A Survey of Potential Security Issues in Existing Wireless Sensor Network Protocols

Ivana Tomić and Julie A. McCann, *Member, IEEE*

***Abstract*—The increasing pervasiveness of Wireless Sensor Networks (WSNs) in diverse application domains including critical infrastructure systems, sets an extremely high security bar in the design of WSN systems to exploit their full benefits, increasing trust while avoiding loss. Nevertheless, a combination of resource restrictions and the physical exposure of sensor devices inevitably cause such networks to be vulnerable to security threats, both external and internal. While several researchers have provided a set of open problems and challenges in WSN security and privacy, there is a gap in the systematic study of the security implications arising from the nature of existing communication protocols in WSNs. Therefore, we have carried out a deep-dive into the main security mechanisms and their effects on the most popular protocols and standards used in WSN deployments i.e. IEEE 802.15.4, B-MAC, 6LoWPAN, RPL, BCP, CTP, and CoAP, where potential security threats and existing countermeasures are discussed at each layer of WSN stack. This work culminates in a deeper analysis of network layer attacks deployed against the RPL routing protocol. We quantify the impact of individual attacks on the performance of a network using the Cooja network simulator. Finally, we discuss new research opportunities in network layer security and how to use Cooja as a benchmark for developing new defenses for WSN systems.**

***Index Terms*—CPS, WSN, security, communication protocols, RPL, network layer attacks, Cooja.**

I. Introduction

TODAY, millions of embedded devices are used in diverse applications to enhance the way we work and live, by saving time and resources and opening new opportunities for growth and innovation [1]. The leading application domains include military and crime prevention, environment, industry and agriculture, and urbanization and infrastructure [2]. The synergy of cyber and physical worlds contribute to Cyber-Physical Systems (CPSs) which are expected to be applied to the crucial areas of national importance (e.g. health care, intelligent transportation, critical infrastructure monitoring and control) therefore they must operate dependably, safely, securely, efficiently and in real-time [3]. The existence of such a large network of interconnected entities poses major security and privacy issues that prevent its wide adoption. As these systems carry sensitive data, security issues should be central to their design; a well-defined security infrastructure that can mitigate the security challenges related to privacy, data integrity, and availability is an absolute requirement [4], [5].

Wireless Sensor Networks (WSNs) are considered as one of the core technologies in implementing CPSs. These are systems of low-cost, low-power, resource constrained devices with sensors and radio transceivers used for communication. WSN's intelligence and power lie in the sum of their parts, their network and interaction, yet communication is their greatest weakness, and many attacks exist to disrupt WSN services. Moreover, they are often deployed in publicly accessible environments. Once combined, the resource restrictions and the physical exposure of sensor devices makes conventional IT security methods inadequate. These fail to consider the numerous interactions among different components, the heterogeneity of the networks, the cyber-to-physical connections and the network's volatile and dynamical nature [6]. Also, they demand computational resources typically unavailable to such devices. New lightweight security mechanisms are needed and their complexity will vary depending on device specification, network technology, and type of application/service provided [7].

There have been several conducted studies and surveys (e.g. [8]–[13]) that have addressed the security aspects of IoT (Internet of Things) and WSNs. For instance, in [8]–[12] the main research challenges and the existing solutions in the field of IoT security are surveyed. The main thread of existing surveys is that they generally focus on identifying the security challenges and threats in IoT and WSNs, as well as give recommendations on how to build new security mechanisms. While we too present a taxonomy of attacks and their consequences on network performance to ensure a comprehensive, up-to-date list and also set up the stage for the further analysis, our survey takes a different direction.

The current paper focuses on looking in depth into existing communication protocols and standards to identify their security gaps. Compared to [13], rather than providing the research challenges and open research issues, we analyze the countermeasures available in the literature to ensure the protection of selected communication protocols from malicious activity. Our discussion is guided by the WSN protocol stack, but we also provide a categorization with respect to the attack they were built for, and we classify them into three groups: preventive solutions, intrusion detection schemes and reactive solutions. This way we measure their resilience towards attack scenarios. The identification of strong and weak features of the countermeasures leads to building more secure protocols for WSNs. Also, we quantify the impact of several network layer attacks on the network's performance using the Cooja simulation tool to show the potential of using Cooja as a benchmark for the development of new security mechanisms. Finally, we briefly highlight that providing a response system that is not only able to detect attackers, but also enables the network to recover from the intrusion and prevent any further disruptions of service is one of the potential research directions

The authors are with the Adaptive Emergent System Engineering Group, Department of Computing, Faculty of Engineering, Imperial College London, South Kensington Campus, London SW7 2AZ, UK
E-mail: i.tomic@imperial.ac.uk; j.mccann@imperial.ac.uk;

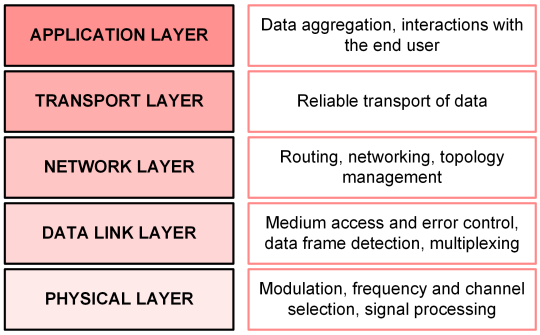

Fig. 1. WSN layered architecture

in the design of more secure WSN systems.

The rest of the paper is organized as follows. Sec. II discusses security requirements, vulnerabilities and mechanisms in WSNs. In Sec. III communication protocols used in WSN deployments are briefly described. In Sec. IV-VI we provide a systematic analysis of attacks and mechanisms for addressing them for each of the protocols presented in Sec. III. In Sec. VII we analyze the effects of network layer attacks on the RPL-based network using the Cooja network simulator. We discuss the opportunity of using the Cooja as a benchmark for developing new defenses. Finally, in Sec. VIII we conclude the article.

II. Security Features of WSNs

A WSN is an infrastructure-less network composed of hundreds of sensor nodes. These cooperatively sense and control the environment to enable its interaction with people or devices [14]. Data is captured at the level of the sensor node, compressed and transmitted to the gateway. Through the gateway connection, data is then passed by the base station to a server. WSNs typically employ layered architecture which typically consists of five layers. These are depicted in Fig. 1 with the problems addressed by each layer. There are several features which make WSNs different from wired networks and more vulnerable to security attacks. These are:

- *Self-organization* - Sensor networks have no fixed structure and positions of sensor nodes are random. Any failures in the network should be neutralized through the self-organizing mechanism to enable nodes to discover their neighbors and reestablish the communication [15].
- *Self-adaptive flow control* - Based on the quality of the link and the number of transmission errors, the transmission flow is adjusted to solve the network performance degradation in unstable transmission conditions [16].
- *Resource restrictions* - Limited processing abilities, storage capacity and communication bandwidth allow the use of a lightweight security mechanisms only, which can prevent most of external attacks, but provide no protection from internal attacks [7].
- *Centralized control* - Sensor nodes are centrally controlled and the data flows between nodes according to the rules of routing algorithm applied. Different routing protocols face different security challenges, but there is a commonality in the fact that most of them were developed without appropriate consideration of security.
- *Open environment* - WSNs are deployed in accessible environments which increases the probability of node capture by adversaries. Then, various internal attacks may be initiated by the compromised node and an adversary may overtake the complete control of network.

Overall, the aforementioned characteristics require the adoption of security mechanisms optimized for use in WSNs such that they provide a high level of efficiency and reliability. Next, we present an extensive, up-to-date list of security requirements and attacks in WSNs with respect to layered WSN architectures with the objective to exploit these in the communication protocols analysis in the further sections. We briefly introduce the notion of security mechanisms in WSNs also following the layered approach.

A. Security Requirements

Traditionally, confidentiality, integrity and availability were considered as security services which should be provided by sensor networks [17].

Confidentiality to ensure the secrecy of the data transmitted between sensor nodes by limiting the data access to intended users only. It is mainly based on the use of cryptographic techniques at physical layer, where data is encrypted at the sending node to prevent information disclosure to unauthorized users [17]. *Integrity* to assure that the data transmitted cannot be altered during transmission until it reaches its original destination. The data integrity may be breached by having a malicious node in the network. This can be solved through the utilization of the automatic code update and recovery process [18]. *Availability* to ensure that the network is able to provide services at any time for the authorized users. Various mechanisms are used to save energy and extend the life of network, but also to prevent denial of service. For example, the denial of service due to jamming is traditionally prevented by spread spectrum techniques.

As WSNs are expected to be integrated into the critical infrastructures where the sensitive data is exchanged and security needs are higher, the additional security requirements have to be defined. These can be grouped into three categories:

1) *Data level requirements*:

- Anonymity - Hiding the source of the data contributes to the information protection and confidentiality.
- Freshness - To guarantee that data is recent and not duplicated.

2) *Access level requirements*:

- Authentication - Verifying that the received message comes from a true sender.
- Authorization - Ensuring that only authorized users and devices have the access to the network.
- Accessibility - Ensuring that sensor nodes have the access to the authorized information only.

3) *Network level requirements*:

- Robustness/Resiliency - To guarantee that the network is able to function and serve the purpose if the number of nodes increases or in the case of some nodes getting compromised.

- Self-organization - Having the sensor nodes that are independent and flexible to self-organize in the case of any node failure or new nodes joining the network.
- Time synchronization - Can be required for different purposes, such as the power conservation, computation of the packet's end-to-end delay, the group synchronization for tracking applications, etc.

The complexity of a security framework will vary depending on the device specification, network technology, and type of application/service provided. Therefore, addressing the security requirements on multiple layers is needed. For example, if sensitive data is measured or shared by devices, the security requirements will be centered on data level requirements to ensure the data protection and confidentiality, but also on the access level requirements to control access to the resources.

B. Security Vulnerabilities

The wireless nature of communication, the lack of physical protection and the resource restrictions make WSNs susceptible to many attacks. In general, attacks can be classified as either *external* or *internal*. An external attacker does not have the control of nodes; it instead injects data or eavesdrops on information to disturb the normal network operation. Contrarily, an internal attacker is able to capture the sensor nodes which enables its further malicious activity. The boundary to divide the attacks as external or internal is not always easy, as they might have similar behavior. That is why most of the research on this topic provides vulnerabilities and security solutions appropriate to the individual layer in the architecture. Similarly, we give a taxonomy of attacks with respect to layered WSN architecture. For completeness, we include the attacks which can be launched against more than one layer of WSN. While we aim to cover the major attacks for WSN, less common attacks might be omitted and new security threats may arise over time due to the very nature of security.

1) *The physical layer* is the lowest layer in WSN protocol stack where the physical characteristics of signal transmission are specified. The broadcast nature of wireless communication makes it susceptible to jamming, eavesdropping, node tampering, and hardware hacking.

2) *The data link layer* enables nodes to access a shared medium and use it efficiently in order to regulate the data flow. It also deals with transmission errors. The most common attacks are related to MAC (Medium Access Control) sublayer of data link layer and these are: jamming and collisions.

3) *The network layer* provides data routing paths for network communication. A malicious node within the network can initiate a broad range of internal attacks, such as spoofing/replaying information, selective forwarding, blackhole, sinkhole, node replication attack, wormhole, and hello flood.

4) *The transport layer* is responsible for the reliable transport of data. During the transmission data can get compromised as well as the connection established between nodes due to a data integrity attack, energy drain attack, and desynchronization attack.

5) *The application layer* aggregates the data and interacts with the end user. It is mostly vulnerable to 'malware' attacks which can affect nodes or application programs such as attacks on reliability and the malicious code attack.

6) *Multi-layer attacks* can be initiated at different layers of the WSN protocol stack or can be developed as a combination of two or more of the previously defined attacks. These are denial of service (DoS) attacks and man in the middle attacks.

In Table I we give a description of all enlisted attacks, we classify them to internal or/and external and we give the consequences they have on the network's performance.

C. Security Mechanisms

WSN architectures use a range of communication protocols to satisfy the communication needs of diverse applications. Even though protocols utilize the limited capabilities of sensor nodes, the majority of them have not been designed with a security goal in mind. Security solutions can be developed at any of the layers of WSN stack as different types of applications may have different requirements. Security at lower layers (physical and MAC) is based on cryptography algorithms and key management mechanisms to ensure data protection and node authentication. Security at the network layer perform identity authentication and communication security through data encryption. Transport layer solutions use two-way authentication schemes aiming towards end-to-end security. However, this is usually maintained at the application layer which has the advantage of setting the security properties on a per-message basis. To have a complete security mechanism, the security of individual layers is absolutely necessary. If one layer gets compromised, the security of the whole network is compromised despite the efficient security mechanisms of the other layers.

A number of researchers have focused their work on designing protocols which support some of the security features. For completeness of the article, we list few examples. In [19], authors proposed two secure building blocks, SNEP and μTESLA, that are optimized for highly resource-constrained sensor networks and provide data confidentiality, two-party data authentication and data freshness. An extension of SNEP is known as TinySec [20] and it provides similar services, while being more efficient. In [21], authors presented LEAP, a symmetric cryptography based solution that proved very effective in defending against some of the network layer attacks. In [22], a link layer protocol LLSP was presented that achieves message integrity and authentication, while [23] describes a SIGF family of configurable secure routing protocols. None of these security measures does not guarantee a complete security solution as they were rather built as defense mechanism to a specific attack or to ensure a particular security requirement.

In this paper, rather than analyzing the features of secure protocols, we focus on the security mechanisms which were proposed in the literature for widely deployed and energy-efficient standards and protocols in WSNs. We categorize the mechanisms into three groups as:

- *Preventive solutions (PS)* that harden network protocols against specific attacks, but fail to address run-time security, they do not halt nor detect intruders nor ensure continued network functionality during an attack.

TABLE I
ATTACKS, THE EXTERNAL/INTERNAL ATTACK CLASSIFICATION AND THE CONSEQUENCES ON THE NETWORK'S PERFORMANCE

Attack	Layer	Type	Features of the attack	Consequences on network's performance
Eavesdropping	Physical	Ex	Overhear and intercept the data in the transmit coverage area of a node, without its knowledge.	Gaining access to the private and/or sensitive information.
Basic jammers	Physical	Ex	Intentional radio emission to prevent or disrupt the transmission of data.	Destroying the signal, causing the congestion and exhausting the nodes' energy.
Node tampering	Physical	Ex/In	Physical replacement of the entire node or its part.	Gaining access and altering sensitive information (e.g. routing tables, cryptographic keys).
Hardware hacking	Physical	Ex/In	Physical damage to nodes by the malicious entities.	Nodes can lose their expected functionality which makes them vulnerable to other risks.
Intelligent jamming	Data link	Ex	Data packets are targeted directly as the protocol rules or the data distribution are known.	Destroying the signal, causing the congestion and exhausting the nodes' energy.
Collision	Data link	In	Using the occupied radio channels will cause collisions with neighboring nodes.	Disrupting the transmission of data, increasing congestion and interference.
Spoofed/altered inf.	Network	Ex/In	Create non-existent information or partially modify data.	Attracting/repelling network traffic, creating routing loops.
Replay attack	Network	In	Repeating a valid data transmission.	Generating false error messages, disrupting the routes, increasing congestion and interference.
Selective forwarding	Network	In	Refusing to forward messages from selected nodes.	Reducing traffic and increasing data loss.
Blackhole	Network	In	Failing to forward any data packets received including its own data.	Reducing traffic and increasing data loss.
Sinkhole	Network	In	Advertising false information to create a center of attraction for other nodes.	Compromise of transmission routes, reducing traffic and increasing data loss.
Sybil attack	Network	In	Presenting multiple identities in the network.	Compromise of transmission routes.
Node replication	Network	Ex/In	Physical capturing of a node, its replication and deployment back into the network.	Compromise of transmission routes, eavesdropping on the falsely created links.
Wormhole	Network	In	Create a low link tunnel between two malicious nodes in different parts of network.	Sending data to the false destinations, undermining cryptography protection.
Hello flood	Network	Ex/In	Broadcasting a hello packet to the whole network with great transmission power.	Increasing energy degradation and collisions, creating false transmission routes.
Data integrity	Transport	In	Data compromising during the transmission by changing the content or injecting false messages.	Falsifying routing data can disrupt the networks normal operation.
Energy drain	Transport	Ex/In	Send as many connection establishment requests to a targeted node/nodes as possible.	Exhausting node resources, if many nodes are affected can lead to the denial of service.
Desynchron. attack	Transport	Ex/In	Forge messages between two nodes making the receiver node to request the retransmission of data so that synchronization is lost.	Unstable or broken communication links, compromise of transmission routes.
Attacks on reliability	Application	Ex/In	Insert the node on the path of communication to generate false data or queries.	Increasing energy degradation and collisions.
Malicious code attack	Application	Ex/In	Inject a "worm" that triggers the application to malfunction or overtakes the complete control of the application services.	Eliminates network's capacity to perform its expected function.
Denial of Service	Multi-Layer	Ex/In	A general attack that could include several other attacks happening simultaneously.	Eliminates network's capacity to perform its expected function.
Man in the middle	Multi-Layer	Ex/In	Sniff the network to intercept the communication between two sensor nodes during the exchange keys stage, without their knowledge.	Gaining access to the private and/or sensitive information.

- *Intrusion Detection Schemes (IDS)* can identify attacks at run-time, but cannot provide a response to the intrusion which would prevent any further disruptions of service.
- *Reactive solutions (RS)* feature in the IDS, but also the response system which enables the network to recover from the intrusion and prevent any further disruptions of service.

A brief protocol description is given next which is followed by an analysis of their security mechanisms in the subsequent sections.

III. WSN STANDARDS & PROTOCOLS

To understand the security requirements of selected protocols and standards, our discussion is guided by the protocol stack in Fig. 2. Compared to the architecture in Fig. 1, it has an additional adaptation layer to enable low-power sensor nodes to connect to the Internet. First, we consider the standards under the IETF standardization work. These can be layered one on top of another and are given in red. Additionally, a lightweight and energy-efficient MAC layer protocol, B-MAC is presented. It is one of the few specialized MAC protocols whose implementation was tested in hardware and it was used as a basis for the development of many other low-power MAC protocols. Also, we consider two collection routing protocols, BCP and CTP, which are used to gather data from multiple sources to a single or multiple sinks. BCP makes routing and forwarding decisions on a per-packet basis without routes establishment, while CTP is the tree-based protocol closely related to RPL. A brief description is given next which will be extended to their security analysis in subsequent sections.

Layers	Protocols
Transport/Application	CoAP
Network/Routing	RPL, BCP, CTP
Adaptation	6LoWPAN
MAC	IEEE 802.15.4.e, B-MAC
Physical	IEEE 802.15.4

Fig. 2. Communication standards & protocols with respect to the layered architecture of WSN

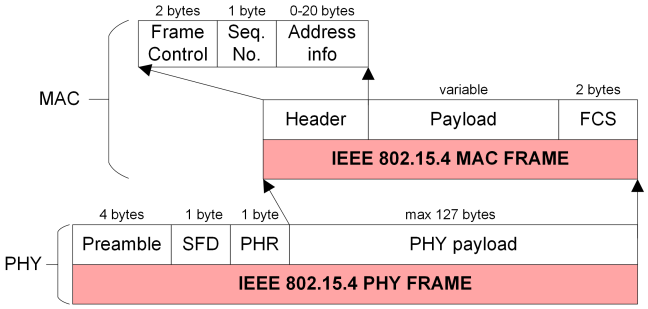

Fig. 3. Typicall IEEE 802.15.4 frame on a 2.4 GHz network

A. IEEE 802.15.4 for PHY and MAC Layer Communication

IEEE 802.15.4 [24] is a radio technology standard that defines both, PHY and MAC layers for low-power and low-data-rate communications. Due to its low power consumption, low cost, and flexibility, it has been used in many industrial applications [25], but also in other fields, such as health monitoring [26], smart home energy management system [27]. The original IEEE 802.15.4 standard from 2006 was amended throughout the years to IEEE 802.15.4.e version that is of particular interest for our discussion as it supports time-synchronized channel hopping communication. We discuss three versions of IEEE 802.15.4 standard, which are:

1) IEEE 802.15.4 PHY: The standard supports 11 channels in low-frequency band (868/915 MHz) and 16 channels in the high-frequency ISM (Industrial, Scientific and Medical) radio band (2.4 GHz). In order to achieve less interference along the frequency bands with an improved signal to noise ratio the standard employs different modulation techniques [13].

2) IEEE 802.15.4 MAC: The standard manages the access to physical channels and time slots, frame detection and node association and it uses CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) method. It has two channel access modes and it defines different types of devices, which provides possibility of having different network topologies (star, peer-to-peer, cluster) [28].

3) IEEE 802.15.4.e MAC: The revised version of IEEE 802.15.4 MAC supports multi-hop communications by employing Time Synchronized Mesh Protocol (TSMP). Devices are synchronized to a schedule which indicates to which neighbor to communicate and on which channel.

Fig. 3 depicts the IEEE 802.15.4 frame structure. The PHY frame contains a synchronization header which consists of a preamble, the Start of Frame Delimiter (SFD) to indicate the start of an arriving packet, and the PHY Header (PHR) to indicate the length of the payload. These are followed by the payload of fixed size of 127 bytes. The MAC frame includes the header (control field, sequence number and address), payload of the variable size and Frame Check Sequence (FCS) used to verify the integrity of the frame. The whole MAC frame size has to be less than 127 bytes to satisfy the size constraint of the physical layer.

B. B-MAC (Berkeley Media Access Control for Low-Power Sensor Networks)

B-MAC [29] belongs to the category of energy-efficient protocols where the energy spent on idle listening is reduced by using some form of a sleep/listen schedule. The protocol uses random access to the communication medium, which means that there are no slots or frames to send the data, but these can be added if there is a need [30]. As the sending and receiving nodes are not synchronized, the transmitter has to transmit a preamble that is long enough to be detected by the receiver which only wakes up periodically (LPL - low-power listening). When a node overhears the preamble, it remains awake to receive the data packet that follows. The behavior of B-MAC sender and receiver is depicted in Fig. 4. The check interval between two channel sensing is defined based on the average node degree and traffic levels [29]. The duration of preamble might be changed depending on the application requirements. In [29], authors showed that B-MAC could achieve duty cycles as low as 1% in a low-traffic network if ideal conditions were assumed. The main disadvantage of the protocol is a large overhead caused by the preamble.

C. 6LoWPAN (IPv6 over Low-power Wireless Personal Area Networks)

6LoWPAN is a network protocol responsible for universal Internet connectivity that enables low-power wireless nodes to connect to the Internet. It can be considered as a key technology that changed a previous perception of IPv6 as being impractical for a use in constrained low-energy wireless communication environments [13]. 6LoWPAN defines the communication on often-called adaptation layer for transmitting IPv6 over IEEE 802.15.4 networks [31]. The adaptation layer fragments the IPv6 packets into smaller pieces, as minimum size of IPv6 packet is 1280 bytes and IEEE 802.15.4 supports 127 bytes long packets. Also, it provides the header compression to optimize the usage of the limited payload space and to ensure that it can be supported by the lower layers [32]. All 6LoWPAN packets transported over the IEEE 802.15.4 MAC layer include a stack of 6LoWPAN headers which use is optional [13]. The protocol supports multihop communication where the nodes can forward packets on each other's behalf. The biggest challenge for 6LoWPAN protocol was to provide a routing solution that supports different communication patterns and deals with limited resources, low-data rates, link failures, and nodes mobility which lead to a new routing protocol, RPL.

D. RPL (Routing Protocol for Low-power and Lossy Networks)

RPL [33] is a distance-vector routing protocol which supports a variety of link layer technologies (IEEE 802.15.4,

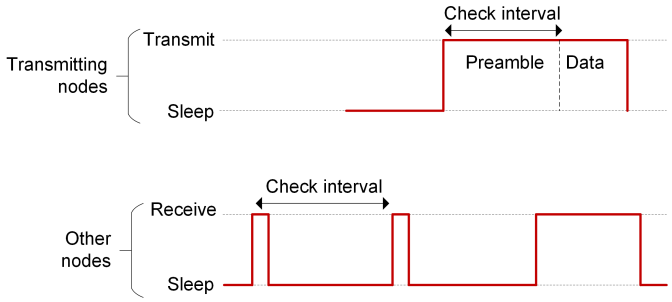

Fig. 4. B-MAC transmitter and receiver behaviour

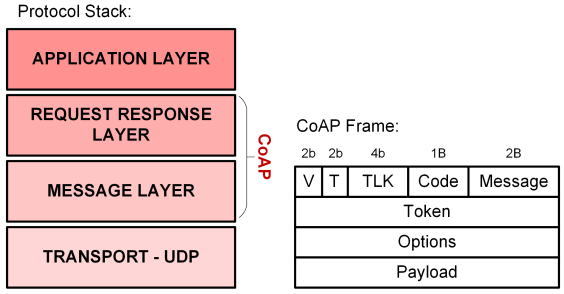

Fig. 5. CoAP protocol stack, message and header format

Wireless HART, ISA100 etc.), sharing the common characteristics of being low bandwidth, lossy and low power. As such, RPL is widely used in WSNs [31]. It defines two types of components: WSN nodes, acting as hosts or intermediate routers, and local border routers (LBRs) responsible for packet translation from the Internet to hosts [32]. By exchanging the node/link metrics, RPL builds a Destination Oriented Directed Acyclic Graph (DODAG) where usually LBRs are roots. The topology is rank metric depended, where the rank metric encodes the distance of each node from a reference root which has rank 1. The best path is computed based on an objective function which, by default, uses a number of hops as the routing metric. Additional metrics could be specified, such as the node energy consumption or the expected number of transmissions (ETX). RPL protocol can support MP2P (Multipoint-to-Point), P2MP (Point-to-Multipoint) and P2P (Point-to-Point) topologies. The topology maintenance and information exchange is supported by four types of control messages: DIO (DODAG Information Object), DAO (Destination Advertisement Object), DIS (DODAG Information Solicitation) and DAO-ACK. RPL has a mechanism for loop prevention and detection. Also, it provides a self-healing through a local or a global repair mechanism in the events of link/node failure or divergence from the optimal network shape.

E. BCP (Backpressure Collection Protocol)

BCP [34] is a low-overhead protocol which was evaluated in real experiments. It is based on the concept of dynamic backpressure routing where there is no explicit path computation between source and destination (i.e. 'routing without routes'). The routing and forwarding paths are chosen based on the link backpressure weight which is a function of the queue and link state information. If the forwarding queue is non-empty, node computes weights for all of its neighbors. If no neighbor with positive weight can be identified, the node waits for a back-off period to recompute the weights. Upon detecting one or more neighbor with positive weights, the node forwards packet to the neighbor with the greatest positive weight. Routing decisions are made separately on a per packet basis [35]. One of the key features of BCP is the last-in-first-out (LIFO) queuing discipline of packets in each node, which decreases the end-to-end packet delay. The LIFO queue is implemented through the notion of virtual queue, which stores no real data and requires only an integer size [34]. If forwarding queue is full and new data arrives, the oldest packet is discarded while the virtual queue is incremented. On the other end, if the data queue is found to be empty, a null packet is forwarded and the virtual queue is decremented. This ensures scalability with a large number of nodes.

F. CTP (Collection Tree Protocol)

CTP [36] is a simple tree-based routing protocol designed for relatively low traffic rates providing many-to-one or one-to-many communication. CTP is a best-effort protocol that does not guarantee 100% reliable delivery. Also, it is address-free and the routes to tree roots are generated by using the expected transmissions (ETX). A single root is allowed which has ETX of 0, while a node's ETX is a sum of the ETX of its parent and the ETX of its link to the parent. If several routes are valid, the route with minimum ETX will be chosen for transmission. Routes are not updated periodically, only when inconsistency in the topology is detected [37]. A loop may occur if node chooses a route with significantly higher gradient value compared to the previous value. This problem is addressed through the broadcast of a beacon frame so that node which sent the data can adjust its routes. Optionally, the routes with ETX higher than the predefined threshold value can be taken out of consideration [36]. The protocol provides a mechanism for avoiding the packet duplication.

G. CoAP (Constrained Application Protocol)

CoAP [38] supports application-layer communication and it has been developed for web transfer within the IoT. Similarly to the Hypertext Transfer Protocol (HTTP), CoAP depends on the representational state transfer (REST) architecture which is embedded in User Datagram Protocol (UDP) for transactions in the 6LoWPAN environments. Opposite to HTTP, which is relatively expensive both in the implementation and code space, CoAP uses very limited resources and with reduced complexity provides the same set of services [38]. The CoAP architecture is split into two layers, message layer and request response layer, which are shown in Fig. 5. The CoAP message starts with a 4-byte fixed header which consists of the version field (V), the message type field (T), the token length field (TKL), the code field and the Message ID. The messages are exchanged asynchronously between two endpoints which is provided through a lightweight reliability mechanism which supports different types of messages: confirmable (CON), non-confirmable (NON), acknowledgement (ACK) and reset (RST)

TABLE II
IEEE 802.15.4 SECURITY SUITES

Security Suite Name	Access Control	Data Encryp.	Frame Integ.	Sequen. Fresh.
None				
AES-CTR	✓	✓		✓
AES-CBC-MAC-128	✓		✓	
AES-CBC-MAC-64	✓		✓	
AES-CBC-MAC-32	✓		✓	
AES-CCM-128	✓	✓	✓	✓
AES-CCM-64	✓	✓	✓	✓
AES-CCM-32	✓	✓	✓	✓

[13]. The request response layer deals with the arrival of messages that are out of order, lost or duplicated.

IV. ATTACKS & SECURITY MECHANISMS FOR PHY AND MAC LAYER COMMUNICATION PROTOCOLS

A. Security & Attacks in IEEE 802.15.4

The security mechanism for IEEE 802.15.4 is implemented only in the MAC layer with the choice of operating in either secured or non-secured mode. The secured mode satisfies four security requirements: access control, data encryption, frame integrity, and sequential freshness [39] which are supported through various security suites. The security suites are using the symmetric cryptography and Advanced Encryption Standard (AES) [13] and they can work in different modes of operation: the counter mode (CTR), the cipher block chaining with message authentication mode (CBC-MAC), or the authenticate-and-encrypt block cipher mode (CCM). Most of them support the message integrity codes (MIC) of a different length (32, 64 or 128 bits) [39]. Table II indicates the security services supported by each suite. The standard does not specify how the keys should be managed or what kind of authentication policies should be used, so this should be addressed by the upper layers of the protocol stack.

Despite the possibility of having secure modes, due to the operating rules and a limited number of communication channels, the standard is susceptible to several basic attacks. These are mainly based on jamming techniques which can lead to more serious DoS and man in the middle attack. The work in [40] showed that the additional security towards sweep and reactive jamming could be provided by the IEEE 802.15.4.e amendment with channel hopping. Also, authors proposed data encryption to prevent data denial. If an attacker corrupts PHR, the time of FCS can be predicted so that the frame is jammed. However, as the encryption covers only MAC payload, an adversary might be able to read the 802.15.4 MAC header and decide on taking an action which can seriously affect the network. For example, if an adversary changes the frame counter or injects false data, that frame will be finally rejected, but it will waste some energy [40]. An additional threat to IEEE 802.25.4 comes from the fact that there is no integrity protection provided on ACK frames, so the eavesdropper can forge the ACK frame and fool the sender of the successful reception of the frame. This could be addressed by using a form of authentication; however the overhead and delays in the network would increase [39].

B. Security & Attacks in B-MAC

To this end, no security mechanism has been defined in the context of B-MAC protocol. B-MAC, but also the other protocols on MAC layer, are vulnerable mostly to jamming and collisions while operating. Due to the use of adaptive thresholding, B-MAC provides some level of immunity against certain type of constant jammers. In the case of the static jammer transmitting at a constant power, and the static node, it is less probable that a jammer will not be detected. The periodical jamming is also not considered as a serious threat to B-MAC, as the protocol uses a periodic cycle only for listening, and not sending. If an attacker wants to perform a jamming attack on B-MAC that uses periodic listening cycles, a preamble interval has to be determined. This is known as a statistical jamming attack based on the probability estimation of packet inter-arrival times [30]. If an adversary chooses to guess, more frequent sampling is needed which reduces the efficiency of jammer. In [41], authors modeled several denial-of-sleep attacks that can severely disrupt the service by knowing a protocol. An additional threat would be if an attacker penetrates link-layer encryption; the network's lifetime could reduce from several months to only few days.

C. Summary

In the context of the IEEE 802.15.4 PHY protocol, existing AES/CCM hardware encryption provides an efficient cryptographic basis which can be reused by the upper layers. However, the keying model should be precisely defined to avoid the danger of different entities using the same key. Additionally, the fact that header and ACK frames are not encrypted could be exploited to perform simple attacks that could lead to an increase in energy consumption or more seriously to DoS. When it comes to the MAC layer protocols, more sophisticated jammers can be considered as a major treat as there is no adequate protection. Table III summarizes all attacks against the IEEE 802.15.4 and B-MAC protocols and countermeasures that exist in the literature. We also comment on the main advantages/disadvantages of the proposed security mechanisms and their type.

V. ATTACKS & SECURITY MECHANISMS FOR ADAPTATION AND NETWORK LAYER COMMUNICATION PROTOCOLS

A. Security & Attacks in 6LoWPAN

No security mechanism has been adopted in the context of 6LoWPAN protocol. The threats to 6LoWPAN are emerging from 802.15.4 and IP networks, but the most severe ones are the consequence of the attacks on the network layer which is usually represented by RPL. The main security threat arising from the adaptation layer itself is a fragmentation attack where changing the packet fragmentation fields could lead to a replay attack that causes the overflowing at receiver side or complete denial of service. This is due to the lack of node authentication when joining the network. In [42], authors proposed new packet format where Timestamp and Nonce options are added to the fragmented packets to guarantee packet freshness. Two additional security schemes to

TABLE III
SUMMARY OF ATTACKS AGAINST IEEE 802.15.4 AND B-MAC AND EXISTING COUNTERMEASURES

Protocol	Relevant Attack	Proposed Countermeasure	Type	Comments
IEEE 802.15.4	Sweep and reactive jamming	IEEE 802.15.4e amendment [40]	PS	Adds secured ACKs and channel hopping; However, it does not ensure defence under wide-band jamming;
	Eavesdropping and forging ACK frame	MIC (Message Integrity Code) [39]	PS	The form of authentication through MIC is supported by built-in AES-CBC-MAC suits; It increases the overhead, and the delay of transmitting a frame;
	Denying data through MAC and PHY header	Encrypting the data payload [40]	PS	It covers only the MAC payload, not headers; By corrupting FCS only, data can be denied or it can lead to waste in energy;
B-MAC	Statistical jamming	Shortening the preamble size [30]	PS	Shortening the preamble (that B-MAC relies on) too much defeats its purpose;
	Denial of sleep attack	Link-layer authentic., anti-replay protection, jamm. identif. & mitigation, broadcast attack defense [41]	PS	There is no energy efficient attack against B-MAC which means that the attacker is awake most of the time. However, this framework has not been simulated/tested;

prevent fragmentation attacks were proposed in [43]. In the content chaining scheme receiving node uses cryptographic mechanisms to verify that received fragments belong to the same packet, while the split buffer approach promotes direct competition between legitimate nodes and an attacker in using deficient buffer resources. The authentication can be ensured by employing network access control framework described in [44].

The 6LoWPAN does not ensure end-to-end protection between an IP sensor node and the Internet which makes it vulnerable to eavesdropping/spoofing and man in the middle attacks. These can be prevented by IPsec which defines a set of protocols to enable the authentication and encryption of each IP packet at the network layer [45]. The most common attack in the category of threats arising from the Internet is the botnet attack where data is forged by the botnet network and the wrong data is sent to the user node. In [46], authors proposed an additional module in 6LoWPAN gateway that analyses data passing though the gateway searching for malicious traffic. The security treats to the 6LoWPAN arising from the RPL routing protocol will be discussed next.

B. Security & Attacks in RPL

RPL protocol was designed to support confidentiality, integrity, availability, and non-repudiation [47]. The current specification defines three basic security modes [13]:

1) *Unsecured mode* - The default mode where no security mechanism is applied to routing, but it supports a link-layer security or other mechanisms used by the network.
2) *Preinstalled mode* - Supports confidentiality, integrity and data authentication based on the use of secure messages and a preconfigured symmetric key. A node may join the RPL network either as a host or as a router.
3) *Authenticated mode* - Nodes which have a preconfigured symmetric key can join the network as hosts only. The routers have to obtain a second key from a key authority which ensures the authentication and the authorization and provides per hop message security between two neighboring nodes.

Despite the specification, none of the RPL security modes have been implemented yet. This makes the RPL prone to the most of internal network layer attacks In Table IV which could severely impact the data routing. However, there is a decent amount of literature on the security mechanisms against internal attacks which are given next.

In [48], authors proposed a lightweight heartbeat protocol to detect faults within the RPL-based network. It was shown that if combined with IPsec [49], the heartbeat protocol can be used to detect selective forwarding attack. In [50], an intrusion detection system has been used to detect spoofed or altered information, sinkhole, and selective forwarding. Selective forwarding attack has been also addressed by using resilient techniques, such as random routes and data replication [51], while the mechanisms for detecting sinkholes were given in [50], [52], and [53]. Hello flood attack cannot exist for a long time within the RPL network due to the self-healing mechanism. However, if combined with some other internal attack the adequate protection will be needed [20]. Wormhole attack can be prevented by using a Merkel tree authentication [54] or separate link-layer keys for different segments of the network [48]. Additionally, in [55] the authors proposed a graph theoretic approach. Sybil attack and clone ID are usually prevented by keeping the track of the number of instances of each identity and by using the geographical location of nodes [48], [56].

The additional attacks on the RPL might arise from its operating rules in optimizing network performance. Examples are DAG/DAO inconsistency attack and rank attack. In the DAG/DAO inconsistency attack an adversary modifies the flags used to detect inconsistencies in the network. As a result the targeted node will discard the packet and reset the trickle timer; hence, the control messages will be sent more frequently which will waste energy and increase delay. In [57], authors proposed to limit the rate of tickle timer resets to 20, while in [58] and [59] two methods, adaptive threshold and dynamic approach, were used. On the other side, in the case of rank attack an adversary can attract the large traffic by advertising false rank value, so non-optimal routes might be established. Solutions to address this problem are given in [60] and [61].

C. Security & Attacks in BCP

As it is primarily academic routing protocol, no security mechanism has been adopted for BCP. The main threat comes from internal attacks where for example, a malicious node can

TABLE IV
SUMMARY OF ATTACKS AGAINST 6LOWPAN, RPL, BCP, AND CTP AND EXISTING COUNTERMEASURES

Protocol	Relevant Attack	Proposed Countermeasure	Type	Comments
6LoWPAN	Fragmentation attack	Timestamp for undirectional and Nonce for bidirectional fragmented packets [42]	PS	Fragmented packet formats have to be redefined; The framework has not been simulated/tested;
		The content chaining scheme and the split buffer approach [43]	PS	The attack is mitigated at moderate memory & computational cost with the increased overhead.
	Authentication attack	Network access control framework [44]	PS	Provides the node identification, but only enables one border router; Not implemented yet;
	Man in the middle, Eavesdropping/spoofing	IPsec (AH and EPS) [45]	PS	Provides end-to-end secure communication; Pre-shared keys mechanism is not very flexible;
	Botnet attack	Bot analysis module [46]	IDS	Good detection rates for large number of nodes; Decreased network performance and large overhead;
RPL	Selective forwarding attack	Lightweight Heartbeat [48]	IDS	It has to be combined with IPsec to detect attack; No defense is provided after the attack is detected;
		Resilient techniques [51]	PS	Improved delivery ratio, but an increase in energy consumption;
	Spoofed/altered inf., sinkhole, selective forwarding	SVELTE [50]	IDS	SVELTEs overhead is small enough; The true positive rate is not 100% due to some false alarms;
	Sinkhole attack	IDS solution [52]	IDS	IPsec and bidirectional communication are necessary.
		Parent fail-over & rank authentication [53]	PS	Combination of both techniques is more effective; Dense networks can combat penetration of sinkholes;
	Wormhole attack	Separate keys for network segments [48]	PS	The solution was not implemented/simulated yet;
		Merkel trees authentication [54]	PS	Node uses a key to encrypt its messages; High jitter and E2E delay until tree has been established;
		Graph theoretic approach [55]	PS	Cryptographic techniques based on local broadcast keys; Low overhead, no synchronization needed;
	Sybil attack, Clone ID	Distributed hash tables (DHT) to store the graphical location of nodes [48], [56]	PS	Problem in how to securely verify the node location; Might not scale well with large networks;
	DAG/DAO inconsistency attack	Limit the rate of tickle timer resets [57]	PS	Threshold value is fixed, no network or node characteristics are taken into account;
		Adaptive threshold [58]	PS	Takes into account the network characteristics;
		Dynamic approach [59]	PS	Improved version as node specific parameters are used;
	Rank attack	VeRa [60]	PS	Authentication mechanism based on hash operations; Low time overhead, but still vulnerable to rank attacks by forgery and replay;
		TRAIL [61]	PS	Improvement of VeRa, requires almost no cryptography, but shows dependency on network sizes;
BCP	Blackhole attack, header/data modif., false routes/queue info.	VAR trust model [35]	IDS	Performance is verified in TinyOS over a 25-node sensor network test-bed; Increased overhead;
	Blackhole, sel. forwarding, on-off and multiple attacks	Virtual trust queuing [62]	RS	The solution sustains the throughput performance under attack; Problems with detecting low rate attacks;
CTP	Sinkhole attack which can lead to other internal attacks	Intrusion detection system based on link quality [63]	IDS	Low rates of false positive, but increased energy consumption; Suitable for large-scale networks;
	N/A	Secure CTP protocol [37]	PS	Provides authentication, integrity and freshness; No implementation with an adversary was provided.
	Data loss, data alteration, sinkhole and selective forwarding	Kinesis [64]	RS	Automated response system to both, attacks and anomalies; The hidden node problem and partitioning of the neighborhood introduce redundant actions.

choose to selectively forward data or drop all received packets. In both scenarios the network operation would be disturbed. Also, by modifying the message header or data itself, the integrity within the network would be affected. Additional threats may arise from BCP operating rules. A malicious node can advertise the false queue size and link quality to either attract or repel any incoming traffic. Also, a node may ignore the information advertised by its neighbors and decide to send packets to highly congested areas.

In [35], the authors presented a trust model for WSNs that work with dynamic backpressure routing. They introduced different trust metrics to monitor the successful forwarding of data packets, as well as the queue size advertisements. The model was implemented in TinyOS in the presence of no forwarding nodes, in the case of header/data modification attacks, misleading routes and false queue information. In [62], authors proposed a virtual trust queuing scheme whereby jointly stabilizing the virtual trust queue and the real packet queue, BCP achieves guarantees of attack resilience as well as throughput performance.

D. Security & Attacks in CTP

CTP does not provide any security measures as it was designed to ensure minimum power consumption. The routes are chosen spontaneously based on the link quality; hence, it can not resist any intrusion. In [63], authors identified the sinkhole attack as a major treat to CTP routing that can initiate other attacks, such as selective forwarding, black holes,

data tampering, etc. They proposed the sinkhole detection approach based on link quality which is characterized by a low rate of false positives and a low energy consumption. Additionally, by changing the CTP operating rules a number of attacks can be launched. For example, a node can advertise false value of ETX which could lead to the presence of loops and inconsistencies within the network. This would increase the number of beacon frames sent in order to adjust the routes, as well as the energy consumption. In [37] the secure version of CPT is given which fulfills the essential security requirements: authentication, integrity and freshness. It is shown that adding security does not necessarily mean an increase in power consumption; however, the network performance was not simulated in the presence of an adversary. In [64], the authors presented Kinesis, an automated response system to both attacks and anomalies. Upon being notified of an incident via the detection scheme, the system matches the appropriate response policy to specify the action.

E. Summary

It can be concluded that network layer protocols are more prone to internal than external attacks. Having a malicious node in the network has to be considered as a serious threat and adequate techniques to detect and mitigate the attack have to be identified. Table IV summarizes all threats against selected network layer communication protocols. We also give the existing countermeasures proposed in the literature describing their main characteristics and the type. The analysis shows that detecting the intrusion only does not give any guarantees of protecting the network at run-time and that more automated solutions are needed.

VI. Attacks & Security Mechanisms for CoAP Application Layer Communication Protocol

The initial version of CoAP had no security features. However, the research community proposed DTLS (Datagram Transport Layer Security) protocol [65] to secure CoAP messages and deal with the unreliable nature of UDP communication. The DTLS guarantees confidentiality, authentication, integrity and non-repudiation. It can support four security modes:

- NoSEc - DTLS is not used.
- PreSharedKey - DTLS is used and a list of predistributed symmetric keys is provided. Nodes which share the same key are authenticated as a part of the group.
- RawPublicKey - DTLS is used and the nodes are provided with a pair of asymmetric keys which are installed on a node in the manufacturing phase.
- Certificate - It's an extension of the RawPublicKey mode where certificate is provided by a certification authority. A list of trusted anchors which can be used to verify the certificates is given to the nodes.

The DTLS consists of two layers. The bottom layer provides a symmetric key encryption, while at the upper layer the 'handshake' process establishes a session key and sets the security settings, so that the data can be carried inside a ciphered message. The main drawback of DTLS is that it does not support multicast communications, which will be required in many IoT environments. The handshake phase is considered as challenging due to its complexity and large number of messages exchanged. If there is a breach in the security within the handshake process it could lead to an exhaustion attack. Also, the handshake messages are too large which causes the fragmentation at 6LoWPAN adaptation layer, so the cost of their computation at the end of handshake process is high [13]. The DLTS provides protection against a replay attack, but even if dropped in the end, packets still need to be processed which increases the energy consumption. It also assumes a large buffer to store all messages which is not applicable to constrained networks. Additionally, while CoAP inquires 2 transactions per transmission, if DTLS is used 4 transactions are needed. All of this implies that an adequate trade-off between security and a lightweight implementation of DTLS has to be provided. In [66], two compression schemes for DLTS were proposed to provide compression of handshake and application data messages which is around 36% of the header length. In [67], a lightweight solution was presented which reduces the number of requests to perform the session and is robust to replay attack, DoS and chosen cipher text.

To summarize, there is a broad range of areas where the DTLS as the CoAP's security mechanism is still lacking. When it comes to its deployment with the constrained devices in IoT the trade-off between security and the overhead has to be taken into account as well as the multicast nature of the IoT environments.

VII. Security Attacks Evaluation in Cooja

Owing to their operating nature, WSN are typically prone to the wide range of attacks discussed in Section II-B. The fact that nodes are deployed in accessible environments raises the danger of their physical capture. Additionally, new malicious node can join the network freely if no authentication technique has been implemented. Understanding the impact and consequences of an attack to the network's performance helps to prevent possible denial of service. Therefore, fast and accurate simulations of WSNs in the presence of an adversary are of the great value in designing resilient, but also secure sensor networks. In [68], authors surveyed most popular network simulators. What is common for all of them is that they lack an unified security module. Rather than proposing a new simulation tool to address security needs, we wish to exploit the features of Contiki's network simulator/emulator Cooja [69]. As Cooja is very popular within the WSN research community, our aim is to examine the possibility of using it as a benchmark for quantifying the impact of attacks and for developing new countermeasures. As an example of how this can be used we analyze the effect that internal attacks have on the performance of RPL-based networks.

Network and threat model. We consider a WSN that has $\mathcal{N} = \mathcal{S} \cup \mathcal{R}$ devices communicating in a multi-hop fashion. $\mathcal{S}$ is the set of all sensor nodes that generate and send data packets, while $\mathcal{R}$ is the set of all roots that collect data packets from the network. We define $\mathcal{N}_x(t) \subseteq \mathcal{N}$ to be the set of one-hop neighbors that node $x \in \mathcal{N}$ can communicate with during

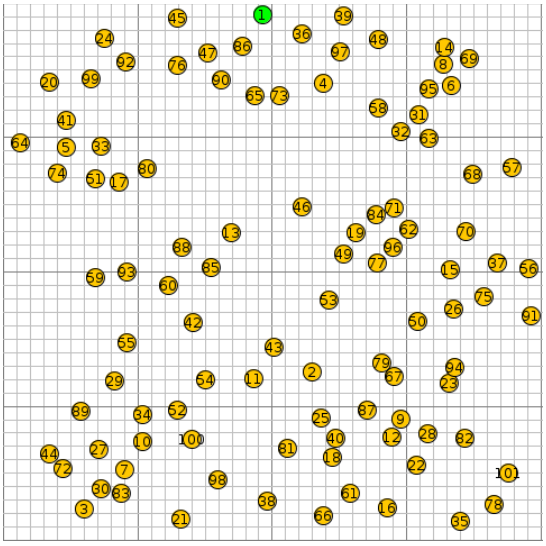

Fig. 6. Simulation environment

time slot t, where $t \in \{1, 2, \ldots, t_f\}$, $t_f < \infty$. The network is modeled as time-variant weighted graph $G(\mathcal{N}, \mathcal{L})$ where $\mathcal{L}$ consists of all possible wireless links for the node pairs $x, y \in \mathcal{N}$. The entry $(x, y) \in \mathcal{L}$ represents the communication link between the source node x and the destination node y. Assuming the standard layered infrastructure of WSNs, we address the attacks specific to the network layer which are: blackhole, hello flood, replay attack, selective forwarding, sinkhole and sybil attack. Also, we consider the effect of having multiple attackers in the network.

Implementation of attacks. At time t each malicious node $x_m \in \mathcal{N}$ is able to perform one of the attacks given below:

1) *Blackhole attack* where the node x_m fails to forward any data packets received from its one-hop neighbors $y \in \mathcal{N}_{x_m(t)}$.
2) *Hello flood attack* where the node x_m broadcasts a hello packet every 20ms in order to cause collisions and jam its one-hope neighborhood.
3) *Replay attack* where the node x_m overhears the traffic of its one-hop neighbors $y \in \mathcal{N}_{x_m(t)}$. Any packets overheard during the neighbors' transmissions are then replayed.
4) *Selective forwarding attack* where the node x_m fails to forward data packets received from two of his neighbors. The set of affected neighbors changes every 60s.
5) *Sinkhole attack* where the node x_m advertises falsely that it's a sink (i.e. $Rank_{x_m}(t) = 1$).
6) *Sybil attack* where the node x_m replicates identity of one of its neighbors $y \in \mathcal{N}_{x_m(t)}$. By having the same ID any data packets sent to y will be also passed to x_m.

Evaluation of the attacks. This stage evaluates the impact of each attack on the network performance. Two types of experiments have been performed on a random network topology using the Cooja network simulator. The network topology is depicted in Fig. 6, while the simulation parameters are given in Table V. First scenario is free from any malicious activity and will be used as a benchmark for evaluating the effects of the attacks. The second scenario replicates the malicious activity, where a malicious node can perform one of the six attacks defined previously. Additionally, we consider the effect of having more than one malicious node in the network. The position of malicious node has been chosen such that the impact to the network performance is ensured (e.g. as leaf nodes are not doing any forwarding tasks and cannot cause the data loss, they are taken out from the consideration).

TABLE V
SUMMARY OF SIMULATION PARAMETERS

Parameter	Value
Simulator	Cooja under Contiki 3.0 OS
Radio environment	Unit disk graph medium (UDGM): dist. loss
Deployment area	400m × 400m
Type & no. of nodes	Cooja mote, 100 senders & 1 sink
Range of nodes	Trans. range: 50m, Interference range: 50m
Physical layer	IEEE 802.15.4
MAC layer	ContikiMAC, IPv6
Network Layer	ContikiRPL
Transport Layer	UDP
Simulation duration	4h
Sending rate	1 packet in every 10 sec

To gain an insight concerning the performance of RPL in the presence of a malicious node we use the following metrics:

1) *Packet Delivery Ratio (PDR)* - PDR represents the ratio between the total number of packets successfully received by the sink and the number of packets sent by the nodes.
2) *End-to-End (E2E) Delay* - E2E delay represents the average time needed for a packet to travel between the source and the destination (sink).

The objective of these simulations is to show how the Cooja simulation tool can estimate the attack impact (in terms of previous metrics) on the network. The results are depicted in Fig. 7. As it can be observed, the attacks can be grouped into three categories as follows: 1) attacks that reduce both, PDR and E2E delay, as the malicious nodes drop data which allows faster delivery of unaffected packets in the network (selective forwarding, blackhole, sinkhole), 2) attacks that reduce PDR, but increase E2E delay due to an increase in the total number of packets in the network (replay attack, hello flood attack) and 3) attacks that do not affect any of the metrics drastically (sybil attack) as some additional metrics might be needed (e.g per node/per packet E2E delay).

Recommendations for using Cooja in designing countermeasures. In this section, we showed that WSN attacks can severely disrupt normal network operation. By extending the features of Cooja we were able to measure and quantify this disruption in a convenient way. The understanding of the impact and behavior will be necessary when protecting the network. Here, in the simulation scenarios, we explored two different metrics. However, there are many others to be tested. For example, if there was a new countermeasure to be implemented its energy overhead could be easily identified through the Powertrace tool in Cooja [70], as well as its resilience towards built-in attacks. This will allow us to test the countermeasure before actual deployment. Therefore, it would be of great interest to the research community to have access to a security module within the Cooja, such as one developed

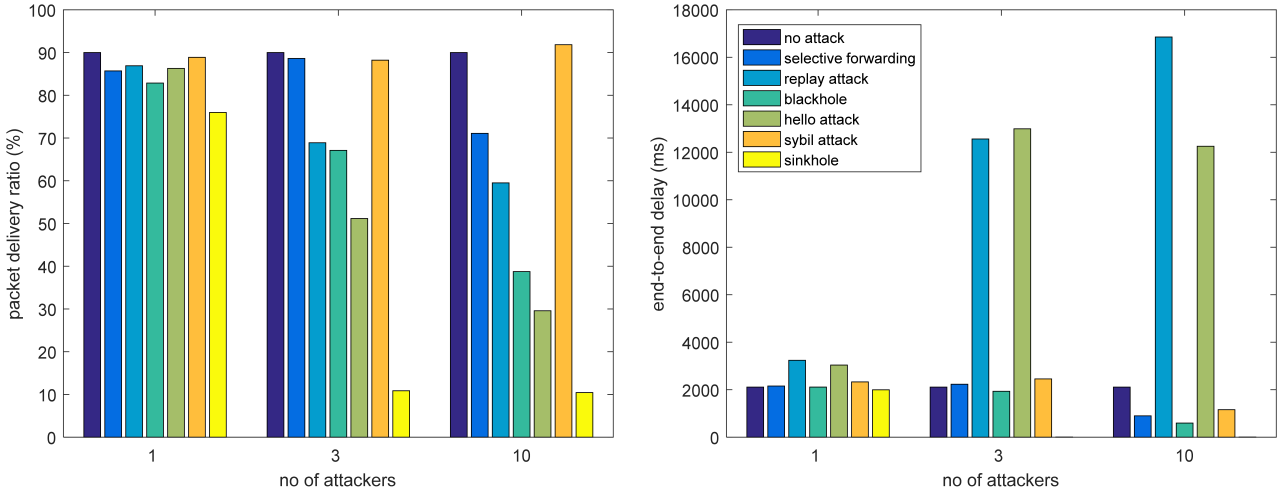

Fig. 7. PDR and E2E delay of the network in the presence of a malicious node/malicious nodes performing different network layer attacks

here, which replicates the most common and most destructive attacks on the WSNs. This would serve as a benchmark to develop and test new security mechanisms which would contribute to faster developments in this research area.

VIII. Conclusion

In this survey we perform an exhaustive analysis on the security of widely deployed communication protocols and standards in WSNs. We show that most of the security solutions in the area are still at a proof-of-concept level and there is a trade-off between the level of security required for a specific application and the overhead in the security mechanism. Also, there is a tendency towards solutions that can detect the intrusion, but also provide an automated response to ensure network's normal operation. Additionally, we give a small-scale example of our security module in Cooja that allows the evaluation of the network's performance in the presence of malicious activity. We believe that this is a step closer to using Cooja as a benchmark for developing new security defenses for the most popular communication protocols.

Acknowledgment

This work has been funded by the UK EPSRC as part of the PETRAS IoT Research Hub - Cybersecurity of the Internet of Things grant no. EP/N023242/1, project IoT in the Park.

References

[1] J. A. Stankovic, Research Directions for the Internet of Things, *IEEE Int. of Things J.*, 1(1), 3–9, 2014.

[2] P. Rawat, K. D. Singh, H. Chaouchi, and J. M. Bonnin, Wireless Sensor Networks: A Survey on Recent Developments and Potential Synergies, *J. Supercomput.*, 68(1), 1–48, 2014.

[3] R. Rajkumar, I. Lee, L. Sha and J. Stankovic, Cyber-Physical Systems: The Next Computing Revolution, In *Proc. of the 47th Design Autom. Conf.*, 731–736. 2010.

[4] F. Mattern and C. Floerkemeier, From the Internet of Computers to the Internet of Things, In *From Active Data Management to Event-Based systems and More*, Springer Berlin, 242-259, 2010.

[5] Y. Mo *et al.*, Cyber-Physical Security of a Smart Grid Infrastructure, *Proc. of the IEEE*, 100(1), 195-209, 2012.

[6] S. Ali *et al.*, Network Challenges for Cyber Physical Systems with Tiny Wireless Devices: A Case Study on Reliable Pipeline Condition Monitoring, *Sensors*, 15, 7172–7205, 2015.

[7] M. M. Hossain, M. Fotouhi, and R. Hasan, Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things, *2015 IEEE World Congress on Services*, 21-28, 2015.

[8] S. Sicari, A. Rizzardia, L. A. Griecob, and A. Coen-Porisini, Security, Privacy and Trust in Internet of Things: The Road Ahead, *Comput. Net.*, 76, 2015.

[9] Y. Wang, G. Attebury, and B. Ramamurthy, A Survey of Security Issues in Wireless Sensor Networks, *IEEE Commun. Surv. & Tuts.*, 8(2), 2006.

[10] C. M. Medaglia and A. Serbanati, An Overview of Privacy and Security Issues in the Internet of Things, *The Internet of Things*, Springer, 2010.

[11] J. S. Kumar and D. R. Patel, A Survey on Internet of Things: Security and Privacy Issues, *Int. J. Comput. Appl.*, 90(11), 20–26, 2014.

[12] J. Lin *et al.*, A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications, *IEEE Int. of Things J.*, 99, 1–1, 2017.

[13] J. Granjal, E. Monteiro, and J. S. Silva, Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues, In *IEEE Commun. Surv. & Tuts.*, 17(3), 1294–1312, 2015.

[14] A. Broring *et al.*, New Generation Sensor Web Enablement, *Sensors*, 11(3), 2652–2699, 2011.

[15] K. Sohrabi, J. Gao, V. Ailawadhi, and G. J. Pottie, Protocols for Self-Organization of a Wireless Sensor Network, In *IEEE Pers. Commun*, 7(5), 16–27, 2000.

[16] International Electrotechnical Commission, Internet of Things: Wireless Sensor Networks, *White Paper*, 2014.

[17] M. Whitman and H. Mattord, Principles of Information Security, 4th ed., *Cengage Learning*, 2012.

[18] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends, In *Proc. of the IEEE*, 104(9), 1727–1765, 2016.

[19] A. Perrig *et al.*, SPINS: Security Protocols for Sensor Networks, *Wireless Netw.*, 8(5), 521–534. 2002.

[20] C. Karlof, N. Sastry, and D. Wagner, TinySec: A Link Layer Security Architecture for wireless Sensor Networks, In *Proc. of the 2nd Int. Conf. on Embedded Netw. Sensor Sys.*, 162-175, 2004.

[21] S. Zhu, S. Setia and S. Jajodia, LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks, In *Proc. of 10th ACM Conf. on Comput. and Commun. Security*, 62–72, 2003.

[22] J. Ren, T. Li, and D. Aslam, A Power Efficient Link Layer Security Protocol (LLSP) for Wireless Sensor Networks, *Military Commun. Conf.*, 2, 1002-1007, 2005.

[23] A. D. Wood, L. Fang, J. A. Stankovic, and T. He, SIGF: A Family of Configurable, Secure Routing Protocols for Wireless Sensor networks, In *Proc. of the 4th ACM Workshop on Security of Ad Hoc and Sensor Netw.*, 35–48, 2006.

[24] IEEE Standard 802.15.4-2003, *IEEE Comput. Soc.*, 2003.

[25] F. Chen, T. Talanis, R. German, and F. Dressler, Real-time Enabled IEEE 802.15.4 Sensor Networks in Industrial Automation, *IEEE Int. Symp. on Ind. Embedded Sys.*, 136–139, 2009.

[26] S. Ullah *et al.*, A Study of MAC Protocols for WBANs, *Sensors*, 10(1), 128–145, 2010.

[27] D. M. Han and J. H. Lim, Smart Home Energy Management System using IEEE 802.15.4 and Zigbee, In *IEEE Trans. on Consumer Electron.*, 56(3), 1403–1410, 2010.

[28] R. Daidone, G. Dini, and M. Tiloca, On Experimentally Evaluating the Impact of Security on IEEE 802.15.4 Networks, *Int. Conf. on Distrib. Comput. in Sensor Sys. and Workshops*, 1–6, 2011.

[29] J. Polastre, J. Hill, and D. Culler, Versatile Low Power Media Access for Wireless Sensor Networks, In *Proc. of the 2nd Int. Conf. on Embedded Netw. Sensor Sys.*, 95–107, 2004.

[30] Y. W. Law *et al.*, Energy-Efficient Link-Layer Jamming Attacks Against Wireless Sensor Network MAC Protocols, *ACM Trans. on Sensor Netw.*, 5(1), article 6, 2009.

[31] M. R. Palattella *et al.*, Standardized Protocol Stack for the Internet of (Important) Things, *IEEE Comm. Surv. & Tuts.*, 15(3), 1389–1406, 2013.

[32] A. Le *et al.*, 6LoWPAN: A Study on QoS Security Threats and Countermeasures using Intrusion Detection System Approach, *Int. J. of Commun. Sys.*, 25(9), 1189–1212, 2012.

[33] T. Winter *et al.*, RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks, https://tools.ietf.org/html/rfc6550, 2012.

[34] S. Moeller, A. Sridharan, B. Krishnamachari, and O. Gnawali, Routing Without Routes: The Backpressure Collection Protocol, In *Proc. of the 9th ACM/IEEE Int. Conf. on Inf. Process. in Sensor Netw.*, 279–290, 2010.

[35] R. Venkataraman, S. Moeller, B. Krishnamachari, and T. R. Rao, Trust-based Backpressure Routing in Wireless Sensor Networks, *Int. J. of Sensor Netw.*, 17(1), 27–39, 2015.

[36] R. Fonseca *et al.*, TEP 123: The Collection Tree Protocol (CTP), 2006.

[37] P. Pecho, P. Hanacek, and J. Nagy, Simulation and Evaluation of CTP and Secure-CTP Protocols, *Radioengineering*, 19(1), 89–99, 2010.

[38] C. Bormann, A. P. Castellani, and Z. Shelby, CoAP: An Application Protocol for Billions of Tiny Internet Nodes, In *IEEE Internet Comput.*, 16(2), 62–67, 2012.

[39] Y. Xiao, S. Sethi, H-H. Chen, and B. Sun, Security Services and Enhancements in the IEEE 802.15.4 Wireless Sensor Networks, *IEEE Global Telec. Conf.*, 1976–1980, 2005.

[40] C. P. O'Flynn, Message Denial and Alteration on IEEE 802.15.4 Low-Power Radio Networks, *4th IFIP Int. Conf. on New Technol., Mobility and Security*, 1–5, 2011.

[41] D. R. Raymond, R. C. Marchany, M. I. Brownfield, and S. F. Midkiff, Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols, In *IEEE Trans. on Veh. Technol.*, 58(1), 367–380, 2009.

[42] H. Kim, Protection Against Packet Fragmentation Attacks at 6LoWPAN Adaptation Layer, *Int. Conf. on Convergence and Hybrid Inf. Technol.*, 796–801, 2008.

[43] R. Hummen *et al.*, 6LoWPAN Fragmentation Attacks and Mitigation Mechanisms, In *Proc. of the sixth ACM Conf. on Security and Privacy in Wireless and Mobile Netw.*, 55–66, 2013.

[44] L. M. L. Oliveira, J. J. P. C. Rodrigues, A. F. de Sousa, and J. Lloret, A Network Access Control Framework for 6LoWPAN Networks, *Sensors*, 13(1), 1210-1230, 2013.

[45] S. Raza, *et al.*, Securing Communication in 6LoWPAN with Compressed IPsec, *Int. Conf. on Dist. Comp. in Sens. Sys. and Workshop*, 1–8, 2011.

[46] E. J. Cho, J. H. Kim, and C. S. Hong, Attack Model and Detection Scheme for Botnet on 6LoWPAN, In *Proc. of the 12th Asia-Pacific Netw. Operations and Manag. Conf.*, Springer, 515-518, 2009.

[47] T. Tsao, *et. al.*, A Security Framework for Routing over Low Power and Lossy Networks, https://tools.ietf.org/html/draft-ietf-roll-security-framework-07, 2012.

[48] L. Wallgren, *et. al.*, Routing Attacks and Countermeasures in the RPL-Based Internet of Things, *Int. J. of Distrib. Sensor Netw.*, 9(8), 2013.

[49] S. Kent, IP Encapsulating Security Payload (ESP), RFC 4303, https://tools.ietf.org/html/rfc4303, 2005.

[50] S. Raza, *et. al.*, SVELTE: Real-Time Intrusion Detection in the Internet of Things, *Ad Hoc Netw.*, 11(8), 2661–2674, 2013.

[51] K. Heurtefeux *et al.*, Enhancing RPL Resilience Against Routing Layer Insider Attacks, *IEEE 29th Int. Conf. on Advanced Inf. Netw. and Appl.*, 802–807, 2015.

[52] E. C. H. Ngai *et al.*, On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks, *IEEE Int. Conf. on Commun.*, 3383–3389, 2006.

[53] K. Weekly and K. Pister, Evaluating Sinkhole Defense Techniques in RPL Networks, *20th IEEE Int. Conf. on Netw. Protocols*, 1–6, 2012.

[54] F. I. Khan *et al.*, Wormhole Attack Prevention Mechanism for RPL based LLN Network, *5th Int. Conf. on Ubiq. and Future Net.*, 149–154, 2013.

[55] L. Lazos *et al.*, Preventing Wormhole Attacks on Wireless Ad Hoc Networks: A Graph Theoretic Approach, *IEEE Wireless Commun. and Netw. Conf.*, 2, 1193–1199, 2005.

[56] J. Newsome *et al.*, The Sybil Attack in Sensor Networks: Analysis & Defenses, In *Proc. of the 3rd Int. Symp. on Inf. Process. in Sensor Netw.*, 259–268, 2004.

[57] J. Hui and J. Vasseur, The Routing Protocol for Low-Power and Lossy Networks (RPL) Option for Carrying RPL Information in Data-Plane Datagrams, RFC 6553, https://tools.ietf.org/html/rfc6553, 2012.

[58] A. Sehgal *et al.*, Addressing DODAG Inconsistency Attacks in RPL Networks, *Global Inf. Infrastructure and Netw. Symp.*, 1–8, 2014.

[59] A. Mayzaud *et al.*, Mitigation of Topological Inconsistency Attacks in RPL-based Low-Power Lossy Networks, *Int. J. of Netw. Manag.*, 2015.

[60] A. Dvir, T. Holczer, and L. Buttyan, VeRA - Version Number and Rank Authentication in RPL, *IEEE 8th Int. Con. on Mobile Ad-Hoc and Sensor Sys.*, 709–714, 2011.

[61] M. Landsmann, M. Wahlisch, and T. C. Schmidt, Topology Authentication in RPL, *IEEE Conf. on Comp. Commun. Workshops*, 73–74, 2013.

[62] Z. Lu, *et al*, Securing the Backpressure Algorithm for Wireless Networks, *IEEE Trans. on Mobile Comp.* 16(4), 1136–1148, 2017.

[63] F. J. Shang, C. Li, and J. L. Qin, Improvement of Approach to Detect Sinkhole Attacks in Wireless Sensor Networks, *Comp., Intell. Comput. and Edu. Technol.*, 695–698, 2014.

[64] S. Sultana, D. Midi, and E. Bertino, Kinesis: a Security Incident Response and Prevention System for Wireless Sensor Networks. In *Proc. of the 12th ACM Conf. on Embedded Netw. Sensor Sys.*, 148–162, 2014.

[65] E. Rescorla and N. Modadugu, DTLS: Datagram Transport Layer Security, RFC 4347, https://tools.ietf.org/html/rfc4347, 2006.

[66] S. Raza *et al.*, Lithe: Lightweight Secure CoAP for the Internet of Things, *IEEE Sensors J.*, 13(10), 3711–3720, 2013.

[67] A. Bhattacharyya *et al.*, LESS: Lightweight Establishment of Secure Session: A Cross-Layer Approach Using CoAP and DTLS-PSK Channel Encryption, *IEEE 29th Int. Conf. on Advanced Inf. Netw. and Appl. Workshops*, 682–687, 2015.

[68] A. Diaz and P. Sanchez, Simulation of Attacks for Security in Wireless Sensor Network, *Sensors*, 16, 1932, 2016.

[69] Contiki operating system, http://www.contikios.org/.

[70] A. Dunkels *et al.*, Powertrace: Network-Level Power Profiling for Low-Power Wireless Networks, http://soda.swedish-ict.se/4112/, 2011.

Ivana Tomić is currently a Research Associate at Imperial College London. She received her PhD in Control Theory from City, University of London in October 2016 where she worked on the implementation of distributed control algorithms in multi-agent networks. Her research interests include security of cyber-physical systems and IoT, distributed control algorithms and optimal control. She is currently researching security of WSNs as a part of PETRAS project 'IoT in the Park' funded by EPSRC.

Julie A. McCann is a Professor in Computer Systems at Imperial College. Her research centers on highly decentralized and self-organizing scalable algorithms for spatial computing systems e.g. wireless sensing networks. She leads both the Adaptive Embedded Systems Engineering Research Group and the Intel Collaborative Research Institute for Sustainable Cities, and is currently working with NEC and others on substantive smart city projects. She has received significant funding though bodies such as the UKs EPSRC, TSB and NERC as well as various international funds, and is an elected peer for the EPSRC. She has actively served on, and chaired, many conference committees and is currently Associative Editor for the ACM Transactions on Autonomous and Adaptive Systems. She is a Fellow of the BCS.