used in signal processing applications l_2 norm, which measures signal energy. However, solving (5) is both numerically unstable and NP-complete. For this reason, the ℓ_0 norm can be replaced by the ℓ_1 norm and problem (5) can be rephrased as the following ℓ_1 norm convex relaxation problem:

$$\hat{\mathbf{b}} = \arg\min \|\mathbf{b}\|_1 \quad s.t. \quad \mathbf{y} = \mathbf{\Theta b}. \tag{6}$$

The ℓ_1 norm ($\|\mathbf{b}\|_1 := \sum_i |b_i|$) can exactly recover the S-sparse signal with high probability using only $M \geq CS\log(N/S)$ measurements ($C \in R^+$) [18]. Finally, the reconstructed signal is given by $\hat{\mathbf{x}} = \mathbf{\Psi}\hat{\mathbf{b}}$. A variety of reconstruction algorithms based on linear programming, convex relaxation, and greedy strategies have been proposed to solve (6). Among them, greedy strategies such as the Orthogonal Matching Pursuit (OMP) [19] are computationally efficient when the signal of interest is highly sparse.

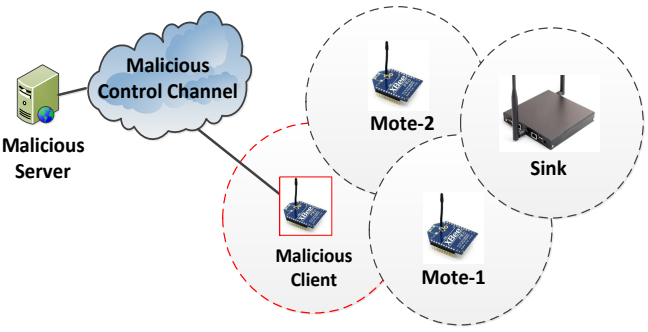


Figure 1: Wireless sensor network topology

IV. Adversary model

The adversary model we consider in this work consists of two distinct entities: (i) the malicious client (MC), and (ii) the malicious server (MS).

MC is a mote with constrained resources (CPU, memory, power) that is positioned in a strategic location within a WSN. Its mission is to observe the wireless traffic and record the timestamps of the captured packets. For this to become feasible, its network interface card is set to promiscuous mode. MC periodically encodes a signal derived from the packet timestamps and compress it, before transmitting it to a more advanced, in terms of resources node (malicious server), for further processing. Figure 1 shows a simulation testbed with two legitimate motes, a single legitimate sink, and the adversary entities (the dotted circles symbolize the transmission ranges of the motes and the MC). MC and MS communicate through a dedicated encrypted malicious control channel (MCC). As it concerns the legitimate WSN, motes periodically transmit sensed data to the sink using different packet transmission rates. Mote-1 transmits with a rate of 10 packets/sec (Flow-1), while Mote-2 transmits with a rate of 17 packets/sec (Flow-2). Therefore, the transmission frequencies of Flow-1 and Flow-2 are 0.1 and 0.059, respectively. The two motes, the sink, and the MC use ContikiOS [20], an open source operating system for WSNs. The testbed is simulated using Cooja, Contiki's simulator/emulator, while the traffic from the motes towards the sink is encrypted using IPsec [21].

The scope of this paper is to show that MC, jointly with MS can perform energy-efficient malicious traffic analysis. MC records data from the captured traffic that are transmitted to the MS for further processing. As it will be shown later, MS uses the LSP technique (Eq. 3) in order to detect the periodic components of the captured traffic. The malicious traffic analysis is first initiated by MC performing several tasks. First, it overhears the wireless channel, recording the timestamps of the captured packets. Then, it encodes the recorded timestamps into a signal that is suitable for spectrum analysis by the MS using the LSP technique. For this specific case, where two motes are available, we encode the recorded timestamps by assigning an amplitude of +1 for the packets

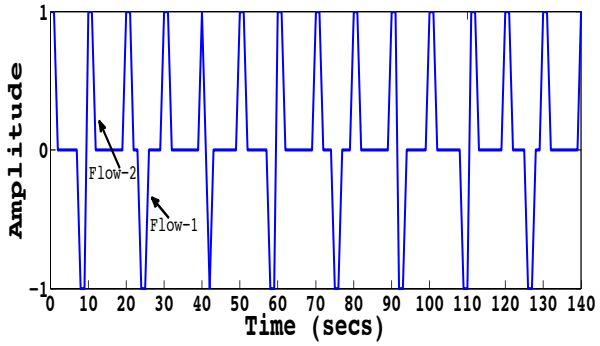


Figure 2: Encoded signal derived from the timestamps of the observed traffic

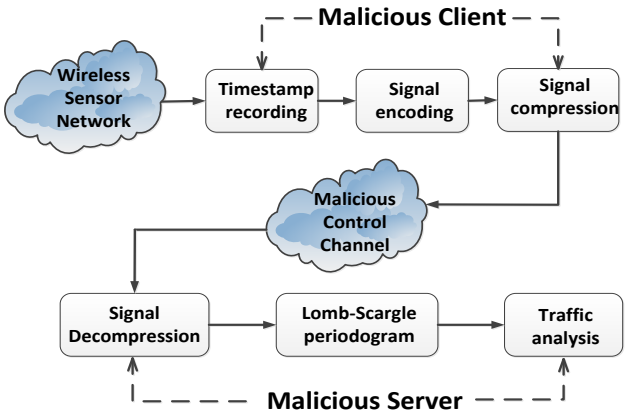


Figure 3: Malicious traffic analysis scheme

belonging to Mote-1, and -1 for the Mote-2 packets. Figure 2 shows an example of an encoded signal produced by MC for a 150 seconds packet trace.

After signal encoding takes place, MC compresses the encoded signal using the CS principles in order to minimize the communication cost with the MS. As MC is a severe resource constrained device, saving energy is of paramount importance. It is well known that most of the energy consumption in WSNs is caused by the transmission and listening operations performed by the motes. In this paper, we minimize the energy spending due to the transmission operations between the MC and the MS, by compressing the encoded signals in MC using CS. Later on, MS decompresses the signal and feeds the LSP algorithm. As mentioned in Section III, in order to compress a signal $\mathbf{x} \in \mathbb{R}^N$, it has to be sparse in some basis $\mathbf{\Psi}$, and it should be written as $\mathbf{x} = \mathbf{\Psi b}$. Unfortunately, although the encoded signal is sparse in the basis $\mathbf{\Psi} = LSP$, it cannot be expressed as a linear function by using LSP as the orthonormal basis $\mathbf{\Psi}$. For this reason, we follow a different strategy, by compressing the encoded signal at MC by using the FFT transform as the $\mathbf{\Psi}$ basis. We have verified that the encoded signal is also sparse in the frequency domain using FFT. When the MS receives the compressed signal, it will decompress it and feed the LSP algorithm. Signal compression at the MC involves the use of a transformation matrix $\mathbf{\Phi} \in \mathbb{R}^{M \times N}$. Hence, if $\mathbf{x}$ is the original (uncompressed) encoded signal, MC compress it using Eq. 4, obtaining $\mathbf{y}$, the compressed version of $\mathbf{x}$.

At this point, we have to choose the appropriate measurement matrix. Recent work has shown that when considering measurement matrices built using values selected independently from certain distributions, exact signal recovery can be achieved with high probability. One such choice is the Gaussian distribution used in several works (e.g. [22]). However, the generation of a Gaussian distribution may not be easily achieved in practical implementations, such in this work. The authors in [23] show that Toeplitz matrices with entries drawn from the same distributions (e.g. Gaussian) are also sufficient to recover a signal with high probability. A Toeplitz matrix has several attracting features [23]: (i) it requires the generation of $O(N)$ random variables, while independent and identically distributed (i.i.d.) matrices require the generation of $O(MN)$ variables, (ii) multiplication with a Toeplitz matrix can be performed using FFT and requires only $O(Nlog_2(N))$ operations, compared to i.i.d. matrices that require $O(MN)$ operations, and (iii) i.i.d. matrices are not easily applicable in certain scenarios (e.g., linear-time invariant systems).

After MC has compressed the encoded signal using the Toeplitz matrix, it transmits it over the MCC using a suitable protocol over UDP. Figure 3 shows the malicious traffic analysis operations.

V. Performance Evaluation

In this section, we show the performance evaluation of the malicious traffic analysis attacks in terms of power consumption, and reconstruction error.

A. Reconstruction error and spectrum graph fidelity

As mentioned in the previous section, MC compresses the signal prior to transmission to the MS. The compression ratio used directly affects the power consumption and the reconstruction error, defined as $e = \frac{||x-\hat{x}||_2}{||x||_2}$, where x and $\hat{x}$ are the original and reconstructed signals, respectively. The higher the compression ratio, the lower the power consumption, and the higher the reconstruction error. In order to show the effect of the compression ratio on the reconstruction error, we vary the compression ratio from 5% to 75%, performing CS compression at the MC, and decompression at the MS. We execute simulations for a total of 3 hours in Cooja. Regarding the CS parameters, we choose the Toeplitz as the measurement matrix, FFT as the transformation matrix, and set $N = 200$ the maximum block size of the encoded signal when applying CS. Figure 4 shows the cumulative density function (CDF) of the reconstruction error for the various compression ratios. Essentially, the reconstruction error depicts the fidelity of the reconstructed signal.

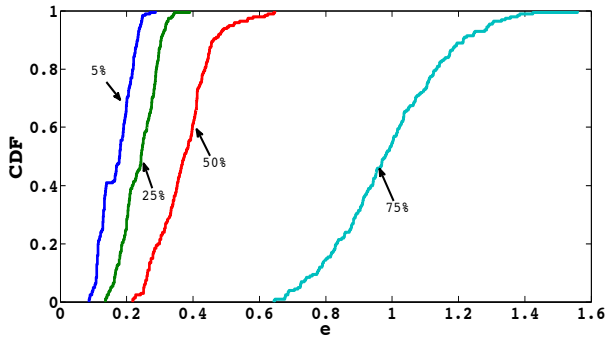


Figure 4: Reconstruction error for different compression ratios

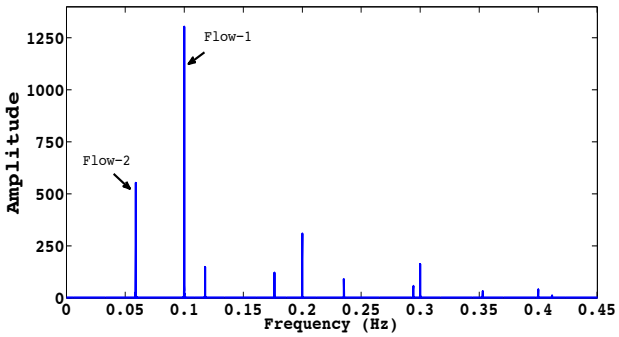


Figure 5: Traffic analysis using the Lomb-Scargle periodogram

Depending on the application, the reconstruction error shown in Figure 4 could be characterized as low, medium, or high for the different compression ratios. In this work, we are primarily interested to decompress the encoded signal, and then use the LSP algorithm in order to find the highest peaks in the frequency domain that signal the basic frequencies of the periodic components in the captured wireless traffic.

Figure 5 shows the spectrum analysis using LSP for an encoded signal that was transmitted from the MC without using CS. The spectrum peaks at the frequencies 0.1 and 0.059 correspond to Flow-1 and Flow-2, respectively. The rest of the peaks correspond to the harmonic frequencies of the flows that can be eliminated by using the appropriate filtering. In Figure 6, we show the traffic analysis revealed by the LSP method when CS is used, and for the different compression rations (that appear on the left side of each graph). For the compression ratios of 5%, 25%, and 50%, the two spectrum peaks clearly reveal the two periodic flows of the WSN. When the compression gets higher (75%), the fidelity of the spectrum graph lowers. This is because, as shown in Figure 4, the reconstruction error significantly increases.

B. Power consumption

MC periodically encodes the captured timestamps and sends the encoded signals to MS for traffic analysis. As already mentioned in the literature, the power consumption related to packet transmissions is the second highest after that due

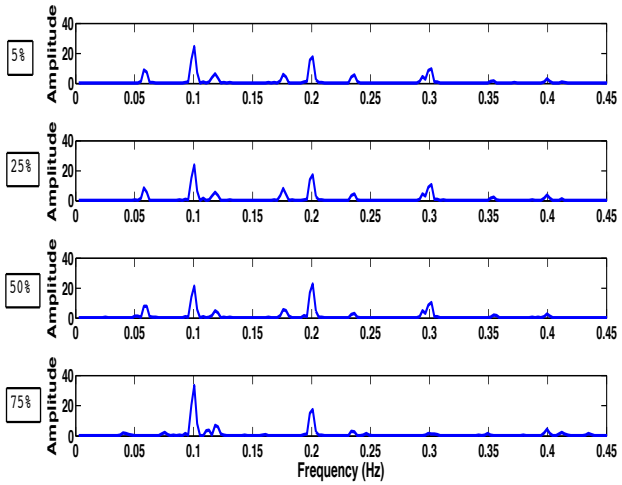


Figure 6: Traffic analysis using the Lomb-Scargle periodogram jointly with Compressed Sensing for different compression ratios

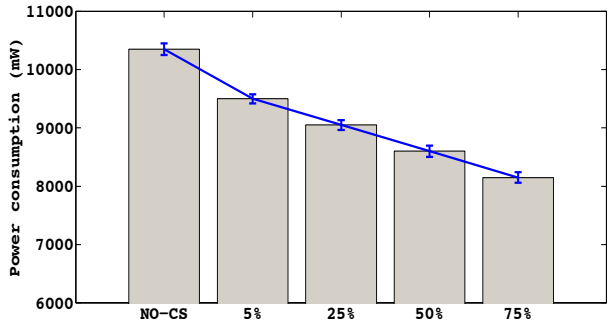


Figure 7: Power consumption of the Malicious Client for the various compression ratios

to the listening operations. We apply CS for compressing the packets MC sends to MS, and so we minimize the power that is consumed for the transmission operations. For measuring the power consumption of the MC, for the different compression ratios applied during CS, we use *powertrace* [24], a built-in power measurement module of Contiki. We simulated a 3-hour run using the topology shown in Figure 1, recording the total power consumption in MC. We repeat this procedure for 50 times, and plot MC's power consumption in Figure 7, where the error bars show the 95% confidence intervals. Observe that as the compression ratio increases, MC's power consumption significantly decreases. This is because less packets are transmitted into the network, hence less power is consumed.

VI. Conclusions

In this work, we presented an adversary model that performs malicious traffic analysis in a WSN. It consists of two distinct entities: a malicious client, and a malicious server.

The malicious client overhears the wireless channel, recording the timestamps of the captured packets. The timestamps are then encoded into signals that are compressed according to the compressed sensing principles. The performance evaluation shows that the power consumption significantly reduces as the compression ratio increases. Furthermore, the fidelity of the spectrum graph produced in the malicious server using the LSP method is high, and it successfully reveals the periodic components of the captured wireless traffic for high compression ratios.

REFERENCES

[1] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Computer Networks, Elsevier*, vol. 52, pp. 2292–2330, 2008.

[2] "Zolertia z1 platform, http://www.zolertia.com/products/z1."

[3] G. Barrenetxea, F. Ingelrest, G. Schaefer, M. Vetterli, O. Couach, and M. Parlange, "SensorScope: Out-of-the-Box Environmental Monitoring," in *Proc. of IPSN*, 2008.

[4] L. Buttyan, D. Gessner, A. Hessler, and P. Langendoerfer, "Application of wireless sensor networks in critical infrastructure protection - challenges and design options," *IEEE Wireless Communications*, vol. 17, pp. 44–49, 2010.

[5] E. Cayirci and T. Coplu, "Sendrom: sensor networks for disaster relief operations management," *Wireless Networks*, vol. 13, pp. 409–423, 2007.

[6] M. Yasutoshi, K. Akiko, and M. Takashi, "Wireless wearable vibration sensor for touch-based life log system," in *Proc. of INSS*, 2012.

[7] A. Milenkovic, C. Otto, and E. Jovanov, "Wireless sensor networks for personal health monitoring: Issues and an implementation," *Computer Communications*, vol. 29, pp. 2521–2533, 2006.

[8] T. He, "Vigilnet: An integrated sensor network system for energy-efficient surveillance," *ACM Transactions on Sensor Networks*, vol. 2, pp. 1–38, 2006.

[9] J. McCulloch, P. McCarthy, S. Guru, W. Peng, D. Hugo, and A. Terhorst, "Wireless sensor network deployment for water use efficiency in irrigation," in *Proc. of REALWSN*, 2008.

[10] G. Werner-Allen, P. Swieskowski, and M. Welsh, "Real-time volcanic earthquake localization," in *Proc. of SenSys*, 2007.

[11] K. Chintalapudi, J. Paek, O. Gnawali, T. Fu, K. Dantu, J. Caffrey, R. Covindan, and E. Johnson, "Structural Damage Detection and Localization Using NETSHM," in *Proc. of IPSN*, 2006.

[12] X. Chen, K. Makki, K. Yen, and N. Pissinou, "Sensor network security: A survey," *IEEE Communications Surveys and Tutorials*, vol. 2, pp. 52–73, 2009.

[13] L. Buttyan and T. Holczerr, "Traffic Analysis Attacks and Countermeasures in Wireless Body Area Sensor Networks," in *Proc. of WoWMom*, 2012.

[14] C. Partridge, D. Cousins, R. K. A. Jackson, T. Saxena, and W. Strayer, "Using Signal Processing to Analyze Wireless Data Traffic," in *Proc. of ACM workshop on Wireless Security*, 2002.

[15] Y. Fan, Y. Jiang, H. Zhu, J. Chen, and X. Shen, "Network coding based privacy preservation against traffic analysis in multi-hop wireless networks," *IEEE Transactions on Wireless Communications*, vol. 10, pp. 834–843, 2011.

[16] J. Deng, R. Han, and S. Mishra, "Countermeasures against traffic analysis attacks in wireless sensor networks," in *Proc. of SECURECOMM*, 2005, pp. 113–126.

[17] P. Welch, "The use of fast fourier transform for estimation of power spectra: A method based on time averaging over short, modified periodograms," *IEEE Transactions on Audio Electroacoustics*, vol. 15, pp. 17–20, 1967.

[18] E. Candes and M. Wakin, "An introduction to compressive sampling," *IEEE Signal Processing Magazine*, vol. 25, no. 2, pp. 21–30, 2008.

[19] J. Tropp and A. Gilbert, "Signal recovery from random measurements via orthogonal matching pursuit," *IEEE Transactions on Information Theory*, vol. 53, pp. 4655–4666, 2007.

[20] "The open source os for the internet of things, http://www.contiki-os.org."

[21] S. Raza, T. Voigt, and U. Roedig, "6LoWPAN Extension for IPsec," in *Proc. of Interconnecting Smart Objects with the Internet Workshop*, 2011.

[22] A. Fragkiadakis, S. Nikitaki, and P. Tsakalides, "Physical-layer Intrusion Detection for Wireless Networks using Compressed Sensing," in *Proc. of WiMob*, 2012.

[23] W. Bajwa, J. Haupt, G. Raz, S. Wright, and R. Nowak, "Toeplitz-structured compressed sensing matrices," in *Proc. of SSP*, 2007, pp. 295–298.

[24] A. Dunkels, J. Eriksson, N. Finne, and N. Tsiftes, "Powertrace: Network-level power profiling for low power wireless networks," Tech. Rep.

Appendix D

Securing Cognitive Wireless Sensor Networks: A Survey

Securing Cognitive Wireless Sensor Networks: a Survey

Alexandros Fragkiadakis*, Vangelis Angelakis†, and Elias Z. Tragos*
*Institute of Computer Science, Foundation for Research and Technology-Hellas, GR 71110, Heraklion, Crete, Greece
†Department of Science and Technology, Linköping University, SE 58183, Linköping, Sweden.
Corresponding author: alfrag@ics.forth.gr

Abstract—Wireless Sensor Networks (WSNs) have gained a lot of attention recently due to the potential they provide for developing a plethora of cost-efficient applications. Although research on WSNs has been performed for more than a decade, only recently the explosion of their potential applicability has been identified. However, due to the fact that the wireless spectrum becomes congested in the unlicensed bands, there is a need for a next generation of WSNs, utilizing the advantages of Cognitive Radio (CR) technology for identifying and accessing the free spectrum bands. Thus, the next generation of wireless sensor networks is the Cognitive Wireless Sensor Networks (CWSNs). For the successful adoption of CWSNs, they have to be trustworthy and secure. Although the concept of CWSNs is quite new, a lot of work in the area of security and privacy has been done until now, and this work attempts to present an overview of the most important works for securing the CWSNs. Moreover, a discussion regarding open research issues is also given in the end of this work.

1 Introduction

WSNs are daily gaining more ground into our lives with applications ranging from construction monitoring and intelligent transport, to smart home control and assisted living. Through the novel communication standards of the past decades such as Zigbee and IEEE 802.15.4, along with the pervasiveness of IEEE 802.11, the development of inter-operability and commercial solutions has been enabled. Typically though, these solutions do suffer from strict deployment design and poor scalability. At the same time, the reliability of WSNs is a key topic for their mass adoption for more critical, rather than luxury or pilot applications, such as the smart metering [1].

Cognitive Radio (CR) features such as the opportunistic spectrum (white space) usage, the introduction of secondary users in licensed bands, and the ability to learn the environment through sensing, present themselves as a mean to overcome spectrum shortage. Enabling such CR characteristics over "traditional" WSNs allows them to change their transmission parameters according to the radio environment, and possibly enhance the reliability of WSNs in areas densely populated by wireless devices. These Cognitive Radio-imbued WSNs (CWSNs) can have access to new spectrum bands with better propagation characteristics. By adaptively changing system parameters like the modulation schemes, transmit power, carrier frequency, channel coding schemes, and constellation size, a wider variety of data rates can be achieved, especially when CWSNs operate on Software-Defined Radios. This can improve device energy efficiency, network lifetime, and communication reliability.

CR technology in CWSNs has largely improved network performance. On the other hand, due to the cognitive nature of these networks, new vulnerabilities have appeared. Attacks targeting a CWSN can come from internal or external network sources. Adversaries can exploit vulnerabilities in different communication layers, many of which target the CR characteristics of the CWSN. There are also special types of attacks that try to infer sensitive information on the application and that execute in the sensors themselves [2]. Our work here aims to make a brief, yet succinct overview of possible attacks on CWSNs. We therefore begin providing a background of WSNs and CWSNs in Sections 2 and 3, respectively. We then move to identify the common features and attacks in both of these types of networks in Section 4. In Section 5, we specify attacks applicable only to CWSNs, and in Section 6 we detail security mechanisms for attack detection at different communication layers. Our work concludes with a discussion of open issues in Section 7.

2 Overview of wireless sensor networks

WSNs have become widely available from the early 2000's, as sensing components and communication modules were already becoming cheap and small [3]. Monitoring the environment with such low cost devices became since then efficient, with a large volume of research having been conducted in the last almost two decades (one can trace the origins of WSNs in [4]). By now, WSN solutions are deployed in large scales, in various places,

and are being widely used in a variety of applications ranging from military [5], to agricultural [6], and from health care [7] to traffic management [8].

A WSN typically comprises a set of sensor nodes equipped with limited, low-power/short-range communication capabilities. Each of these nodes is a computational/communication platform which consists of (at least) a sensing module, a transceiver, a processor unit, and a power unit. The sensor node has typically small physical dimensions and its components are inexpensive. To make these sensor nodes more appealing, communication is commonly based on the license-free Industrial, Scientific and Medical (ISM) frequency band [9], in order to further limit operational costs for the overall WSN installation, and to enable direct use of off-the-shelf communication solutions [10].

Depending on the application and deployment scenario, WSNs may vary in the communication paradigm they employ [11]. WSN applications set up to observe and consequently report to a "fusion center" the occurrence of an event (such as a fire), do not need to transmit continuously all measurements acquired by the sensors [12]. On the other hand, in scenarios such as pollution measurements [13] or seismic activity, the raw data can well be meaningful in its entirety; in such a case, the transmissions required would clearly be producing a heavy communication load, thus efficient channel access between the nodes as presented in [14] is required. These two extremely different cases indicate a mapping to the range of communication modes that may have to be used to handle the WSN most limiting resources: spectrum and energy (see [15], [16] and the references therein). A very rudimentary method to address these is WSN topological solutions which can be multi-hop [17], hierarchical [18] or one-hop to infrastructure [19]. Each one in the respective references given has a reasoning to the underling spectrum management. Furthermore, in each of these cases a key factor that affects the system design is the power source and lifetime requirement of the WSN [20]. The node power unit, mentioned earlier, may be unlimited: for example in indoor scenarios where the nodes can be directly plugged to the power grid. In such cases, energy plays little to no role. On the other hand, there can be extremely constrained scenarios such as the Smartdust, where literally every mWatt has to be accounted for, as the battery providing power is constrained even by its physical size, let alone its capacity. Energy harvesting [9] has recently been gathering a significant attention as it can enable extension of the node lifetime, leveraging the environment resources (heat, motion, RF radiation, etc.).

3 Enhancing Wireless Sensor Networks with CR Technology

While the WSN solutions were progressing well into the late 2000's, the dramatically rising demand for wireless connectivity brought the spectrum utilization into the spotlight. Cognitive radio [21] and opportunistic communications, especially under the paradigms of opportunistic access or delay tolerant networking, came naturally into the frame of WSNs [22], [23]. Research has thus began into considering CR aspects for WSNs [24], [25].

Opportunistic access is based on sending the transmissions over the "most suitable" spectrum band under a set of predefined application-driven requirements. With delay tolerance, a temporal aspect comes also into play: nodes can withhold data and transmit them at the "best" possible moment, subject to the application delay constraints. To enable these features, an additional amount of dedicated spectrum sensing is required by the nodes, and in some cases local coordination schemes are used in order to cooperatively infer about the radio spectrum usage at a specific area [26], [27]. This flexibility is further employed to adjust transmission parameters (modulation and coding schemes, and transmission power) to reduce overall power consumption. Existing schemes developed to obtain spectrum awareness for cognitive radios in some cases consider the power consumption problem [28], [29], a clearly critical issue for CWSN. Reduced power consumption considered in CWSNs not only can extend the lifetime of sensor nodes, but can also limit the overall spectrum inefficiencies of the network, allowing for a substantial increase in spectrum utilization [30], [31].

4 Features and Common Attacks in WSNs and CWSNs

4.1 Common features of WSNs and CWSNs

WSNs and CWSNs are two types of sensor networks that have a number of common characteristics. They consist of miniature devices, called as motes or sensors that are severe resource constrained devices in terms of memory, processing, and energy [32], [33]. They usually do not perform any computation on the data they collect; they just forward this information to much more powerful devices (called as sinks) for further processing.

The communication medium used for both WSNs and CWSNs has a broadcast nature and the used spectrum is split into several channels, depending on the protocol used. For example, there are up to 16 available channels for the IEEE 802.15.4 in the 2.4 GHz frequency band.

In both types of networks, the communication protocols used have a number of inefficiencies and vulnerabilities that allow potential attackers to launch a variety of destructive attacks against these networks. The result of these attacks has catastrophic consequences including network performance deterioration, information theft, lifetime minimization, battery depletion, etc.

A multi-hop type of communication is often used in both types of networks (e.g. [34]) when data from a large

and/or harsh area have to be sensed. Information flows from a sensor to a sink through multiple intermediate sensors that route packets according to an appropriate routing algorithm (e.g. RPL [35]). In a number of contributions, the network is split into several clusters and decisions are taken by the cluster heads in order to minimize sensors communication overhead and save energy, prolonging network's lifetime.

In both types of networks, network topology is highly dynamic and unpredictable without any central management. This is the case when sensors are deployed in harsh and volatile environments (e.g. [36], [37]). In such cases, adversaries can more easily attack and compromise the WSN.

4.2 Common attacks against WSNs and CWSNs

The above common characteristics of WSNs and CWSNs make them vulnerable to a number of security threats. A diverse range of vulnerabilities are exploited by adversaries who can have several incentives, e.g. network disruption, information theft, etc. In general, there are two types of attackers [38]: (i) external attackers that are not authorized participants of the sensor network, and (ii) internal attackers that have compromised a legitimate sensor, and use it to launch attacks in the network. Furthermore, attackers can be classified into passive and active. Passive attackers monitor network traffic without interfering with it. Their aim is to eavesdrop on the exchanged information and to acquire private data, or to infer about information-sensitive applications that execute in the sensors (e.g. [2]). Active attackers disrupt network operation by launching several types of attacks that cause DoS (Denial-of-Service) in the WSN.

A severe DoS attack is jamming at the physical layer of the network. An adversary by creating interference, mainly through energy emission in the neighboring channels of the channel used by the sensor network ([39]), substantially increases the noise such that potential receivers become completely unavailable to receive and decode any information. This results to packet loss and further retransmissions by the senders that potentially lead to energy waste in the sensor network.

Jamming attacks can also be launched at the link layer. Here, an attacker can violate several characteristics of the communication protocol and cause packet collisions, exhausting sensors' resources. The authors in [40] show how a single adversary can cause severe performance degradation by violating several rules of the link layer protocol (back-off mechanism). Another popular attack is the Sybil attack where an adversary maliciously uses the identities of a number of sensors. This is achieved either by learning other sensor's identities or by fabricating new ones [41]. Furthermore, other types of attacks such as MAC spoofing ([42]) and ACK attacks ([43]) can cause confusion and packet loss in the network.

A major challenge in a WSN is maximizing its network lifetime by choosing the appropriate mode of communication. Single-hop communication, where the sensors communicate directly to a sink, is the flavour mode when the number of the sensors and the communication radius are small [44]. On the other hand, when the number of sensors is large (a typical case when a large area has to be covered by sensors) multi-hop communication is the most appropriate mode that saves sensors' energy, prolonging network's lifetime. In the multi-hop scenario, sensors have a dual role; they sense the environment and they also route the packets of their neighbors towards the sink (and vice-versa). Packet forwarding and optimal path selection is performed by following an appropriate routing protocol. Adversaries can exploit several vulnerabilities and launch attacks against multi-hop sensor networks. Various attacks have been reported in the literature:

- **Selective forwarding attack**, where attackers drop the packets they have to route, randomly or selectively based on some rules (e.g. packets that originate from a specific sensor).
- **Sinkhole attack**, where an attacker by broadcasting fake information make the legitimates nodes believe that the attacker is attractive according to the routing protocol. If this attack is successful, neighboring sensors will forward their packets to the attacker that is then free to alter or steal information or drop the packets.
- **Wormhole attack**. This attack is performed by a number of colluding adversaries that forward packets between them through a direct long-distance and low-latency communication link (wormhole link). With this attack, legitimates sensors at a specific area of the network believe that they are close neighbors with sensors of another area that is however far away. This illusion creates confusion and affects routing within the network.

Except the above attacks that exploit several vulnerabilities in different layers of the communication stack, there is a special type of attack that aims to infer about information-sensitive application that execute in the sensors. Suppose that there is an on-body sensor network (e.g. [45]) consisting of a number of sensors that record high-sensitivity data such as the heart rate, oxygen saturation, etc. Usually these applications transmit the sensed data to a sink in a periodic fashion [46]. Recent works ([2], [46]) have shown that adversaries can infer about these applications by passively monitoring the network traffic and detecting its periodic components that can finally reveal the potential medical applications. This becomes feasible using the appropriate signal processing techniques (e.g. Lomb-Scargle periodogram) that discover traffic's periodic components even if it is encrypted.

5 Specific attacks against CWSNs

As described in the previous section, WSNs and CWSNs have a number of common features and hence some common vulnerabilities that can be exploited by potential adversaries. Nevertheless, CWSNs have two unique characteristics (that WSNs do not have) due to their cognitive nature [47]:

- **Cognitive capability** which allows sensors to sense the environment for white spaces. Then, through a spectrum management process they decide upon which band to use for transmission, and how to estimate the related to transmission physical layer parameters (frequency, modulation type, power, etc.). The cognitive cycle consists of several mechanisms: (i) radio environment, (ii) spectrum sensing, (iii) spectrum analysis, and (iv) spectrum decision.
- **Reconfigurability** that allows sensors to change on-the-fly their physical layer parameters and adapt to their environment. As sensors in CWSNs opportunistically use the fallow bands, they have to be flexible and vacate a band if a primary transmission is detected.

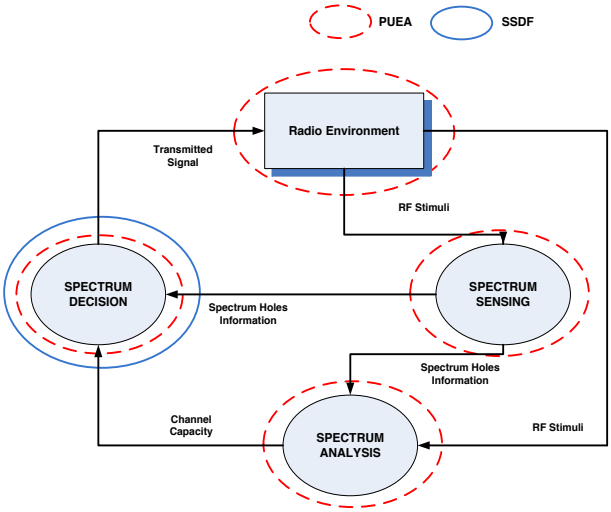


Fig. 1: The cognitive cycle [47]

These unique characteristics make CWSNs vulnerable to a number of novel attacks. One of the most destructive attacks is called as **primary user emulation attack** (PUEA). In this attack, an adversary mimics a primary user (PU) by transmitting fake incumbent signals [48]. Legitimate sensors will immediately evacuate the specific (under attack) frequency band, seeking for an alternative band to operate. Adversaries launching this attack can be of two types: (i) greedy sensors that emit the fake incumbent signals in order to make legitimate sensors evacuate the band in order to acquire its exclusive use, and (ii) malicious sensors that aim to cause a DoS attack making sensors hop from band to band. Regardless the type of the adversary, the PUEA attack can cause severe network disruption and a huge energy waste to the legitimate sensors. Fig. 1 [47] shows that the PUEA attack affects all parts of the cognitive cycle.

As mentioned before, spectrum sensing is a fundamental operation, and is one of the most challenging issues of the cognitive cycle. Spectrum sensing is the task of obtaining awareness about the spectrum usage and the possible presence of primary users [49]. During this operation, there is always the risk for the cognitive sensors not to correctly decode and hence detect the primary signals because of the shadow fading and hidden node effects. If this happens, harmful interference will be created to the primary transmitters. Collaborative spectrum sensing has been proposed as a solution to this problem [50]. In collaborative spectrum sensing, all sensors perform spectrum sensing and report their findings to a fusion centre (FC). The FC after performing a spectrum analysis procedure based on the sensors' reporting, decides if a spectrum hand-off has to be performed, and at which frequency band. In a CWSN, the sink or the cluster heads (if the sensor network uses clusters) can have the role of the FC. However, if the network is not partitioned into clusters, or the sink is far away from the majority of the sensors, this centralized scheme is not feasible. In such cases, distributed sensing can take place, where each sensor based on its own spectrum observation and the observations shared by its neighboring sensors, makes its own spectrum decisions [51].

Adversaries can exploit the above mechanisms and affect FC's decision (or their neighbors' decision in distributed sensing) by sending false observations regarding spectrum usage. This attack is called as **spectrum sensing data falsification** attack (SSDF). SSDF attackers can report that a specific band is vacant when it is not, or that is occupied by primary signals when it is not. In the first case, harmful interference to the primary users will be created, while in the latter, legitimate sensors will keep performing costly (in terms of energy) spectrum hand-offs. Attackers can have different motives: (i) they can be greedy users that continuously report that a specific band is occupied in order to acquire its exclusive use, and (ii) they can be malicious nodes that by sending false observations, aim to create interference to primary transmitters or create a DoS attack to the network due to the continuous spectrum hand-off of the legitimate sensors. SSDF attacks can also be initiated by unintentionally misbehaving sensors that report false observations because some parts of their software or hardware components are malfunctioning. This type of attack can substantially degrade network's performance as the authors in [52] show. Regarding the cognitive cycle, the SSDF attack affects the spectrum analysis, and spectrum decision operations (Fig. 1).

6 Security, privacy and reliability mechanisms for CWSNs

6.1 Security

Securing a WSN is of paramount importance, and for this reason a large number of contributions exist in the literature for the detection and mitigation of attacks against this type of networks. Depending on the attack type, different strategies and algorithms are followed.

6.1.1 Physical layer attack detection

As mentioned in Section 4.2, jamming at the physical layer can cause disruptive DoS attacks in a WSN. The detection techniques try to (almost) instantly detect that a jamming attack is taking place by considering various metrics. The authors in [53] use the signal-to-interference-plus-noise ratio (SINR) as the metric that can signal the jamming attack. The recorded SINR values are fed to a cumulative-sum algorithm that is able to detect abrupt changes that are caused by the attacker's presence. The performance of this anomaly-based detection algorithm is augmented if several monitors are used in a collaborative intrusion detection scheme. In [54], the definition of several types of attackers is given, and jamming detection is performed by using multiple if-else statements considering as metrics the *packet delivery ratio*, the *bad packet ratio*, and the *energy consumption amount*. In [55], a distributed anomaly detection algorithm is presented based on simple thresholds, and a method for combining measurements using the Pearsons product moment correlation coefficient. RF jamming attacks is the focus of [56] where the proposed algorithm applies high order crossings, a spectral dissemination technique that distinguishes normal scenarios from two types of defined attackers. The detection algorithm is based on thresholds considering the signal strength and location information. The authors in [57] propose DEEJAM, a defensive mechanism that uses an IEEE 802.15.4-based hardware. Here, the proposed algorithm hides messages from a jammer, evades its search, and reduces the impact of the corrupted messages.

6.1.2 Link layer attack detection

Contributions that study the detection of attacks at the link layer include [40]. Here, an anomaly-based algorithm is presented considering the ratio of the corrupted packets over the correctly decoded packets as the metric that reveals jamming when the attacker's energy is emitted on the same channel. In [58], the authors explore energy-efficient attacks targeting three WSN protocols: (i) S-MAC, (ii) B-MAC, and (iii) L-MAC. As a countermeasure they suggest the use of shorter data packets for the L-MAC, and high duty cycle for the S-MAC. Link layer misbehaviour in [59] is detected by applying a non-parametric cumulative-sum algorithm considering the expected back-off value of the honest participants. MAC address spoofing detection in WSN is studied in [60]. In that work, an approach based on Gaussian mixture models that considers RSS (Received-Signal-Strength) profiles is used to detect if a MAC address is spoofed. RSS is a metric that is hard to forge arbitrarily, and it highly depends on the transmitter's location. The authors in [42] propose an algorithm that leverages the sequence number field carried by the data packets. This algorithm records the sequence number of each received frame and that of the last frame coming from the same source node. When the gap between the current sequence number and the last recorded one is between a specific range, is considered as abnormal. For each abnormal frame, a verification process follows to declare the specific frame as normal or spoofed.

Regarding the Sybil attack detection, the algorithm in [61] uses the ratios of the RSSI (received-signal-strength-indicator) recorded in a number of sensor monitors when a packet is transmitted within their communication range. If these ratios are very close to the ratios computed when a packet with a different identity is used, the corresponding transmitter is flagged as a Sybil attacker. In [62], the detection algorithm exploits the characteristic that every Sybil (forged) sensor has the same set of neighbors as they are created by the same adversary. It detects the Sybil attack by comparing the information collected from neighboring sensors (contained in small messages). In [63], Sybil attacks are detected by exploiting the spatial variability of radio channels in environments with rich scattering. An enhanced physical layer authentication scheme is used for both wideband and narrowband wireless systems.

6.1.3 Network layer attack detection

As described in Section 4.2, a wide number of vulnerabilities of the routing protocols can be exploited in sensor networks. Different countermeasures have been proposed for the detection of these attacks. In [64], a lightweight scheme uses a multi-hop acknowledgment technique to launch alarms when responses from intermediate sensors are missing. Each time a sensor receives a data packet, it sends an ACK to the sensor that handled the packet in the previous hop. If a sensor receives less than a number of ACK packets within a specified time, it suspects that the previous report it forwarded, has been dropped by a malicious sensor. If this is the case, it sends an alarm packet to the sink, reporting its next-hop sensor as a potential malicious sensor. The sink after it receives all alarm packets it infers about the malicious sensors. The authors in [65] propose a centralized scheme with the use of support vector machines (SVMs). A 2D SVM is initially trained when no attacker is present, using the hop count and the measured bandwidth at the sink as features. At run time, the detection algorithm based on the SVM executes at the sink. A different approach is followed in [66] where each sensor observes the behavior of its neighbors recording the number of packets they

forward, along with the source address of the originating sensor. Based on these observations, it updates a trust metric for each of its neighbors that reveals the potential attackers. After a sensor has been labelled as an attacker, the routing tables are modified in order to isolate that sensor from the network.

For the detection of the sinkhole attacks, a distributed detection scheme is presented in [67]. Every sensor S_i is set in promiscuous mode and records the route update packets transmitted by its neighbors. Furthermore, two rules have been defined that if violated, an alert message is broadcasted: (i) if sender's ID matches S_i's ID, and (ii) if sender's ID does not belong to the known IDs of S_i's neighbors. This detection scheme also employs a collaborative detection algorithm that reveals the potential attacker based on an intersection computation of the information carried by the alert messages. Ngai et al. [68] propose a detection algorithm that consists of two steps: (i) it locates a list of suspected sensors by checking data consistency based on the information sensors report to the sink, and (ii) it labels a sensor as an attacker by analyzing the network flow information (represented by directed edges between communicating sensors). The authors in [69] show that shortest-path routing protocols select a series of paths whose length exhibits a log-normal distribution. Based on this observation, they propose an anomaly detection algorithm by deriving tolerance limits from the log-normal distribution of path lengths when no attacker is present.

Regarding the wormhole detection, the scheme proposed in [70] considers the round-trip-time (RTT) between an originating sensor and its destination. RTT depends on how far the intermediate sensors are located. If a wormhole attack is in progress, RTT can significantly increase, as packets are replicated in a different part of the network from colluding attackers. In [71], a localized scheme based on connectivity graphs is proposed. It seeks for *forbidden substructures* in the connectivity graphs that should not be present under normal circumstances. The authors in [72] propose a distributed detection algorithm that detect wormhole attacks based on the distortions these attacks create in the network. This scheme uses a hop counting technique as a probe procedure, reconstructing local maps for each sensor, and then a diameter-feature that depends on the number of neighboring nodes, for anomaly detection.

6.1.4 Detection of attacks that exploit vulnerabilities of the cognitive nature of CWSNs

A possible framework for securing CR networks has been proposed in [73] and can easily be extended to secure CWSNs. This framework attempts to identify the mechanisms that can mitigate the specific attacks on Cognitive Radio networks. As discussed in Section 5, there are two major types of attacks that can be launched against CWSNs: (i) PUEAs, and (ii) SSDF attacks. Regarding the detection of the PUEAs, there is a large number of significant contributions that split into two main categories: (i) location-based, and (ii) non-location based. Location-based contributions assume that the locations of the primary transmitters are known a priori.

The work in [48] considers both the location information of the primary transmitter along with the RSS values collected by a separate sensor network each time an primary transmission is taking place. Based on the RSS measurements the location of the transmitter is estimated, and if it is different than the (already) known location of the legitimate primary transmitter, an alarm is triggered. Jin et al. [74] developed an algorithm that considers the received power measured at the radio interfaces of the secondary users (SUs) in a specific band. Then, by using Fenton's approximation and Wald' sequential probability radio test, they decide on the corresponding hypothesis about the presence or not of a PUEA attacker. The received power is also considered in [75] where the authors propose a variance method to detect the attack. This scheme first estimates the variance of the received power from the primary transmitter, and then it determines whether a received signal is from the primary transmitter or from an attacker.

In non-location based algorithms like in [76], the locations of the primary transmitters is not required to be known. The authors state that the channel impulse response can reveal if a primary transmitter has moved to a different location. Their approach uses a *helper node* (HN) that is located very close to a primary transmitter in a fixed location. This node is used as a bridge between the SUs and the primary transmitter by allowing SUs to verify cryptographic signatures by HN's signals, and then obtain HN's link signals in order to verify primary transmitter's signals. The authors show that by using the first and second multi-path components measured at HN, they can verify if the transmitted signal belongs to the legitimate primary user or it is fake. The scheme presented in [77] uses a public key cryptography mechanism where a primary transmitter integrates its transmitted data with cryptographic signatures. Each SU that detects a primary signal attempts to verify its integrated signatures. If verification fails, the signal is characterized as fake.

Regarding the SSDF attack detection, in [52] a centralized algorithm calculates the trust values of SUs based on their past record. Additionally, consistency checks are performed because the trust values can become unstable if an attacker is present or there is not enough information. If the consistency value and the trust value of an SU drops below a specific threshold, the specific SU is characterized as an attacker. Rawat et al. [78] propose a centralized scheme that computes a reputation metric for each SU based on SU's past observation, and the decision is made by the FC during that round of observations. If there is a decision mismatch, SU's reputation metric is increased by one, and if it becomes larger than a predefined threshold, SU is labelled as

an attacker. Reputation metrics are also used by other similar contributions like in [79], [80].

6.2 Privacy

Although security attacks in WSNs have been very extensively researched until now, "privacy" attacks are a not so common research topic. Most works until now have focused mainly on protecting the location privacy of the sensor nodes, while others focus on protecting the data traffic that are transmitted by the nodes. However, when sensors are enhanced with CR technology, the traditional WSN privacy attacks still exist, with the addition of other attacks for eavesdropping the sensing data (in collaborative spectrum sensing) and the context of the exchanged sensor data, for impersonating the PU and against the anonymity of a sensor node. In this section the common attacks against privacy on CWSN are described, together with the existing mechanisms for mitigating these attacks.

6.2.1 CR Location privacy

Location privacy is a major research topic in cognitive WSNs due to the fact that the spectrum opportunities (namely the unoccupied spectrum frequencies or the white spaces) are heavily depending on the location of both the sensor nodes and the PUs. The received PU signal at the sensor nodes is highly related to the distance between the sensor nodes, and a malicious user can identify the sensor node location using geo-location mechanisms. Furthermore, in participatory sensing [81] the data from the sensor nodes are usually tagged with location and the time.

According to [82], the respective location privacy attacks can be either external (combined with eavesdropping) or internal. An external attacker can intercept the spectrum sensing reports that are exchanged throughout the CWSN by eavesdropping the communication of the sensor nodes either with each other, or with the FC (in case of a centralized spectrum sensing system). That way, the attacker is able to know the received PU signals of all sensor nodes and by correlating the data with its own sensing reports, he is able to identify the location of the sensor nodes. An internal attacker can be either another node participating in the collaborative sensing or the fusion center (or an attacker impersonating the fusion center). That way the attacker seems to be a legitimate node that receives the sensing reports from all other nodes, and can easily compromise their location by correlating the data with his physical location. An internal attacker can also exploit the results of the aggregated sensing reports that are being transmitted by the FC. That way, comparing the reports before and after the inclusion of a new node in the network, it is easy to identify its location.

6.2.1.1 Mitigation

For preserving the privacy of cognitive sensor nodes, in [82] a combination of techniques for cryptography and sensing data randomization has been proposed. The first technique uses the concept of secrets [83] and each sensor encrypts its sensing data in such a way that the FC should get all reports in order to be able to decrypt the aggregated sensing report. That way, a malicious user cannot decrypt the reports of a specific user by intercepting either its reports or even the encrypted reports from all sensors, hence sensors' locations cannot be estimated.

Another proposal ([82]) for protecting the location of cognitive sensors includes the transmission of dummy sensing reports from one of the legitimate nodes or the fusion center when a new node is joining or leaving the network. Although this can degrade the performance of collaborative sensing, an appropriate selection of the dummy report and its weight on the overall sensing aggregation can have a minimal impact, without affecting significantly the sensing result.

Proposals for ensuring location privacy in participatory sensing include the anonymization of sensing reports using the principle of k-anonymity [84], [85], [86], [87], which assumes that at least k users are located at the same area, and thus they tag their sensing reports with an area "ID", and not with their actual location information. That way, if an attacker eavesdrops the reports of the sensor nodes, only an abstract view of the general area of the users could be extracted and not an actual location. However, the performance of such a sensing system is heavily depending on the size of the area, because a small area can result to an optimum sensing result but can also give enough information to the attacker to identify the location of the sensor nodes. On the other hand, a large area may preserve the nodes' location information, but can degrade significantly the performance of the participatory sensing system.

6.2.2 Sensed data privacy

Like traditional WSNs, CWSNs are deployed for getting automated measurements and transmitting them to an application server for processing. This information may be sensitive in some applications and must be protected from unauthorized access and use. For example, hijacking the information sent by sensors measuring the energy consumption of devices in a household, may reveal the presence/absence of the habitants, which could be utilized by burglars. Respective attacks against the sensor data include eavesdropping, impersonation, and traffic analysis [88].

Eavesdropping (or passive monitoring) is a very common attack on WSNs, under which an attacker is listening the communication channel of the sensor nodes and intercepts their data. In this attack, the malicious

node is hidden from the sensor nodes because it does not communicate directly with them. Under the impersonation attack, the malicious node impersonates either a legitimate node or the FC, and gets the data directly from the legitimate sensor nodes. This attack can be the first point to launch other attacks changing the data and transmitting false data to the other nodes. The traffic analysis is used by attackers to extract the context of data that are transferred by the sensors, and is achieved by analysing the traffic patterns from eavesdropping the wireless links. Using the traffic analysis attack, a malicious node can also identify some nodes that have a special role in the CWSN (i.e. who has the role of the FC).

6.2.2.1 Mitigation

Targeting to avoid the disclosure of the sensed data to unauthorized recipients, several proposals have been made in the literature, which mainly focus on anonymity schemes or on information flooding. Using anonymization, the data sent by a legitimate node do not contain personal information that can be used to track back the measurements to the originating sensor node [89]. In [90], a framework for context-aware privacy of sensor data is proposed, which includes a two step process of (i) identifying which data will be shared, and (ii) obfuscating the data before transmitting them. Although most previous anonymization proposals were focused on protecting sensor location information [82], [91], they can be relatively easily adapted to the sensed data that the nodes are transmitting. Information flooding is another technique that can be used to protect the data privacy in CWSNs, as proposed in [92], which discusses that probabilistic flooding can give good protection to the node information while being energy efficient.

7 Conclusion

WSNs and CWSNs are two similar sensor network types with quite a few common features. Recently there has been an explosion of Smart City applications for providing advanced ICT-based services to citizens with the use of enhanced WSN networks. For the realization of such applications a plethora of sensing and actuating devices are usually installed either in a city area or within buildings. In this context, the WSNs will be playing a significant role in the everyday life of people, and thus their security is of great importance. This explosion in the number of wireless sensing and actuating devices in city areas together with the continuous installation of many (public and private) wireless access networks in these areas, have resulted in congestion in the unlicensed spectrum bands (ISM bands around 2.4 GHz) that are used for both WSNs and WiFi. For mitigating the congestion effects on the WSN networks, there are proposals to equip the latter with CR technology forming the CWSNs, which on the one hand solves several issues of traditional WSNs security-wise, but introduces new security threats.

Securing WSNs and CWSNs is of key importance, and a large pool of contributions from the literature for the detection and mitigation of attacks against these networks has been presented in this paper. Furthermore, an overview of the most common attacks against CWSN is presented in Table 1. Depending on the attack type, different strategies and algorithms are followed. Exploiting the CR features of CWSN enables two major classes of attacks that can be launched against them: (i) PUEAs, and (ii) SSDF attacks. Regarding the detection of the PUEAs a significant number of contributions exist which can be broken into two categories: (i) location-based, and (ii) non-location based. For the former the key challenge is the detection of the attacker's location, an issue that is open in many other problems of wireless networking. The SSDF attack detection in the literature presented here is primarily based on the notions of reputation and trust, given the collaborative nature of the proposed solutions. Regarding privacy, the most common attacks are those against identifying the location of the cognitive sensors node, and those against intercepting the sensing data.

Although much research has been done in the literature regarding the security of the CWSNs, there are still several challenges and open research issues remaining. One of the most important challenges is related to introducing trust within the CWSN architecture. Although several attempts for mitigating SSDF attacks are introducing reputation mechanisms for the cognitive nodes, these can be considered as an "add-on" feature, while a trust framework embedded within the cognitive nodes that not only addresses the SSDF attacks, but ensures the complete trustworthy operation (starting from the sensed data and going all the way up to ensuring the trustworthiness of the applications that run on the nodes) of the cognitive nodes. Another open challenge is related to designing lightweight cryptographic algorithms that could run on the very resource-limited cognitive sensor nodes, focusing on private-key cryptography, efficient key distribution schemes for symmetric key cryptography, and efficient key management protocols for public key cryptography. Regarding routing, in CWSNs there is a need for further research on secure routing schemes taking into account the spectrum assigned to each one of the intermediate nodes, as well as the mobility of the nodes, and the potential scalability and efficiency issues. Moreover, in data aggregation mechanisms there is a need for further research on enhancing the data aggregation and securing it against malicious cognitive users, introducing trust and security metrics. Other open research issues regarding security in CWSNs that need to be addressed in future research include the use of geo-location information for improving security i.e. in PUEA attacks, the investigation of

TABLE 1: Attacks against CWSNs.

Type of attack	OSI Layer	Characteristic	Common with WSN
Jamming	Physical layer	DoS attack creating interference, increasing packet loss and collisions	Yes
Back-off attack	Link Layer	an attacker causes severe performance degradation by minimizing the CWmin and thus his back-off period	Yes
Sybil attack	Cross layer	stealing sensors identities, i.e. MAC address, IP address, etc.	Yes
MAC spoofing	Link layer	alternating a MAC address on a network interface can help an unauthorized intruder enter a secure network	Yes
Selective forwarding attack	Network layer	attackers drop packets they have to route	Yes
Sinkhole attack	Network layer	attacker broadcasts false routing related information so that neighbouring nodes send them their packets and steals information or drops them	Yes
Wormhole attack	Network layer	adversaries exchange packets through a long-distance and low-latency links affecting routing making legitimate sensors believe that they are neighbours with sensors of another area	Yes
PUEA	Physical layer	adversaries mimic PU so that hey exploit unused frequencies that the other nodes assume as occupied by the PU.	No
SSDF attack	Physical layer	attackers provide false information regarding spectrum occupancy	No
Location privacy attacks	Physical layer	attackers intercept signals and sensing reports so that with data correlation they can identify the sensor location	No
Sensed data privacy attacks	Physical/link layer	attackers eavesdrop the channel and analyse the traffic to intercept the sensed data that are transmitted by the sensors	Yes

intelligent physical layer security mechanisms that exploit CR characteristics, the development of distributed mechanisms against SSDF attacks and the design of efficient cooperative mechanisms against malicious nodes and intruders.

ACKNOWLEDGMENT

The research leading to these results has received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) under grant agreements no. 609094 and no. 612361.

REFERENCES

[1] A. Liotta, D. Geelen, G. Kempen, and F. Hoogstraten, "A survey on networks for smart-metering systems," *International Journal of Pervasive Computing and Communications*, vol. 8, pp. 23–52, 2012.

[2] A. Fragkiadakis and I. Askoxylakis, "Malicious traffic analysis in wireless sensor networks using advanced signal processing techniques," in *Proc. of WoWMom*, 2013, pp. 1–6.

[3] I. Akyildiz, Y. S. W. Su, and E. Cayirci, "Wireless sensor networks: a survey," in *Comput. Networks (Elsevier)*, vol. 38, no. 4, 2002.

[4] S. DUST, "SMART DUST Autonomous sensing and communication in a cubic millimeter." [Online]. Available: http://robotics.eecs.berkeley.edu/~pister/SmartDust/

[5] M. Winkler, M. Street, K.-D. Tuchs, and K. Wrona, "Wireless sensor networks for military purposes," in *Autonomous Sensor Networks Springer Series on Chemical Sensors and Biosensors*, vol. 13, 2013, pp. 365–394.

[6] Y. Xiaoqing, W. Pute, W. Hana, and Z. Zhanga, "A survey on wireless sensor network infrastructure for agriculture," in *Computer Standards and Interfaces*, vol. 35, no. 1, 2013, pp. 59–64.

[7] J. Ko and J. Chenyang Lu ; Srivastava, M.B. ; Stankovic, "Wireless sensor networks for healthcare," in *Proceedings of the IEEE*, vol. 98, no. 11, 2010.

[8] A. Pascale, F. Deflorio, and B. Dalla Chiara, "Wireless sensor networks for traffic management and road safety," in *IET Intelligent Transport Systems*, vol. 6, no. 1, 2012.

[9] e. a. Fan Zhang, "A batteryless 19uw mics/ism-band energy harvesting body area sensor node soc," in *Solid-State Circuits Conference Digest of Technical Papers (ISSCC)*, 2012.

[10] B. Buchli, F. Sutton, and J. Beutel, "Gps-equipped wireless sensor network node for high-accuracy positioning applications," in *EWSN 2012, , LNCS 7158*. Springer-Verlag Berlin Heidelberg, 2012.

[11] P. Santi, in *Topology Control in Wireless Ad Hoc and Sensor Networks*. Wiley, 2005.

[12] G. Wittenburg, "Cooperative event detection in wireless sensor networks," in *Communications Magazine*. IEEE, 2012.

[13] R. P. K.K. Khedo and A. Mungur., "A wireless sensor network air pollution monitoring system." in *International Journal of Wireless and Mobile Networks*, vol. 2, no. 2, 2012.

[14] A. Antonopoulos and C. Verikoukis, "Network-coding-based cooperative arq medium access control protocol for wireless sensor networks," *International Journal of Distributed Sensor Networks, Hindawi*, vol. 2012, 2012.

[15] J. A. S. G. Zhou and S. H. Son, "Crowded spectrum in wireless sensor networks," in *Proc. 3rd Wksp. Embedded Net. Sensors*, 2006.

[16] "Energy conservation in wireless sensor networks: A survey," *Ad Hoc Networks*, vol. 7, no. 3, pp. 537 – 568, 2009.

[17] R. K. Tarek F. Abdelzaher, Shashi Prabh, "On real-time capacity limits of multihop wireless sensor networks," in *IEEE Real-Time Systems Symposium*, 2004.

[18] v. S. M. Iwanicki, K., "On hierarchical routing in wireless sensor networks," in *Information Processing in Sensor Networks, (IPSN)*, 2009.

[19] J. Z. . L. S. . H. H. . Y. Yang, "Mobile cellular networks and wireless sensor networks: toward convergence," in *IEEE Communications Magazine*, vol. 50, no. 3, 2012.

[20] W. Y. L. I. F. Akyildiz and K. R. Chowdhury, "Crahns: Cognitive radio ad hoc networks," in *Ad Hoc Networks*, vol. 7, no. 5, 2009.

[21] S. Haykin, "Cognitive radio: Brain-empowered wireless communications," in *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 2, 2005.

[22] Z. D. Senhua Huang, Xin Liu, "Opportunistic spectrum access in cognitive radio networks," in *IEEE INFOCOM*, 2008.

[23] O. S. A. Lindgren, A. Doria, "Probabilistic routing in intermittently connected networks," in *SIGMOBILE Mobile Computing Communications Review*, vol. 23, no. 2, 2003.

[24] M. C. V. I. F. Akyildiz, W.-Y. Lee and S. Mohanty, "Next generation/dynamic spectrum access/cognitive radio wireless networks: A survey," in *Computer Networks (Elsevier)*, vol. 50, no. 13, 2006.

[25] O. Akan, O. Karli, and O. Ergul, "Cognitive radio sensor networks," in *IEEE Network*, vol. 23, no. 4, 2009.

[26] S. Maleki, A. Pandharipande, and G. Leus, "Energy-efficient distributed spectrum sensing for cognitive sensor networks," in *IEEE Sensors Journal*, vol. 11, no. 3, 2011.

[27] E. Tragos, S. Zeadally, A. Fragkiadakis, and V. Siris, "Spectrum assignment in cognitive radio networks: A comprehensive survey," *Communications Surveys Tutorials, IEEE*, vol. 15, no. 3, pp. 1108–1135, Third 2013.

[28] J. Han, W. Jeon, and D. Jeong, "Energy-efficient channel management scheme for cognitive radio sensor networks," in *IEEE Transaction on Vehicular Technology*, vol. 60, no. 4, 2011.

[29] C. H. L. J. Y Xu, C Wu, "A cluster-based energy efficient mac protocol for multi-hop cognitive radio sensor networks," in *IEEE Globecom*, 2012.

[30] A. G. AS Zahmati, X Fernando, "Application-specific spectrum sensing method for cognitive sensor networks," in *IET Wireless Sensor Systems*, 2013.

[31] E. Tragos and V. Angelakis, "Cognitive radio inspired m2m communications," in *Wireless Personal Multimedia Communications (WPMC), 2013 16th International Symposium on*, June 2013, pp. 1–5.

[32] B. Otal, C. Verikoukis, and L. Alonso, "Efficient power management based on a distributed queuing mac for wireless sensor networks."

[33] J. Zarate, E. Stavrou, A. Stamou, P. Angelidis, L. Alonso, and C. Verikoukis, "Energy-efficiency evaluation of a medium access control protocol for cooperative arq."

[34] N. Gazoni, V. Angelakis, V. Siris, and B. Raffaele, "A framework for opportunistic routing in multi-hop wireless networks," in *Proc. of PE-WASUN*, 2010, pp. 50–57.

[35] U. Herberg and T. Clausen, "A comparative performance study of the routing protocols load and rpl with bi-directional traffic in low-power and lossy networks (lln)," in *Proc. of PE-WASUN*, 2011, pp. 1–8.

[36] G. Werner-Allen, K. Lorincz, M. Welsh, O. Marcillo, J. Johnson, M. Ruiz, and J. Lees, "Deploying a wireless sensor network on an active volcano," *IEEE Internet Computing*, vol. 10, pp. 18–25, 2006.

[37] B. Hull, V. Bychkovsky, Y. Zhang, K. Chen, M. Goraczko, A. Miu, E. Shih, H. Balakrishnan, and S. Madden, "Cartel: A distributed mobile sensor computing system," in *Proc. of ACM SenSys*, 2006, pp. 1–14.

[38] X. Chen, K. Makki, K. Yen, and N. Pissinou, "Sensor network security: A survey," *IEEE Communications Surveys and Tutorials*, vol. 11, pp. 52–73, 2009.

[39] A. Fragkiadakis, V. Siris, and A. Traganitis, "Effective and robust detection of jamming attacks," in *Proc. of Mobile Summit*, 2010, pp. 1–8.

[40] A. Fragkiadakis, E. Tragos, T. Tryfonas, and I. Askoxylakis, "Design and performance evaluation of a lightweight wireless early warning intrusion detection prototype," *EURASIP Journal on Wireless Communications and Networking*, vol. 2012, pp. 1–18, 2012.

[41] C. Loo, M. Ng, C. Leckie, and M. Palaniswami, "Intrusion detection for routing attacks in sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2, pp. 313–332, 2006.

[42] F. Guo and T. Chiueh, "Sequence number-based mac address spoof detection," in *Proc. of RAID*, 2005, pp. 1–20.

[43] Y. Xiao, S. Sethi, H. Chen, and B. Sun, "Security services and enhancements in the ieee 802.15.4," in *Proc. of Globecom*, 2005, pp. 31–35.

[44] J. Shi, X. Zhong, and S. Chen, "Study on communication mode of wireless sensor networks based on effective result," *Journal of Physics*, vol. 48, pp. 1317–1321, 2006.

[45] B. Otal, L. Alonso, and C. Verikoukis, "Novel qos scheduling and energy-saving mac protocol for body sensor networks optimization," in *Proc. of BodyNets*, 2008, pp. 1–4.

[46] L. Buttyan and T. Holczerr, "Traffic analysis attacks and countermeasures in wireless body area sensor networks," in *Proc. of WoWMom*, 2012, pp. 1–6.

[47] A. Fragkiadakis, E. Tragos, and I. Askoxylakis, "A survey on security threats and detection techniques in cognitive radio networks," *IEEE Communications Surveys and Tutorials*, vol. 15, pp. 428–445, 2013.

[48] R. Chen, J. Park, and J. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 26, pp. 25–37, 2008.

[49] T. Yucek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," *IEEE Communications Surveys and Tutorials*, vol. 11, pp. 116–130, 2009.

[50] S. Zarrin and T. Lim, "Cooperative quickest spectrum sensing in cognitive radios with unknown parameters," in *Proc. of Globecom*, 2009, pp. 1–6.

[51] Z. Tian, E. Blasch, W. Li, G. Chen, and X. Li, "Performance evaluation of distributed compressed wideband sensing for cognitive radio networks," in *Proc. of ISIF*, 2008, pp. 1–8.

[52] W. Wang, H. Li, Y. Sun, and Z. Han, "Attack-proof collaborative spectrum sensing in cognitive radio networks," in *Proc. of CISS*, pp. 130–134.

[53] A. Fragkiadakis, V. Siris, N. Petroulakis, and A. Traganitis, "Anomaly-based intrusion detection of jamming attacks, local versus collaborative detection," *Wireless Communications and Mobile Computing*, pp. 1–19, 2013.

[54] M. Cakiroglou and T. Ozcerit, "Jamming detection mechanisms for wireless sensor networks," in *Proc. of 3rd Int. Conference on Scalable Information Systems*, 2008.

[55] A. Sheth, C. Doerr, D. Grunwald, R. Han, and D. Sicker, "MOJO: a distributed physical layer anomaly detection system for 802.11 WLANs," in *ACM MobiSys*, 2006, pp. 191–204.

[56] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks," in *Proc. of ACM MobiHoc*, May 2005.

[57] A. Wood, J. Stankovic, and G. Zhou, "Deejam: Defeating energy-efficient jamming in ieee 802.15.4-based wireless networks," in *Proc. of SECON*, 2007, pp. 60–69.

[58] Y. Law, L. van Hoesel, J. Doumen, P. Hartel, , and P. Havinga, "Energy-efficient link-layer jamming attacks against wireless sensor network mac protocols," in *Proc. of SASN*, 2005, pp. 1–38.

[59] A. Cardenas, S. Radosavac, and J. Baras, "Evaluation of detection algorithms for mac layer misbehavior: Theory and experiments," *IEEE/ACM Transactions on Networking*, pp. 605–617, 2009.

[60] Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, "Detecting 802.11 mac layer spoofing using received signal strength," in *Proc. of Infocom*, 2008, pp. 1–9.

[61] M. Demirbas and Y. Song, "An rssi-based scheme for sybil attack detection in wireless sensor networks," in *Proc. of WoWMoM*, 2006, pp. 1–5.

[62] K. Ssu, W. Wang, and W. Chang, "Detecting sybil attacks in wireless sensor networks using neighboring information," *Elsevier Computer Networks*, vol. 53, pp. 3042–3056, 2009.

[63] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Channel-based detection of sybil attacks in wireless networks," *IEEE Transactions on Information Forensics and Security*, vol. 4, pp. 492–503, 2009.

[64] B. Yu and B. Xiao, "Detecting selective forwarding attacks in wireless sensor networks," in *Proc. of IPDPS*, 2006, pp. 1–8.

[65] S. Kaplantzis, A. Shilton, N. Mani, and Y. Sekercioglu, "Detecting selective forwarding attacks in wireless sensor networks using support vector machines," in *Proc. of ISSNIP*, 2007, pp. 335–340.

[66] Y. Cho and G. Qu, "Detection and prevention of selective forwarding-based denial-of-service attacks in wsns," *International Journal of Distributed Sensor Networks*, vol. 2013, pp. 1–17, 2013.

[67] I. Krontiris, T. Dimitriou, T. Giannetsos, and M. Mpasoukos, "Intrusion detection of sinkhole attacks in wireless sensor networks," in *Proc. of ALGOSENSORS*, 2008, pp. 150–161.

[68] E. Ngai, J. Liu, and M. Lyu, "An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks," *Elsevier Computer Communications*, vol. 30, pp. 1–12, 2007.

[69] D. Dallas, C. Leckie, and K. Ramamohanarao, "Hop-count monitoring: Detecting sinkhole attacks in wireless sensor networks," in *Proc. of ICON*, 2007, pp. 176–181.

[70] Z. Tun and A. Maw, "Wormhole attack detection in wireless sensor networks," in *Proc. of World Academy of Science, Engineering and Technology*, 2008, pp. 545–550.

[71] R. Maheshwari, J. Gao, and S. Das, "Detecting wormhole attacks in wireless networks using connectivity information," in *Proc. of Infocom*, 2007, pp. 1–9.

[72] Y. Xu, G. Chen, J. Ford, and F. Makedon, "Detecting wormhole attacks in wireless sensor networks," in *Proc. of IFIP*, 2008, pp. 267–279.

[73] A. Mihovska, R. Prasad, E. Tragos, and V. Angelakis, "Design considerations for a cognitive radio trust and security framework," in *Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), 2012 IEEE 17th International Workshop on*, Sept 2012, pp. 156–158.

[74] Z. Jin and K. Subbalakshmi, "Detecting Primary User Emulation Attacks in Dynamic Spectrum Access Networks," in *Proc. of ICC*, 2009, pp. 1–5.

[75] Z. Chen, T. Cooklev, C. Chen, and C. Pomalaza-Raez, "Modeling primary user emulation attacks and defenses in cognitive radio networks," in *Proc. of IPCCC*, 2009, pp. 208–215.

[76] Y. Liu, P. Ning, and H. Dai, "Authenticating primary users' signals in cognitive radio networks via integrated cryptographic and wireless link signatures," in *Proc. of the 2010 IEEE Symposium on Security and Privacy*, 2010, pp. 286–301.

[77] C. Mathur and P. Subbalakshmi, "Digital signatures for centralized DSA networks," in *Proc. of the 1st IEEE Workshop on Cognitive Radio Networks*, 2007, pp. 1037–1041.

[78] A. Rawat, P. Anand, H. Chen, and P. Varshney, "Countering byzantine attacks in cognitive radio networks," in *Proc. of ICASSP*, 2010, pp. 3098–3101.

[79] R. Chen, J. Park, and K. Bian, "Robust Distributed Spectrum Sensing in Cognitive Radio Networks," in *Proc. of Milcom*, 2008, pp. 1876–1884.

[80] E. Noon and H. Li, "Defending against hit-and-run attackers in collaborative spectrum sensing of cognitive radio networks: A point system," in *VTC*, 2010, pp. 1–5.

[81] J. Burke, D. Estrin, M. Hansen, A. Parker, N. Ramanathan, S. Reddy, and M. B. Srivastava, "Participatory sensing," in *In: Workshop on World-Sensor-Web (WSW06): Mobile Device Centric Sensor Networks and Applications*, 2006, pp. 117–134.

[82] Z. Gao, H. Zhu, S. Li, S. Du, and X. Li, "Security and privacy of collaborative spectrum sensing in cognitive radio networks," *Wireless Communications, IEEE*, vol. 19, no. 6, pp. 106–112, 2012.

[83] E. Shi, R. Chow, T. h. Hubert Chan, D. Song, and E. Rieffel, "Privacy-preserving aggregation of time-series data," in *In NDSS*, 2011.

[84] K. L. Huang, S. Kanhere, and W. Hu, "Towards privacy-sensitive participatory sensing," in *Pervasive Computing and Communications, 2009. PerCom 2009. IEEE International Conference on*, 2009, pp. 1–6.

[85] C. Cornelius, A. Kapadia, D. Kotz, D. Peebles, M. Shin, and N. Triandopoulos, "Anonysense: Privacy-aware people-centric sensing," in *Proceedings of the 6th International Conference on Mobile Systems, Applications, and Services*, ser. MobiSys '08. New York, NY, USA: ACM, 2008, pp. 211–224. [Online]. Available: http://doi.acm.org/10.1145/1378600.1378624

[86] A. Kapadia, N. Triandopoulos, C. Cornelius, D. Peebles, and D. Kotz, "Anonysense: Opportunistic and privacy-preserving context collection," in *Proceedings of the 6th International Conference on Pervasive Computing*, ser. Pervasive '08. Berlin, Heidelberg: Springer-Verlag, 2008, pp. 280–297. [Online]. Available: http://dx.doi.org/10.1007/978-3-540-79576-6_17

[87] L. Sweeney, "K-anonymity: A model for protecting privacy," *Int. J. Uncertain. Fuzziness Knowl.-Based Syst.*, vol. 10, no. 5, pp. 557–570, Oct. 2002. [Online]. Available: http://dx.doi.org/10.1142/S0218488502001648

[88] J. Sen, "Security and privacy challenges in cognitive wireless sensor networks," in *Book Chapter in Cognitive Radio Technology Applications for Wireless and Mobile Ad hoc Networks*. IGI-Global, 2013.

[89] Y. Ouyang, Z. Le, Y. Xu, N. Triandopoulos, S. Zhang, J. Ford, and F. Makedon, "Providing anonymity in wireless sensor networks," in *Pervasive Services, IEEE International Conference on*, 2007, pp. 145–148.

[90] S. Chakraborty, K. R. Raghavan, M. P. Johnson, and M. B. Srivastava, "A framework for context-aware privacy of sensor data on mobile systems," in *Proceedings of the 14th Workshop on Mobile Computing Systems and Applications*, ser. HotMobile '13. New York, NY, USA: ACM, 2013, pp. 11:1–11:6. [Online]. Available: http://doi.acm.org/10.1145/2444776.2444791

[91] M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," in *Proceedings of the 1st International Conference on Mobile Systems, Applications and Services*, ser. MobiSys '03. New York, NY, USA: ACM, 2003, pp. 31–42. [Online]. Available: http://doi.acm.org/10.1145/1066116.1189037

[92] C. Ozturk and Y. Zhang, "Source-location privacy in energy-constrained sensor network routing," in *In ACM SASN*, 2004, pp. 88–93.