future internet

MDPI

Article

"Network Sentiment" Framework to Improve Security and Privacy for Smart Home

Tommaso Pecorella, Laura Pierucci * and Francesca Nizzi

Department of Information Engineering, Università di Firenze, Via di Santa Marta 3, 50139 Firenze, Italy; tommaso.pecorella@unifi.it (T.P.); francesca.nizzi@unifi.it (F.N.)

* Correspondence: laura.pierucci@unifi.it; Tel.: +39-055-2758626

Received: 31 October 2018; Accepted: 17 December 2018; Published: 19 December 2018

Abstract: A Smart Home is characterized by the presence of a huge number of small, low power devices, along with more classical devices. According to the (IoT) paradigm, all of them are expected to be always connected to the Internet in order to provide enhanced services. In this scenario, an attacker can undermine both the network security and the user's security/privacy. Traditional security measures are not sufficient, because they are too difficult to setup and are either too weak to effectively protect the user or too limiting for the new services effectiveness. The paper suggests to dynamically adapt the security level of the smart home network according to the user perceived risk level what we have called *network sentiment* analysis. The security level is not fixed, established by a central system (usually by the Internet Service Provider) but can be changed with the users cooperation. The security of the smart home network is improved by a distributed firewalls and Intrusion Detection Systems both to the smart home side as to the Internet Service Provider side. These two parts must cooperate and integrate their actions for reacting dynamically to new and on going threats. Moreover, the level of *network sentiment* detected can be propagate to nearby home networks (e.g., the smart home networks of the apartments inside a building) to increase/decrease their level of security, thus creating a true in-line (IPS). The paper also presents a test bed for Smart Home to detect and counteract to different attacks against the IoT sensors, Wi-Fi and Ethernet connections.

Keywords: Internet of Things; security; dynamic protection

1. Introduction

In a Smart Home environment several specific home automation devices, (e.g., temperature monitoring sensors, air quality devices, infotainment system, Smart TVs, fire and/or gas detectors, etc.) might need to communicate with the external networks (e.g., smoke detection alarm) and receive commands to perform various actions (e.g., increase the temperature in the house or remotely monitor with surveillance cameras unattended rooms or child's rooms).

The more the home becomes smarter, the more the problem of cyber security becomes important. As a matter of fact, several recent attacks have been performed by exploiting vulnerabilities of small devices (e.g., My Friend Cayla, a famous toy [1] attacked for configuration mistakes, i.e., default password unchanged), and by using this high number of devices as sources for (DDoS) attacks (see for example [2] or the malware Mirai in the 2016 [3,4]). Moreover, malicious attacks may bring a significant impact not only to the network security but also to the safety of the user. For example, by using Internet device–scanning search engines such as Shodan (https://www.shodan.io), it is possible to obtain a list of home surveillance cameras with their IP addresses, geographic locations, etc. [5]. A burglar can control when the IP webcam is more frequently accessed and consequently can understand if the house owner is away from the house.

Unfortunately, the obvious security approaches are not really feasible: (i) upgrading the software of the vulnerable appliances is often impossible (the end-users have often limited capabilities), (ii) substituting them with more secure devices is not a viable solution (too expensive for Home scenario), and (iii) blocking their traffic preemptively might prevent their functionality altogether. Moreover, classical security approaches (i.e., the use of restrictive rules for firewalls, strong authentication system to access the network, e.g., IEEE 802.1X) are designed for those attacks which are not in the interior network while the IoT devices are vulnerable to intrusion both from Internet than from wireless attacks originated from inside the smart home network.

To make effective the connections of resource-constrained IoT devices the IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) are standardized [6], empowered by protocols such as 6LoWPAN adaptation layer [7], Routing Protocol for Low Power and Lossy Networks [8] and the Constrained Application Protocol (CoAP) [9,10]. The 6LoWPAN network uses compressed IPv6 protocol for networking and IEEE 802.15.4 as data-link and physical layers protocol. Each layer in 6LoWPAN can be vulnerable to security threats and, unfortunately, standard preventive security mechanisms, such as cryptography and authentication, cannot detect all possible attacks, such as insider attacks (e.g., routing attacks) or a guy who uses a legal key but has malicious intent.

As consequence, (IDS)s specifically designed for IoT are necessary as a second line of defense to provide more security awareness and to add some dynamic threat protection functionalities to a network.

All these actions are not easy for a normal user, and they limit the network usability. For these reasons the network security is often neglected in many domestic networks, and even in some enterprise ones. We believe that the network itself must adaptively react to new threats, increasing the security measures when there is an effective, on going, vulnerability exploitation, and relaxing the rules when there is no real threat. In the following, we will call the dynamic threat evaluation as *network sentiment analysis*.

With respect to this, the paper shows an architecture, called SHIELD, with a distributed firewalls and threat analysis system. One part of the security infrastructure must be as close as possible to the user, potentially at the user's premises, and another part in the (ISP) network.

Our contribution over the state of the art is about the way these elements should be integrated. In the past the firewalls acted as separate entities. We argue that all the user firewalls and IDSs should be part of an integrated ecosystem, reacting dynamically to new and ongoing threats. In this vision, the whole system should be orchestrated by a coordinator hosted by the ISP (or by any secure and trusted provider), which is responsible for evaluating the risk measure of each user and of the ISPs as a whole. In this vision, if the network sentiment level of a smart home network is increased due to the risk of attack, this information can be propagated to the nearby smart home networks (e.g., in the different apartments in the same building) which can take counteractions automatically establishing a real time Intrusion Prevention System (IPS).

The *network sentiment* approach will:

- Ease the network security setup,
- Make it more reactive toward incoming threats,
- Keep the number of security rules to the minimum necessary to guarantee an adequate security and
- Increase the security level in networks geographically close or with similar characteristics in terms of firmware of devices, connections and applications.

Moreover, the paper also presents a testbed able to detect and react against attacks on Ethernet, Wi-Fi connections and IoT protocols. The testbed described in the paper has the goal to outline that the proposed SHIELD architecture is feasible. Toward this end, the hardware used in the testbed reflects as much as possible a normal Linux-based Customer Premises Equipment (CPE). As a consequence, we expect that implementing the SHIELD functionalities on a commercial CPE will be very easy.

The paper is organized as follows. Section 2 presents a brief overview of the state of the art in the field of security and privacy challenges and threat models for smart home environment and IoT. Section 3 outlines the proposed security framework, called SHIELD system, for smart home highlighting the main characteristics of the dynamic network sentiment analysis and threat reactions. Section 5 shows the implemented smart home test bed. Finally, in Section 6, we discuss security and privacy solutions for smart home environment and future directions are provided.

2. Related Works

In a IoT smart home scenario many small, low power, low computation devices are used in the segment of home automation to improve the quality of services and, as consequence, the quality of experience offered to the users [11]. Different aspects for preserving privacy can be found in [12] and several papers in literature examine the security challenges and threats suited for smart homes, as in [6,13], where surveys of existing protocols for secure communications on IoT can be found, together with open challenges and research issues in this area. In [14] a protocol is proposed to secure route optmization and handover management, which uses trust between Proxy mobile IPv6 (PMIPv6) domain and smart home to ensure security as well as performance over the path between mobile nodes and home IoT devices. In [15], the authors propose a secure scheme for data uploading on Cloud to guarantee the integrity of the data with a session key generation assisted by the home gateway. In [5], a review of existing network techniques for enhancing IoT security is provided together with future key technologies for trusted Smart Home systems such as system auto-configuration and security update. A gateway architecture is chosen as the most appropriate for resource-constrained devices and for high system availability. In [16] the authors propose a cross layer method to overcome the traceability of the user in smart home networks 6LoWPAN . In this case, the IEEE 802.15.4 standards [17] foresees to cipher the payload but leaves out the headers containing the layer 2 addresses of the source and destination of the packets. In the proposed method all the nodes change periodically all their addresses, both at layer 2 and 3, to secure of both the 802.15.4 and 6LoWPAN protocols.

However traditional Information and Communications Technology (ICT) standard security solutions, such as crytography and authentication tecniques, do not prevent all possible attacks and are not tailored for smart home environment due to the resource-constrained IoT devices, to their heterogeneous interaction and to their different policy and connectivity domains.

As consequence, IDSs are required to detect intruders and malicious activities to threaten the network. IDSs can be classified in signature-based or behavior-based. Signature-based IDSs use pattern-matching techniques to detect an attack, while behavior-based IDSs analyze the devices behavior to detect anomalies. The first type is best suited for known attack and the second one for unknown attacks. Hybrid detection technique combining signature and anomaly based approaches can improve the efficacy of IDS.

Furthermore, IDSs can be classified in Host, Network or Distributed. Host IDSs only process the data of a single node, Network IDSs are able to monitor a network (typically one or more links), and Distributed IDSs are able to process the data of multiple, independent probes and/or multiple federated IDSs. Several IDSs are designed for wireless sensor networks (WSN), a general survey on IDS and IPS can be found in [18]. However, these IDSs are not directly applicable for IoT because IoT devices are globally accessible, are resource-constrained, are heterogeneous, adopt new protocols such as COAP, RPL. A survey of more IoT-oriented IDSs can be found in [19–22].

Most of these IDSs focus only on threats at network layer. Examples of real-time IDS for IoT can be SVELTE [23] which meets the requirements of IPv6-connected IoT devices and detects routing attacks such as sink-hole, selective forwarding, and spoofed or altered routing information; Complex Event-processing (CEP) [24] which detects events in real-time by analyzing the stream of information; the IDS by [25] which targets Denial of Service (DoS) attacks on RPL.

In [26] an intrusion detection and prevention framework is proposed to detect DoS attacks on the network and attacks against the normal operations rules of the CoAP protocol.

An IoT security framework for Smart Home is introduced in [27] and a general threat model to recognize the vulnerabilities for IoT services against cyberattacks is analyzed. A smart home testbed is considered to monitor variables and control elements with different protocols such as Wi-Fi, ZigBee, etc. An IDS based on anomaly behavior analysis (ABA) of the end nodes operations allows to detect and classify a wide range of attacks against IoT devices, such as replay attacks, delay attacks, (DoS) or DDoS attacks, noise injections, etc.

In [28] a security framework for home network is proposed with residential gateways as devices responsible for the exchange of information between the ISP infrastructure and the customer network to develop a vastly distributed IDS/IPS, enforcing preventive or corrective countermeasures, according to the instructions issued by the ISP. This securiy framework, as other papers in literature, foresee to move the security intelligence in the ISP. In our system, only the bare minimum necessary to calculate the users' similarity score is known by the ISP, while the actual countermeasures (i.e., the network configuration) is left to the smart home side (SHIELD Home (SH) device). This enables scalability (because the ISP does not have to address all the users' CPE details), fine-grained configuration (the SH device knows more precisely the actual user's network configuration), and it allows the user (if he is an expert) to override the security setup proposed by the ISP. Moreover, our solution provides a high degree of flexibility with respect to the different IoT networks, which are often user-owned and deployed. These networks are difficult to manage by the ISP in a "pure" centralized way and all the current approaches are not sufficiently reactive and dynamic to protect the smart environments adequately. As a matter of fact, in the current architectures attacking a network triggers only a local response, and it does not have any system-level reaction. We believe that our *network sentiment analysis* fills the gap between actual network security techniques and a more coordinated reaction system.

3. SHIELD System

In a Smart Home each Internet-connected device has its own peculiar security and availability requirements. There are still a number of issues to be addressed, particularly in the IoT network section, related to the devices deployment and initialization.

As mentioned in the Introduction, we believe that the real problem is to have a dynamic security protection system able to react to possible threats by reconfiguring in real-time the security defenses of the network (e.g., firewalls). As a matter of facts, the main problem with traffic filtering is the user. If the firewall is too restrictive, the user (if he/she is an expert) will disable (or circumvent) it. If the firewall is too restrictive, it is useless. Moreover, the vast majority of the users do not have the technical skills to understand the firewall configuration and to autonomously update the firewall rules if a new threat is discovered.

A common approach is to protect the user with an ISP-level firewall, but this architecture is not scalable and it does not adapt to the needs of different users. Moreover, the attack could be originated from inside the Smart Home network thanks, e.g., to an infected mobile device. For this reason we think that it is mandatory to provide both types of protection: at ISP level and in the user's premises. Therefore it is necessary the use of IDSs to add end-to-end threats protection to the smart home network and the Internet [29].

Signature-based and anomaly behaviour-based IDSs are extremely useful, but they are even more difficult to configure for the end-user. Moreover, any IDS kind is subject to a lot of false warnings, either false positives or about attacks that cannot succeed (e.g., an attack aimed at a type of device that is not in the network). In order to avoid an excessive computational complexity on the IDS, only the relevant threats for a given network should be trapped, plus the ones that are believed to be actively being exploited by attackers. As a consequence, IDS as well must be dynamically configured in response to on going threats. Moreover, signature and anomaly based IDSs analyze usually data traffic while new IDS should be specifically designed for IoT smart home environment where the attacks can also be the altering, e.g., of the reported data from sensors, or the controls of actuators.

In 6LoWPAN networks, 6LoWPAN border routers (6LBR) are used to integrate the WSN with Internet and thanks to their resources availability they can support intrusion detection system and generate alerts. As consequence, a hybrid topology for IDSs can be envisaged where detection capability are distributed and with a central unit responsible for decision operations and countermeasures.

For this reason, we propose to adopt the architecture outlined in Figure 1. This architecture is designed to guarantee the interoperability with existing Internet standards and the communications of sensing devices with other Internet components in the context of future IoT distributed applications.

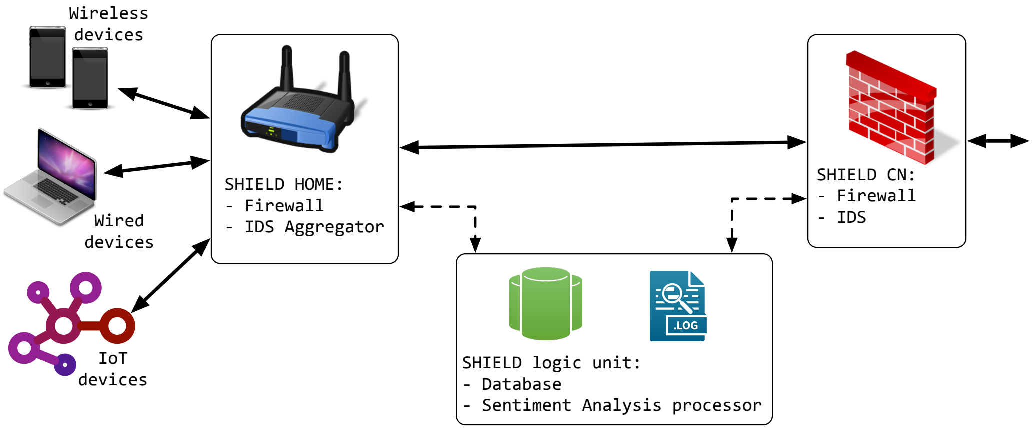


Figure 1. SHIELD Architecture.

In Figure 1, we outlined the three major components of a Smart Home environment: devices connected by high-bandwidth wireless networks (typically Wi-Fi), devices connected through cables (Ethernet, Power Line Communications, etc.), and IoT devices—in the figure the IoT devices are represented as IEEE 802.15.4 nodes, but other standards are possible. Furthermore, IoT devices can be differentiated according to their role and their security/reliability requirements [30].

Each device type and every connection technology needs its own particular detection approach. As an example, wired connections need only a wiretap on the main switch (usually the home gateway), while special receivers will be needed for wireless connections (e.g., high gain antennas).

To detect attacks in multihops networks (e.g., IEEE 802.15.4) it is possible to use multiple probing point on special nodes. It is worth noticing that the probe points should be connected to a master IDS engine through a secure side-channel, and that the load balancing between the master IDS and the probes depends on the side-channel congestion and the energy consumption of each device. Even if this is an important point, we will not further analyze it, leaving a full analysis to a future paper.

In the security system for a smart home, hereafter called SHIELD system, the (SCN) is the element in the ISP network that is responsible for (a) firewalling the ISP and users networks from attacks originating from the outside of the ISP network, (b) analyzing the traffic to spot suspicious traffic and (c) collecting all the data from the ISP IDS.

The network element responsible for protecting the home network side is the (SH). From a logical point of view, the entities are two, the SHIELD Firewall and the SHIELD IDS Aggregator. The first is responsible for filtering the traffic from and to the ISP, while the second controls and harmonizes all the different IDSs present in the SH network.

The SH is responsible for (i) correctly configuring the IDS to match the threats that are meaningful for the Smart Home environment (e.g., by silencing the alarms for patched devices), (ii) activating security countermeasures (e.g., firewall rules, to block further communications from the attacked sensor) for actively exploited vulnerabilities.

The ‘core’ of the SHIELD architecture is the (SLU). This entity receives all the (anonymized) IDSs alarms and warnings from all the SH in the ISP domain. The SLU focuses on discovering various relations between individual warnings/alerts and, according to alert correlation scores, it can change the *Network Sentiment* level and take various countermeasures, e.g., modify the firewalls configurations, block further communications from the attacked IP address, up to block further communications between the attacked Smart Home domain and Internet. In the SLU, the *Network Sentiment* processor analyzes similarities scores among different smart home networks, in order to implement preemptive countermeasures in these networks. As a matter of fact, it is more than possible that an attack will propagate to smart home networks ‘close’ to the network under attack, as shown in Figure 2.

The SLU logic is presented in Figure 3, where it is outlined the different behavior with respect to an ongoing attack (*Alarm*) and to a possible attack (*Warning*). The first triggers an immediate reaction, while the second is evaluated according to the frequency of similar warning alerts, and the presence of similar warnings sent by different users. The SLU evaluates the attack type, the possible outcomes, and can select the most appropriate mitigation techniques, eventually modifying the ISP-level firewall rules. However, the most important element of the SLU is, in our opinion, the capability to propagate the *Network Sentiment*, i.e., the overall status of the network with respect to on going attacks, to the different SH units. This feature enables a *preemptive* security approach, where a SH is ‘immunized’ from an attack that did target another SH (Figure 2).

Moreover, the SLU can issue periodic or triggered warnings (e.g., e-mails, messages on the SH display, on application etc.) to inform the users about the firewalling decisions, how to improve the network security, etc. In this way, the users should be able to customize the system to better suit their needs. As an example a non-technical user could aim for maximum automatic protection, while a skilled user could decide to ignore some threats and planned actions (at his own risk).

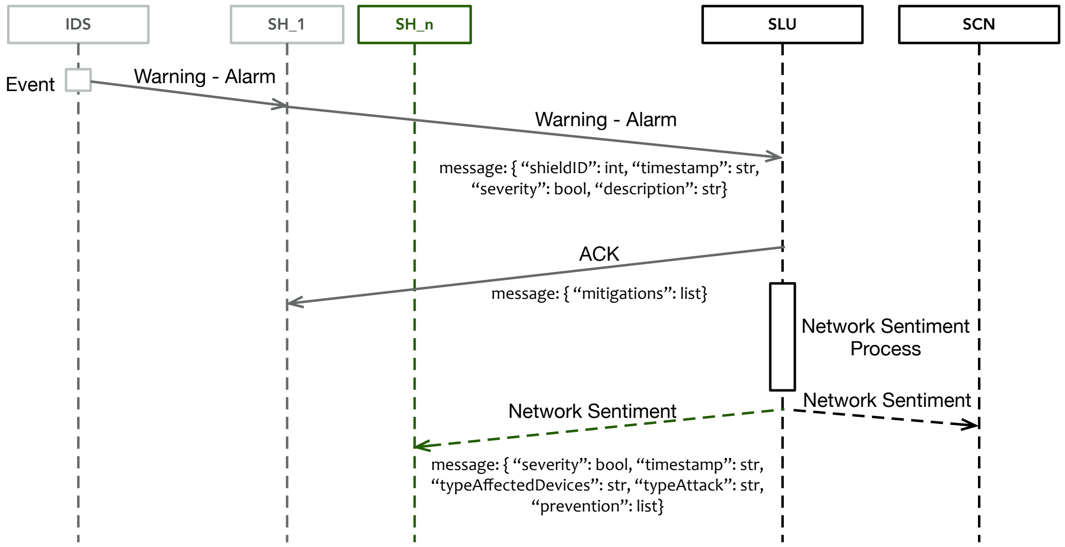

IDS
SH_1
SH_n
SLU
SCN
Event
Warning - Alarm
Warning - Alarm
message: { “shieldID”: int, “timestamp”: str, “severity”: bool, “description”: str}
ACK
message: { “mitigations”: list}
Network Sentiment Process
Network Sentiment
Network Sentiment
message: { “severity”: bool, “timestamp”: str, “typeAffectedDevices”: str, “typeAttack”: str, “prevention”: list}

Figure 2. SHIELD blocks interaction.

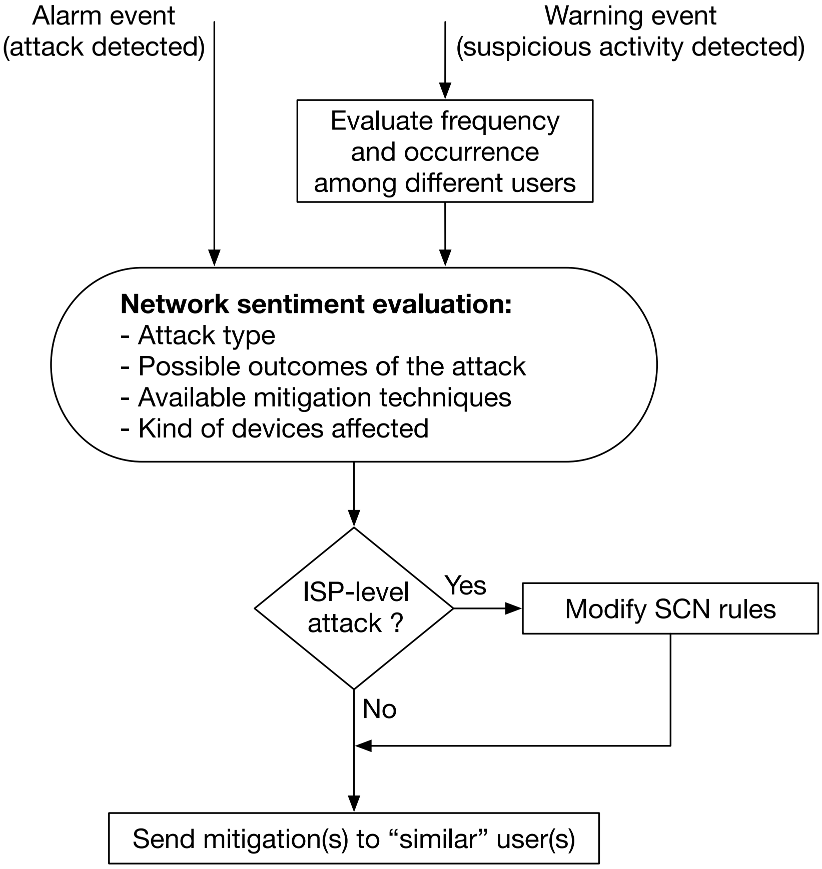

Alarm event
(attack detected)
Warning event
(suspicious activity detected)
Evaluate frequency and occurrence among different users
Network sentiment evaluation:
- Attack type
- Possible outcomes of the attack
- Available mitigation techniques
- Kind of devices affected
ISP-level attack ?
Yes
Modify SCN rules
No
Send mitigation(s) to "similar" user(s)

Figure 3. SLU logic.

4. Network Sentiment

The *Network Sentiment* should not be confused with a simple reaction to an ongoing threat. On the contrary, the Network Sentiment is something that affects each user in a different way, and it should be built according to a number of parameters that are inherently user-specific.

As an example, a user with no computers or devices of type *X* will not have his *Network Sentiment* changed if there is an ongoing threat specifically targeted toward this kind of devices.

The Network Sentiment is also aimed at evaluating and reacting to threats that are spatially or socially correlated. As an example, a port scan detected over a particular wireless network means that the attacker is physically close to the target network. As a consequence, the physically nearby networks must activate proper countermeasures.

However, the Network Sentiment protection can be extended to non-physical spaces, such as participation in groups, e.g., social media, common interests, etc. An attack spreading through social engineering and/or social media interactions can be actively mitigated.

As a matter of fact, the *Network Sentiment* must:

- Evaluate the presence of an attack (or the attack probability),
- Evaluate the means of the attack spreading, and
- Use the users similarities to strengthen the protection of the potential victims, where the users similarities refers to the attack type, network kind (e.g., devices, topology), users' behviour (e.g., use of Internet services, online social relationships), network location, etc.

In order to evaluate the *Network Sentiment*, the SLU must collect several SH information e.g.,:

- The OS type and version being used in the Smart Home. This is necessary to evaluate the presence of vulnerabilities in the devices.

- The user's location—to evaluate the likeliness of "geographical correlated" attacks (e.g., Wi-Fi password cracking attempts)
- The user's social behavior—to predict the spread of social-spreading malware, e.g., malware carried by a social platform, such as Facebook.
- Ongoing attacks (low confidence, high confidence, confirmed),
- Attack type (e.g., DDoS, fault data injection),
- Attack effectiveness (i.e., if there are infected hosts in the user network),
- Number of blocked attacks,
- etc.

These informations can be organized in an Intrusion Detection Message Exchange Format (IDMEF) message [31] and sent to the ISP. The exact message encoding is not important in this context, but it should be standardized to allow the interoperability between different vendors. Moreover, the SLU must evaluate (CVE) reports [32] to properly block potential or ongoing threats and to suggest possible actions to the users (e.g., system upgrades).

Thanks to the users reports, the ISP can compute different types of metrics. Some alert reports (e.g., a confirmed ongoing attack) will result in an immediate response by the system. The reaction will still be dependent on the attack type, e.g., a phishing attack could result in an alert to the 'friends' of the attacked used (measured by the mail messages, social media connections, etc.). Other attacks will need more reports, possibly by different users, to trigger a response. This is particularly true for suspicious activities that could be simply an unexpected, albeit normal, user behavior. In this case, a consensus-based algorithm can be used to evaluate the threat.

The feedback from the SLU to the SH can be performed by IDMEF messages or, as in the previous case, any other standard message type.

Summarizing, the exchange of the *Network Sentiment* informs both the SH and the SCN about the ongoing attacks in the network. In this way, the whole ISP network is treated as one whole network, without the distinction between (CN) and users s (LANs).

4.1. Enhanced Services Enabled by SHIELD

The SHIELD system is meant to protect the user network with minimal interaction with complex devices like firewalls and IDS. However, to think about it as a simple security framework would be reductive. As a matter of fact, the SHIELD devices can greatly improve the user experience and, at the same time, provide a way to keep the user up-to-date with the current and ongoing threats to his/her network without generating overreactions.

We believe that the user should be constantly aware of the status of their network, including the ongoing attacks. However, this must not raise anxiety in the user, but promote a conscious utilization of the network. As a consequence, the SH device must constantly communicate with the user, e.g., by infographics on a display or via smartphone applications. Putting the user in the loop can also increase the good behaviours of the users, like keeping their systems up-to-date, and even the device vendors ones, increasing the chances that a vendor will actively support its products by patching security bugs in the devices firmwares.

Moreover, we want to stress that SHIELD acts as a true IPS. As a matter of fact a 'traditional' IPS can block an on going threat, while SHIELD can block a threat before hand, simply because another user in close network is subject to the same threat. As a consequence, SHIELD is really an intrusion prevention mechanism.

4.2. Security Considerations

Like every networked system, also SHIELD is sensible to threats. As a matter of fact, an attacker could take advantage of the SHIELD system to fake an ongoing attack, causing (for example) a DoS. For this reason, it is important that the SHIELD system is protected and considered as a primary asset of the ISP. If we define a security zone as a network area with a well-defined perimeter and a strict boundary protection, we have that:

- The SLU and the SCN are in the same security zone,
- The SLU and the SH are in different security zones,
- The SCN and the SH are in different security zones.

In other terms, we can safely assume that the SLU and the SCN are inside the administrative domain of the ISP and their communication security is automatically guaranteed. On the contrary, a (MiM) attack between the SH and the ISP network is considered possible because an attacker can disguise itself as a legitimate user. As a consequence, the communications between the IDS probes (or the distributed IDS system) and the SH must be adequately secured.

It is out of the scope of this paper to describe the security algorithms that can be used to properly secure the above mentioned communication channels but the system should, at minimum, provide a strong authentication between the SH and the other two SHIELD entities, possibly by using certificates and/or smart cards. Moreover, the SH device should pass severe vulnerability assessment tests and be tamper-proof. If this is not the case, the SHIELD system must consider all the attacks reports from the users as simple warnings (low confidence reports), and use consensus algorithms to reject spurious data.

5. Smart Home Testbed

In order to evaluate the SHIELD framework, we built a prototype of the SH and the SLU. In particular, the SH prototype is equipped with Ethernet, Wi-Fi and IEEE 802.15.4 interfaces. Moreover, different attack types have been tested to evaluate the system feasibility.

The SHIELD testbed is shown in Figure 4. The SH (shown to the left) is an UDOO board and an OpenMote CC2538 module as Border Router for 6LoWPAN (6LBR). The UDOO board is a single board with an ARM Cortex-A9 CPU, RAM DDR3 (1 GB), GPIOs, microUSB ports, Gigabit Ethernet and WiFi module while OpenMote-CC2538 is based on Texas Instruments CC2538 System on chip with an IEEE802.15.4 transceiver. The SH has three local interfaces (Wi-Fi, Ethernet, and IEEE 802.15.4) and an Ethernet link to the (emulated) ISP network. The SLU and part of the SCN have been emulated with a virtual machine (PC at top-right of Figure 4). The used Smart Home devices are connected trhough the Ethernet, Wi-Fi and IEEE 802.15.4 interfaces of the SH. The attacks have been performed with a normal PC (center right in Figure 4).

The SH monitors all data traffic of the private network on all involved interfaces. Whenever SH detects an attack to some devices connected to the network, it generates an alert which is sent to the SLU.

Without loss of generality, we used the Bro Network Security Monitor [33] to monitor the traffic, with custom rules to detect the possible attacks used during the tests. Moreover, we have prepared a python3 script in order to parse the IDS file logs searching for warning/alarms. The script parses both Ethernet and Wi-Fi logs and, when a warning/alarm is found, contacts the SLU. In particular, the Bro alerts have been converted to an appropriate interexchange format (IDMEF) and sent to the SLU for further processing. In response to an alert, the SLU will send a command to the SH which will take appropriate actions according to the type of threat detected. A simplified and interactive visualization of the alert is also provided to the user through a graphical interface.

As mentioned earlier, the threat report could also not trigger any action of the SH in case the *Network Sentiment* for that particular user, according to that particular attack, is not changed (i.e., the attack is not relevant for the user). Nonetheless, the attack could be relevant for other users, and it is important to report its presence. For this reason, the SLU inserts the threat in the Shield database. In our experiment, the database is a MySQL db with customized tables.

The chosen hardware reflects as much as possible a normal Linux-based (CPE). As a consequence, we expect that implementing the SH functionalities on a commercial CPE will be very easy. In this case, the CPE becomes the central element of the Smart Home network, guaranteeing not only the device connectivity, but also the whole network security. However, it is also possible to use an external SH unit, provided that it can monitor the home network links (wired and wireless).

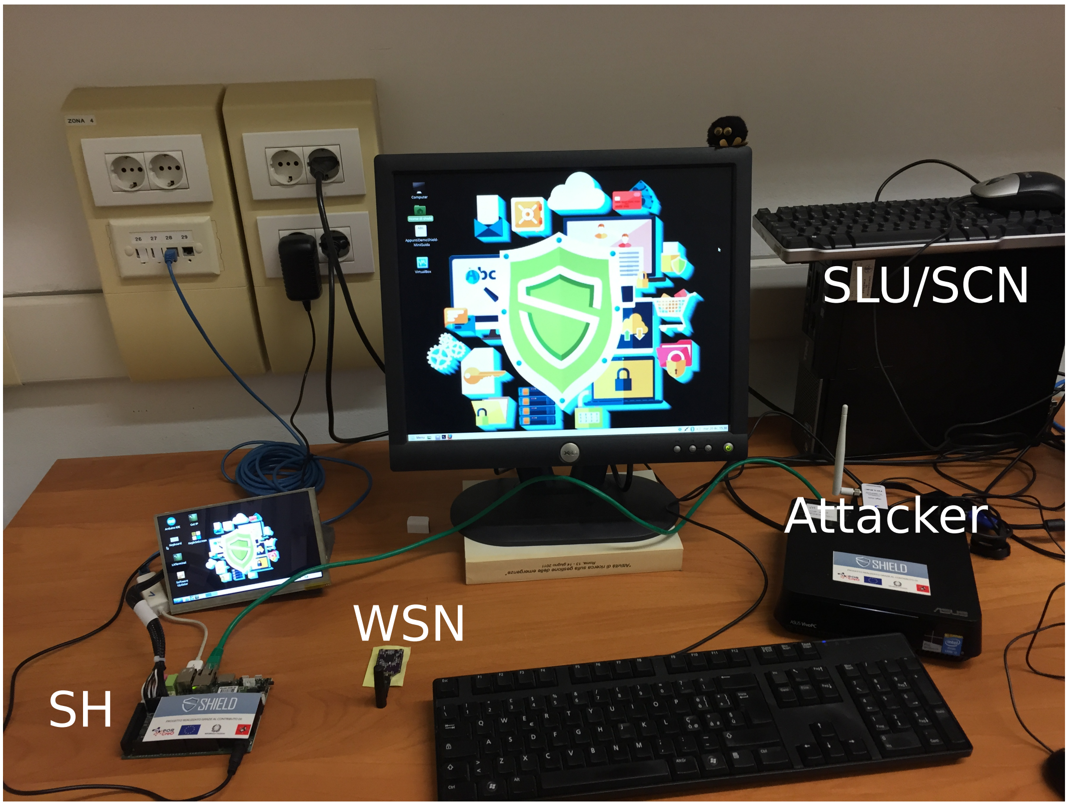


Figure 4. SHIELD test bed.

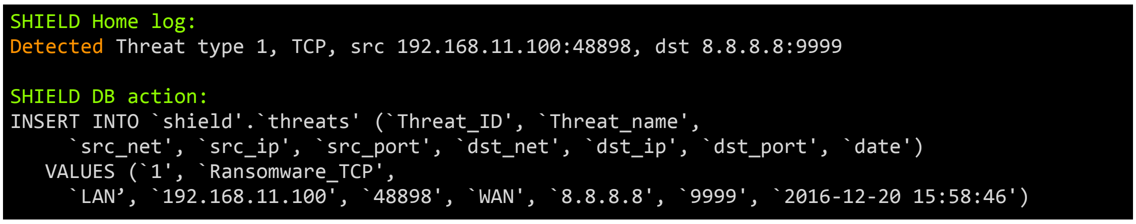
5.1. *Attacks*

To test the SHIELD system functionalities, we implemented three types of attacks: a ransomware, a port scan attack and an unauthorized access/query to the sensors via the CoAP.

5.1.1. Ransomware

To simulate the attack, we simulated a connection from a PC connected by Ethernet to an external host on a particular set of ports and with a given payload signature. The attack can use TCP, UDP, IPv4 or IPv6.

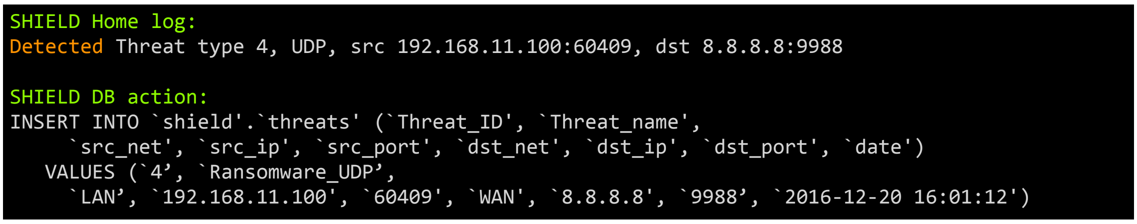
Figures 5 and 6 show, respectively, the detection of the two threats (ransomware on TCP and UDP) by the parser log. Once the threat is detected, the IDS sends an alert to the SLU. In this case, the reaction is to block the communication and promptly alert the user to take immediate actions.



```
SHIELD Home log:
Detected Threat type 1, TCP, src 192.168.11.100:48898, dst 8.8.8.8:9999

SHIELD DB action:
INSERT INTO `shield'.`threats' (`Threat_ID', `Threat_name',
     `src_net', `src_ip', `src_port', `dst_net', `dst_ip', `dst_port', `date')
   VALUES (`1', `Ransomware_TCP',
     `LAN’, `192.168.11.100', `48898', `WAN', `8.8.8.8', `9999', `2016-12-20 15:58:46')
```

Figure 5. Detection of Ransomware attack on TCP.



```
SHIELD Home log:
Detected Threat type 4, UDP, src 192.168.11.100:60409, dst 8.8.8.8:9988

SHIELD DB action:
INSERT INTO `shield'.`threats' (`Threat_ID', `Threat_name',
     `src_net', `src_ip', `src_port', `dst_net', `dst_ip', `dst_port', `date')
   VALUES (`4’, `Ransomware_UDP’,
     `LAN’, `192.168.11.100', `60409', `WAN', `8.8.8.8', `9988’, `2016-12-20 16:01:12')
```

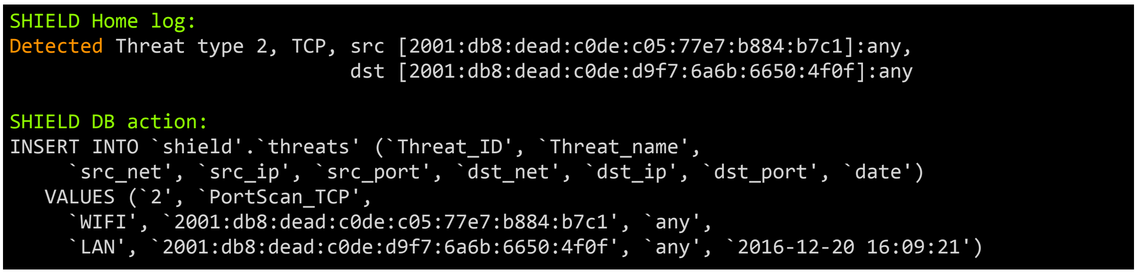
Figure 6. Detection of Ransomware attack on UDP.

5.1.2. Port Scanning

To simulate unauthorized intrusion, we performed a port scan on a LAN-connected host from a machine connected via the Wi-Fi. The command is:

```
# nmap -6 -sS --data-string deadbeef 2001:db8:dead:c0de::b981
```

Figure 7 shows the detection of the port scanning attack by the IDS and, consequently, the notification of the attack from the SH to the SLU. The reaction to this threat is twofold: the attacker is isolated (e.g., by disconnecting the terminal from the WiFi), and the SH configuration is updated to react to port scanning attacks. Moreover, the Network sentiment processor sends updated configurations to the geographically close SHs. The updated configurations will also include increased UDP port scan detection and an increased security against unauthorized access, for example by forcing a key refresh on all the wireless devices. The last action can be justified by assuming that the attacker gained access to the victim's Wi-Fi network and, by extension, could also try to attack the neighbor networks.



```
SHIELD Home log:
Detected Threat type 2, TCP, src [2001:db8:dead:c0de:c05:77e7:b884:b7c1]:any,
                             dst [2001:db8:dead:c0de:d9f7:6a6b:6650:4f0f]:any

SHIELD DB action:
INSERT INTO `shield'.`threats' (`Threat_ID', `Threat_name',
     `src_net', `src_ip', `src_port', `dst_net', `dst_ip', `dst_port', `date')
   VALUES (`2', `PortScan_TCP',
     `WIFI', `2001:db8:dead:c0de:c05:77e7:b884:b7c1', `any',
     `LAN', `2001:db8:dead:c0de:d9f7:6a6b:6650:4f0f', `any', `2016-12-20 16:09:21')
```

Figure 7. Detection of a port scan from an host in the Wi-Fi network.

5.1.3. IoT Devices Attacks

We focus more closely on the application layer to detect attacks against the normal operation rules of the CoAP protocol.

In 6LoWPAN network, CoAP was designed for resource-constrained devices with the goal of guaranteeing interoperability with the web. It uses UDP over IP as transport stack. A 4-byte fixed header and a compact encoding of options are taken on to reduce the transmission overhead by limiting the fragmentation on the link layer.

As previous shown in Section 2 the attacks on routing operations with RPL are analyzed mainly in literature although the using of security mechanism such as DTLS in CoAP (CoAPs) does not assure protection against DoS and other types of messages, e.g., malformed CoAP requests. As consequence attacks against the application layer can be underestimated.

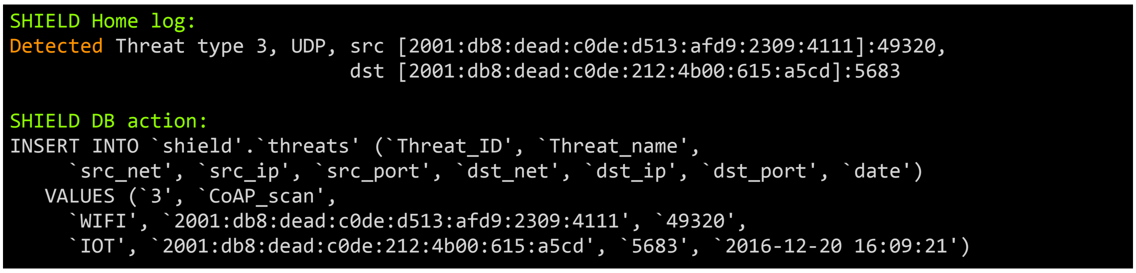
In this case, we consider an attacker that attempts to interrogate a sensor via the CoAP protocol [9], trying to read the device hardware and firmware characteristics. This kind of attack can have different outcomes, ranging from violation of the privacy, to the devices battery draining.

In our tests, the attacker would read the sensor temperature and the board firmware details:

```
# coap-client -v 5 coap://[v6addr]/sensor/temp
# coap-client -v 1 coap://[v6addr]/riot/board
```

where v6addr is `2001:db8:dead:c0de:7dfe:dff9:f7ff:ddf7`.

In Figure 8 the attack is detected by the IDS and through the SH sent to the SLU. The detection is triggered by the requests frequency and the suspicious request of the board firmware version. As a matter of fact, the user only needs this information when upgrading the node firmware, while for an attacker it represents an useful information to perform a targeted attack. The reaction includes a limitation on the requests from the specific user (rate limit), alerts to the authorized users about the suspicious activity, a more detailed analysis on the traffic from the attacker up to the advertisement to the SCN unit.



```
SHIELD Home log:
Detected Threat type 3, UDP, src [2001:db8:dead:c0de:d513:afd9:2309:4111]:49320,
                             dst [2001:db8:dead:c0de:212:4b00:615:a5cd]:5683

SHIELD DB action:
INSERT INTO `shield'.`threats' (`Threat_ID', `Threat_name',
     `src_net', `src_ip', `src_port', `dst_net', `dst_ip', `dst_port', `date')
   VALUES (`3', `CoAP_scan',
     `WIFI', `2001:db8:dead:c0de:d513:afd9:2309:4111', `49320',
     `IOT', `2001:db8:dead:c0de:212:4b00:615:a5cd', `5683', `2016-12-20 16:09:21')
```

Figure 8. Detection for IoT attack.

6. Conclusions

In this paper, we present an IoT security framework for the smart home environment. Our idea is to reach a dynamic security level for this smart infrastructure based on a *network sentiment analysis*. In the proposed architecture, smart gateway/firewalls at the ISP side and close to the user smart home cooperate to detect and react against different types of attacks from within the smart home network, i.e., the Wi-Fi, Ethernet world or from IoT devices. In particular, the user gateway did not have a predefined and fixed security level established when it was installed but can change its security rules and actions in reaction to the dynamic threat level measured by the SHIELD Logic Unit (SLU).

The two zones ISP and the smart home LAN cooperate in a unique integrated security framework. For example, if the smart home gateway (the IDS system) detects an attack, it reacts and the same information, distributed to the ISP, can be spread to the other gateways near to the smart home under attack (e.g., in a building we can consider a gateway for each smart home) to increase also their security and prevention level in a *social* security vision.

Our testbed validates the approach feasibility and that a simple CPE can easily perform all the required tasks to guarantee a Smart Home security.

The examples demonstrate that the SHIELD architecture allows a great flexibility on the kind of attacks to react to, without the installation of complex rules on the SH. Moreover, the *Network Sentiment* analysis allows the integration of behavioral, signature or hybrid based IDSs, enhanced by the knowledge of similarity-driven activity reports.

Future works will be oriented toward the design and evaluation of automatic attack correlation engines, in order to enhance the SLU sentiment analysis processor. In particular, machine learning algorithms are considered as potential candidates for the automatic interrelationship analysis between attacks and users relationships (physical or social).

Author Contributions: All the authors contributed equally to the paper. T.P. and L.P. mainly worked on the system architecture, while F.N. mainly worked on experiments.

Funding: The SHIELD Project funded by Tuscany Region FESR 2014–2020 and the project "GAUChO—A Green Adaptive Fog Computing and Networking Architecture" funded by Progetti di Ricerca di Rilevante Interesse Nazionale (PRIN) Bando 2015 supported this work.

Acknowledgments: The authors want to thanks L. Brilli for his technical support in the testbed setup.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

CN	Core Network
CPE	Customer Premises Equipment
CVE	Common Vulnerabilities and Exposures
DoS	Denial of Service
DDoS	Distributed Denial of Service
IDS	Intrusion Detection System
IoT	Internet of Things
IPS	Intrusion Prevention System
ISP	Internet Service Provider
LAN	Local Area Network
MiM	Man in the Middle
SLU	SHIELD—Logic Unit
SH	SHIELD—HOME
SCN	SHIELD—Core Network

References

1. Frenkel, S. A Cute Toy Just Brought a Hacker into Your Home. Available online: https://www.nytimes.com/2017/12/21/technology/connected-toys-hacking.html (accessed on 18 December 2018).
2. Gallagher, S. How One Rent-a-Botnet Army of Cameras, DVRs Caused Internet Chaos. Available online: https://arstechnica.com/information-technology/2016/10/inside-the-machine-uprising-how-cameras-dvrs-took-down-parts-of-the-internet/ (accessed on 18 December 2018).
3. Kolias, C.; Kambourakis, G.; Stavrou, A.; Voas, J. DDoS in the IoT: Mirai and Other Botnets. *Computer* **2017**, *50*, 80–84. [CrossRef]
4. Antonakakis, M.; April, T.; Bailey, M.; Bernhard, M.; Bursztein, E.; Cochran, J.; Durumeric, Z.; Halderman, J.A.; Invernizzi, L.; Kallitsis, M.; et al. Understanding the Mirai Botnet. In Proceedings of the 26th USENIX Conference on Security Symposium, SEC'17, Vancouver, BC, Canada, 16–18 August 2017; USENIX Association: Berkeley, CA, USA, 2017; pp. 1093–1110.
5. Lin, H.; Bergmann, N.W. IoT Privacy and Security Challenges for Smart Home Environments. *Information* **2016**, *7*, 44. [CrossRef]
6. Granjal, J.; Monteiro, E.; Silva, J.S. Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 1294–1312. [CrossRef]
7. Kim, H. Protection Against Packet Fragmentation Attacks at 6LoWPAN Adaptation Layer. In Proceedings of the 2008 International Conference on Convergence and Hybrid Information Technology, Daejeon, Korea, 28–30 August 2008; pp. 796–801.
8. Winter, T.; Thubert, P.; Brandt, A.; Hui, J.; Kelsey, R.; Levis, P.; Pister, K.; Struik, R.; Vasseur, J.P.; Alexander, R. RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks. Available online: http://www.rfc-editor.org/info/rfc6550 (accessed on 18 December 2018).
9. Shelby, Z.; Hartke, K.; Bormann, C. The Constrained Application Protocol (CoAP). Available online: https://www.rfc-editor.org/info/rfc7252 (accessed on 18 December 2018)).
10. Bormann, C.; Castellani, A.P.; Shelby, Z. CoAP: An Application Protocol for Billions of Tiny Internet Nodes. *IEEE Internet Comput.* **2012**, *16*, 62–67. [CrossRef]
11. Pierucci, L. The quality of experience perspective toward 5G technology. *IEEE Wirel. Commun.* **2015**, *22*, 10–16. [CrossRef]
12. Kambourakis, G. Anonymity and closely related terms in the cyberspace: An analysis by example. *J. Inf. Secur. Appl.* **2014**, *19*, 2–17. [CrossRef]
13. Lee, C.; Zappaterra, L.; Choi, K.; Choi, H.A. Securing smart home: Technologies, security challenges, and security requirements. In Proceedings of the 2014 IEEE Conference on Communications and Network Security, San Francisco, CA, USA, 29–31 October 2014; pp. 67–72.

14. Shin, D.; Sharma, V.; Kim, J.; Kwon, S.; You, I. Secure and Efficient Protocol for Route Optimization in PMIPv6-Based Smart Home IoT Networks. *IEEE Access* **2017**, *5*, 11100–11117. [CrossRef]
15. Shen, J.; Wang, C.; Li, T.; Chen, X.; Huang, X.; Zhan, Z.H. Secure data uploading scheme for a smart home system. *Inf. Sci.* **2018**, *453*, 186–197. [CrossRef]
16. Brilli, L.; Pecorella, T.; Pierucci, L.; Fantacci, R. A Novel 6LoWPAN-ND Extension to Enhance Privacy in IEEE 802.15.4 Networks. In Proceedings of the 2016 IEEE Global Communications Conference (GLOBECOM), Washington, DC, USA, 4–8 December 2016; pp. 1–6.
17. *IEEE Standard for Local and Metropolitan Area Networks—Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)*; IEEE Std 802.15.4-2011 (Revision of IEEE Std 802.15.4-2006); IEEE Std: Piscataway Township, NJ, USA, 2011; pp. 1–314.
18. Fuchsberger, A. Intrusion Detection Systems and Intrusion Prevention Systems. *Inf. Secur. Tech. Rep.* **2005**, *10*, 134–139. [CrossRef]
19. Gendreau, A.A.; Moorman, M. Survey of Intrusion Detection Systems towards an End to End Secure Internet of Things. In Proceedings of the 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), Vienna, Austria, 22–24 August 2016; pp. 84–90.
20. Bostani, H.; Sheikhan, M. Hybrid of anomaly-based and specification-based IDS for Internet of Things using unsupervised OPF based on MapReduce approach. *Comput. Commun.* **2017**, *98*, 52–71. [CrossRef]
21. Illiano, V.P.; Muñoz-González, L.; Lupu, E.C. Don't fool Me!: Detection, Characterisation and Diagnosis of Spoofed and Masked Events in Wireless Sensor Networks. *IEEE Trans. Depend. Secur. Comput.* **2017**, *14*, 279–293.
22. Zarpelão, B.B.; Miani, R.S.; Kawakani, C.T.; de Alvarenga, S.C. A survey of intrusion detection in Internet of Things. *J. Netw. Comput. Appl.* **2017**, *84*, 25–37. [CrossRef]
23. Raza, S.; Wallgren, L.; Voigt, T. SVELTE: Real-time intrusion detection in the Internet of Things. *Ad Hoc Netw.* **2013**, *11*, 2661–2674. [CrossRef]
24. Cugola, G.; Margara, A. Processing Flows of Information: From Data Stream to Complex Event Processing. *ACM Comput. Surv.* **2012**, *44*, 15. [CrossRef]
25. Zhang, K.; Liang, X.; Lu, R.; Shen, X. Sybil Attacks and Their Defenses in the Internet of Things. *IEEE Internet Things J.* **2014**, *1*, 372–383. [CrossRef]
26. Granjal, J.; Pedroso, A. An Intrusion Detection and Prevention Framework for Internet-Integrated CoAP WSN. *Secur. Commun. Netw.* **2018**, *2018*, 1753897. [CrossRef]
27. Pacheco, J.; Hariri, S. IoT Security Framework for Smart Cyber Infrastructures. In Proceedings of the 2016 IEEE 1st International Workshops on Foundations and Applications of Self* Systems (FAS*W), Augsburg, Germany, 12–16 September 2016; pp. 242–247.
28. Cruz, T.; Simões, P.; Monteiro, E.; Bastos, F.; Laranjeira, A. Cooperative security management for broadband network environments. *Secur. Commun. Netw.* **2015**, *8*, 3953–3977. [CrossRef]
29. Scarfone, K.A.; Mell, P.M. *Guide to Intrusion Detection and Prevention Systems (IDPS)*; Technical Report SP 800-94; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2007.
30. Fantacci, R.; Pecorella, T.; Viti, R.; Carlini, C. A network architecture solution for efficient IoT WSN backhauling: Challenges and opportunities. *IEEE Wirel. Commun.* **2014**, *21*, 113–119. [CrossRef]
31. Debar, H.; Curry, D.; Feinstein, B. The Intrusion Detection Message Exchange Format (IDMEF). Available online: https://www.rfc-editor.org/info/rfc4765 (accessed on 18 December 2018).
32. Martin, R.A. Managing vulnerabilities in networked systems. *Computer* **2001**, *34*, 32–38. [CrossRef]
33. The Bro Network Security Monitor. Available online: https://www.bro.org (accessed on 3 January 2017).