A Survey on Security and Privacy Issues in Internet-of-Things

Yuchen Yang, Longfei Wu, Guisheng Yin, Lijie Li, and Hongbin Zhao

***Abstract*—Internet-of-Things (IoT) are everywhere in our daily life. They are used in our homes, in hospitals, deployed outside to control and report the changes in environment, prevent fires, and many more beneficial functionality. However, all those benefits can come of huge risks of privacy loss and security issues. To secure the IoT devices, many research works have been conducted to countermeasure those problems and find a better way to eliminate those risks, or at least minimize their effects on the user's privacy and security requirements. The survey consists of four segments. The first segment will explore the most relevant limitations of IoT devices and their solutions. The second one will present the classification of IoT attacks. The next segment will focus on the mechanisms and architectures for authentication and access control. The last segment will analyze the security issues in different layers.**

***Index Terms*—Internet-of-Things (IoT), privacy, security, survey.**

I. Introduction

INTERNET-OF-THINGS (IoT) is a collection of "things" embedded with electronics, software, sensors, actuators, and connected via the Internet to collect and exchange data with each other. The IoT devices are equipped with sensors and processing power that enable them to be deployed in many environments. Fig. 1 presents a variety of common IoT applications, including smart home, smart city, smart grids, medical and healthcare equipment, connected vehicles, etc. The fast growth of the number of IoT devices utilized is predicted to reach 41 billion in 2020 with an $8.9 trillion market [1] as stated in the 2013 report of the International Data Corporation. The difference between IoT and the traditional Internet is the absence of Human role. The IoT devices can create information about individual's behaviors, analyze it, and take action [2]. Services provided by IoT applications offer a great benefit for human's life, but they can come with a huge price considering the person's privacy and security protection.

As the IoT manufacturers failed to implement a robust security system in the devices, security experts have warned the potential risk of large numbers of unsecured devices connecting to the Internet [3]. In December of 2013, a researcher at Proofpoint, an enterprise security firm, discovered the first IoT botnet. According to Proofpoint, more than 25% of the botnet was made up of devices other than computers, including smart TVs, baby monitors, and other household appliances. Recently, Dyn, Manchester, New Hampshire-based provider of domain name services, experienced service outages as a result of what appeared to be well coordinated attack [4]. On October 21, 2016, many websites including: Twitter, Netflix, Spotify, Airbnb, Reddit, Etsy, SoundCloud, and The New York Times, were reported inaccessible by users caused by a distributed denial of service attack (DDoS) attack using a network of consumer devices from the IoT.

Security and privacy remain huge issues for IoT devices, which introduce a whole new degree of online privacy concerns for consumers. That is because these devices not only collect personal information like users' names and telephone numbers, but can also monitor user activities (e.g., when users are in their houses and what they had for lunch). Following the never-ending string of disclosures about major data breaches, consumers are wary of placing too much personal data in public or private clouds, with good reason [5].

There are many published surveys on IoT security issues and challenges. Granjal *et al.* [6] analyzed existing solutions for the IoT standardized communication protocols (PHY, MAC, network, and application) and cross-layer mechanisms

Fig. 1. IoT applications.

Manuscript received December 22, 2016; revised April 4, 2017; accepted April 8, 2017. Date of publication April 17, 2017; date of current version October 9, 2017. This work was supported by the National Natural Science Foundation of China under Grant 61502116. *(Corresponding author: Lijie Li.)*

Y. Yang, G. Yin, L. Li, and H. Zhao are with the College of Computer Science and Technology, Harbin Engineering University, Harbin 150001, China (e-mail: yangyuchen521_1979@aliyun.com; yinguisheng@hrbeu.edu.cn; lilijie@hrbeu.edu.cn; z-hb@vip.sina.com).

L. Wu is with the Department of Computer and Information Sciences, Temple University, Philadelphia, PA 19123 USA (e-mail: longfei.wu@temple.edu).

Digital Object Identifier 10.1109/JIOT.2017.2694844

whenever applicable. Sicari *et al.* [7] presented research challenges and the current solutions in the field of IoT security focusing on the main security issues which were identified in eight categories: 1) authentication; 2) access control; 3) confidentiality; 4) privacy; 5) trust; 6) secure middleware; 7) mobile security; and 8) policy enforcement. They raised some open issues, and suggesting some hints for future research. Roman *et al.* [8] focused on the analysis of the centralized and distributed approaches. They introduced an attacker model that was applied to both centralized and distributed IoT architectures, and studied the main challenges and promising solutions in the design and deployment of the security mechanisms.

In this survey paper, we explore the IoT security and privacy issues in four aspects. The first part presents the most relevant limitations of IoT devices and their solutions. The second part discusses the classification of existing IoT attacks. Then, we explore the IoT authentication and access control schemes and architectures proposed in recent literature. Finally, we analyze the security issues and mechanisms in the perception layer, network layer, transport layer, and application layer, respectively.

II. IoT Device Limitations

Why is it difficult to secure and apply security features to IoT as those used in traditional Internet? Trappe *et al.* [9] presented the issue of IoT constraints, and their effects on using current cryptographic tools as the ones utilized in traditional Internet. The two main limitations are the battery capacity and computing power.

A. Battery Life Extension

As some IoT devices are deployed in environments where charging is not available, they only have a limited energy to execute the designed functionality and heavy security instructions can drain the devices' resources. Three possible approaches can be used to mitigate this issue. The first is to use the minimum security requirements on the device, which is not recommended especially when dealing with sensitive data. The second approach is to increase the battery capacity. However, most IoT devices are designed to be lightweight and in small size. There is no extra room for a larger battery. The final approach is to harvest energy from natural resources (e.g., light, heat, vibration, and wind), but this type of approach would require an upgrade to the hardware and significantly increase the monetary cost.

B. Lightweight Computation

The paper [9] mentioned that conventional cryptography cannot work on IoT systems, since the devices have limited memory space which cannot handle the computing and storage requirements of advanced cryptography algorithms. To support security mechanisms for the constrained devices, the authors suggested reusing existing functions. An example is to use physical layer authentication by applying signal processing at the receiver side to verify whether a transmission came from the expected transmitter in the expected location. Alternatively, a specific analog characteristics of a transmitter can be used to effectively encode analog information. These analog nuances cannot be predicted or controlled in manufacturing, and can serve as a unique key. This way of authentication has little or no energy overhead because it takes advantage of radio signals.

Shafagh *et al.* [10] proposed an encrypted query processing algorithm for IoT. The approach allows to securely store encrypted IoT information on the cloud, and supports efficient database query processing over encrypted data. Specifically, they utilize alternative lightweight cryptographic algorithms that replace additive homomorphic encryption and order-preserving encryption with Elliptic Curve ElGamal and mutable order preserving encoding algorithms, where they made some changes to suit the computation limitations of IoT devices. The system scheme replaces the Web application communication with an end-to-end (E2E) system that stores encrypted data from personal devices on cloud database, and data encryption/decryption is performed at the client-side. The keying material will only reside in the personal device, and the need of a trusted proxy which has access to all the secret keys is eliminated. The system architecture includes three main parties: 1) IoT devices; 2) users; and 3) the cloud. The application data can be stored in the cloud by directly uploading it by the smart device or via a gateway like a wearable device. The paper addressed only some encryption schemes that support the most used queries in IoT data processing. However, the design can be extended to cover more schemes. The experiment results showed an improvement in the time performance compared to existing schemes.

Kotamsetty and Govindarasu [11] proposed an approach to reduce latency for IoT when performing query processing over encrypted data by applying latency hiding technique, which consists of breaking down the query results of large size into small sized data sets. This allows computational work to be performed on a set of data while fetching the remaining encrypted information. To decide the appropriate data size to be requested in each iteration in order to minimize the latency, the study proposed an algorithm that starts with an initial data size and adoptively adjust the size to minimize the gap between computation and communication latencies in each iteration. The algorithm has two variants: the first starts with a size that is a fraction of the large query size. In the second variant, the starting size is fixed. The experiment results demonstrated that the proposed approach outperforms existing solutions in terms of latency for queries with larger data size.

Salami *et al.* [12] proposed a lightweight encryption scheme for smart homes based on stateful identity-based encryption (IBE), in which the public keys are merely identity strings without the need for a digital certificate. This method is known as Phong, Matsuka, and Ogata's stateful IBE scheme. It is the combination of IBE and stateful Diffie-Hellman encryption scheme. To add more efficiency to the proposed scheme and reduce the communication cost, the research study divides the encryption process into key encryption and data encryption, with the focus on the second one, because the size of ciphertexts produced by key encryption is larger than the one resulted from the data encryption. This division led to two-sub algorithms: 1) KEYEncrypt and 2) DATAEncrypt. The first

is for encrypting a session key, and the second is for data encryption. The resulted ciphertext from the sub algorithms is transmitted separately in a way that data ciphertexts are transmitted many times without attaching the key ciphertext. The evaluation results showed that the proposed scheme is secure against plaintext attacks. Also, the performance analysis showed that it outperforms the regular IBE scheme in terms of speeding up the encryption operations, and reducing approximately one-third of communication overhead.

III. Classifications on IoT Attacks

Previous survey works have conducted comprehensive studies on IoT security. They have provided insightful classifications of IoT attacks and solutions.

Andrea *et al.* [13] come up with a new classification of IoT devices attacks presented in four distinct types: 1) physical; 2) network; 3) software; and 4) encryption attacks. Each one covers a layer of the IoT structure (physical, network, and application), in addition to the IoT protocols for data encryption. The physical attack is performed when the attacker is in a close distance of the device. The network attacks consist of manipulating the IoT network system to cause damage. The software attacks happen when the IoT applications present some security vulnerabilities that allow the attacker to seize the opportunity and harm the system. Encryption attacks consist of breaking the system encryption. This kind of attacks can be done by side channel, cryptanalysis, and man-in-the-middle attacks. They also presented a multilayered security approaches to address the IoT structure layers and encryption system vulnerabilities and security issues. Based on the study, to countermeasure the security problems at the physical layer, the device has to use secure booting by applying a cryptographic hash algorithms and digital signature to verify its authentication and the integrity of the software. Also, a new device must authenticate itself to the network before any transmission or reception of data. In addition to that, a device should carry an error detection system, and all of its information has to be encrypted to maintain data integrity and confidentiality. At the network layer, authentication mechanisms and point-to-point encryption can be used to ensure data privacy and rooting security. The application layer can also provide security by means of authentication, encryption, and integrity verification, which allows only the authorized users to access data through control lists and firewalls, in addition to the use of anti-virus software.

Ronen and Shamir [14] introduced a new taxonomy classification for IoT attacks based on how the attacker features deviates from the legitimate IoT devices. The categories are presented in: ignoring, reducing, misusing, and extending the system functionality. The study focused on the functionality extension attacks on smart lights. The paper presented two attacks: the first one consisted of creating a covert channel to capture confidential information from an organization building that implemented smart lights which are connected to the internal sensitive network. The work is done by using an optical receiver that could read the data from a distance of over 100 m by measuring the exact duration and frequency of the small changes in the lights intensity. The second attack showed that an attacker can use those lights to create strobes in the sensitive light frequencies, which can lead to a risk of epileptic seizures. The experiments showed that it is necessary to focus on security issues during the different phases of designing, implementing and integrating of the IoT devices.

IV. IoT Authentication and Access Control

A. IoT Authentication Scheme

Salman *et al.* [15] proposed a new IoT heterogeneous identity-based authentication scheme by applying the concept of software defined networking (SDN) on IoT devices. SDN can be deployed using fog-distributed nodes. Each set of devices is communicating with a gateway that can support authentication for the things. These gateways are also connected to a central controller which has access to the central data. The authentication process has to go through the gateway and then the controller in order to give access to the things. The message flow between the three levels: 1) things; 2) gateway; and 3) the controller, happens in three phases. The first phase consists of obtaining an authentication certificate for the gateway from a controller. Phase two consists of things registration to the gateway. The final phase is the authentication request which is sent from the IoT device to the gateway. The experimental evaluation shows that the proposed scheme is immune to masquerade attack, man-in-the-middle attack, and replay attack.

Porambage *et al.* [16] proposed and designed a pervasive authentication protocol and a key establishment scheme for the resource constrained wireless sensor networks (WSNs) in distributed IoT application, called PAuthKey. The proposed PAuthKey protocol comprises two phases: 1) registration phase for obtaining cryptographic credentials to the edge devices and end users and 2) authentication phase for authentication and key establishment in mutual communication. With PAuthKey protocol, end-users can authenticate themselves to the sensor nodes directly and acquire sensed data and services. The protocol supports the distributed IoT applications, since the certificates are lightweight and can be handled by the high resource constrained devices, irrespective of their originality.

Ho *et al.* [17] studied the security vulnerabilities of smart locks by observing five types of locks: 1) August; 2) Danalock; 3) Kevo; 4) Okidokeys; and 5) Lockitron. The paper focused on the consequence of the door's automatic unlocking system. Some locks have the capability to unlock the door if the owner is located in a certain distance from the door. This feature allows to open the door even if the owner does not have the intent for the action to occur, especially, when the person is inside the home. This can create an insecure feeling for the resident and allows the attacker to seize the opportunity and enter the home when the owner is around without his/her permission. To countermeasure this vulnerability, the study proposed a touch-based intent communication solution that prevents locks to unlock the door without the owner intent to do it. In this solution, the authorized user has to wear a special wearable device that communicate with the lock via an ear bone conduction microphone. A hand-held vibrator is

used to transmit the intent signal. The wearable device will detect the vibration and send an unlock command. The results showed that the system unlocks only when it detects the person's action, and it did not react to the vibration caused by any of daily activities such as computer tone and phone vibration; however, the solution presented some limitations like the addition of hardware to the smart lock, and the wearable device to be able to transmit the vibrations. Also, the vibration sensor may not detect the intent action if the wearable device is loosen, or the user is touching the door with the hand which is not wearing the device.

Sharaf-Dabbagh and Saad [18] proposed a new approach for authentication process using the device's unique fingerprint. According to the study, each device has a unique fingerprint which consists of multiple features such as location, physical state of object, or transmitter state. A group of IoT objects may have different types of fingerprinting features. For that reason, conventional device fingerprinting techniques cannot be used for the IoT object's authentication. The paper proposed the use of transfer learning, to authenticate devices that have different feature spaces. To apply the new idea, the research study followed two-fold approach. First, it verifies if the message is sent by a single object. Then, it validates the legitimacy of the sending device. To realize the first phase, the paper adopted the infinite Gaussian mixture mode (IGMM) as a generative model assuming that the fingerprints for each object follow a multivariate Gaussian distribution. The second phase was done by comparing the clustering results from the IGMM with the expected cluster shape for the device. This was done by applying Bhattacharyya distance. However, the environment can cause changes in some devices' fingerprint features. To solve this issue, the study applied transfer learning techniques to differentiate between normal changes due to the environment effects, from the malicious changes produced by attackers. This is done under two assumptions. The first is that the changes can affect more than an object at the same time, and the second is that an attacker cannot target all objects affected by the environment. The test results of the proposed authentication approach showed an increase in the authentication performance compared to conventional authentication techniques.

Zhang and Green [19] proposed an algorithm to defend against DDoS attacks by considering a network composed of four groups of nodes: 1) working node; 2) monitoring node; 3) legitimate user node; and 4) the attacker node. The algorithm proposed consists of addressing each node's DDoS security issues in the network. The working nodes are considered as the devices that collect information and execute simple tasks. They have memory computation, storage, and energy limitations. To countermeasure the DDoS attack, the working node has to differentiate between malicious requests and legitimate ones. A sender that sends the same content messages will be flagged and saved in a list of served requests to check for further attacker requests. The list has to be of small size due to the devices' space constraint. A legitimate user node has to send request with lower frequency and reasonable content. A monitoring node is included in the scheme for future work implementation. The node will be responsible for storing the old records of attackers in order to prevent the working nodes from serving the malicious attacks. In the proposed algorithm, an attacker's request has only one chance to be served. After the second attempt, the attacker is put in the attacking list, and its packets will be dropped. The study simulation results showed that the algorithm is effective for detecting and preventing DDoS.

Bouij-Pasquier *et al.* [20] proposed an authorization access control model called SmartOrBAC that extends the organization-based access control (OrBAC) model to fit the IoT network requirements by including collaboration-related and context aware concepts, and dividing the IoT network structure into four abstraction layers: 1) constrained; 2) less constrained; 3) organization layer; and 4) collaboration layer across domain access control, with a central authorization engine for each separate group of components within a specific layer. The constrained layer, as its name says, contains devices with constrained capabilities. A less constrained device is associated to a group of the first layer components to take in charge the intensive computation tasks within the same security domain. This central element of the less constrained layer is referred as client authorization engine, on the client side, and resource authorization engine, on the source side. The organization layer specifies the security access policies for each group of the client and the resource organization. It also structures them into different security domains. The fourth layer comes to enhance the OrBAC access model with the addition of collaboration related concepts. This added layer is responsible for establishing agreements and rules cross the domain access control. The evaluation of the presented model showed that it is less complex that the capabilities-based models. It also ameliorates the security policy management cost, and reduces the risks of errors.

B. IoT Authentication Architecture

Dos Santos *et al.* [21] proposed an architecture for secure communication between constrained IoT devices using Datagram Transport Layer Security (DTLS) based on certificates with mutual authentication. The communication is done by introducing a new device called IoT security provider (IoTSSP), which is responsible for managing and analyzing the devices' certificates along with authentication and session establishment between the devices. The infrastructure could be composed by one or more IoTSSPs. Each one is responsible for a set of constrained devices. Optional handshaking delegation, and transfer of session are the two new main mechanisms that are introduced in the study. The first mechanism consists of delegating the handshaking process to the IoTSSP upon the reception of a client request for authentication to communicate with a constrained device. The handshaking execution module in IPv6 over low power wireless personal area networks border router redirect the message to the IoTSSP, which replies to the Internet device to verify its request. It then communicates the message to the constrained device and check for its availability. This process also prevents DoS attacks. After the authentication process is finished, the second mechanism will take place by using a DTLS extension called session transfer

ticket that transfer a secure communication session to the constrained device, which will receive all the parameters of the active session defined in the IoTSSP.

The proposed solution in [22] is based on a lightweight key agreement protocol, the IBE, and pseudonym-based encryption to ensure anonymity, data secrecy, and trust between IoT or WSN nodes in the network. Their architecture consists of a base station (BS), a sink node (SN), and a set of nodes (N). The BS contains the PKG server where the nodes' IDs are stored. Their solution requires that all the messages to be transmitted to the SN which then send them to their final destination, and each transmission is acknowledged by an ACK message. The encrypted data will incur a message authentication code function before sending the message. Also, in order to obscure a sent message with an ACK message, the study proposed that both messages will have the same length. Another requirement is that a shared session key should be established between N node and SN, and between SN and BS. Each node N should use a virtual ID and apply PBC technique. Four phases need to be followed to establish the proposed system model. The first step is the network setup, which is also divided in three steps to setup the system's security parameters. These steps consists of configuring the PKG in the BS node, and the SN and N nodes parameters. The second phase highlights the mechanisms that ensures both SN and N nodes are legitimate devices in the network. The third and fourth phase is the establishment of session keys between N node and SN, and between SN and BS. The proposed solution was shown to be resistant to most known attacks in the WSN and IoT. The results also showed an improvement in security and privacy preservative performance.

Yoshigoe *et al.* [23] proposed a way to hide real network traffic with synthetic packet-injection framework, thus making traffic analysis difficult for hackers. The framework consists of a synthetic packet engine (SPE) that generates and inject additional packets to the network whenever needed. These false packets mimic the behavior of real actions, like opening a door, which is followed by the action of locking the door after a few seconds. The SPE can be incorporated with the use of a VPN, which can encrypt the data and hide the packets sequence number that can distinguish between real traffic and the injected ones. The SPE can also be integrated as a part of both the client and the server process. This combination can be applied to application that does require immediate response from the server, which is not supported when using the SPE with the VPN.

The object security approaches (i.e., placing security within the application payload) have also been considered as a viable option to provide fine grained access control with an assertion-based authorization framework. Seitz *et al.* [24] addressed the authorization and access control issues in the context of interconnected systems consisting of resource constrained devices not directly operated by humans. This requires the device to be able to handle connections from other entities, distinguish between requests from different entities, and enforce respective fine-grained authorization decisions. In the proposed authorization framework, the decisions are based on local data and device's local conditions, which adds significant flexibility to the access control models that can be supported.

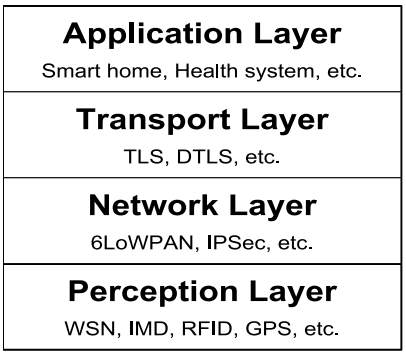


Fig. 2. IoT layered analysis.

To address the limitations of existing connection-oriented security architecture in terms of the scale and resulting latency on small constrained IoT devices, Vučinić *et al.* [25] proposed an object-based security architecture (OSCAR) that leverages the security concepts both from content-centric and traditional connection-oriented approaches. They used the secure channels established by means of DTLS for key exchange, and provided a mechanism to protect from replay attacks by coupling with the constrained application protocol (CoAP) application protocol. OSCAR intrinsically supports caching and multicast, and does not affect the radio duty-cycling operation of constrained objects. The experimental evaluation shows that OSCAR can achive significant energy savings at constrained servers and reasonable delays.

Cirani *et al.* [26] proposed an architecture IoT-OAuth-based authorization service (OAS) targeting HTTP/CoAP services to provide an authorization framework, which can be integrated by invoking an external OAS. The IoT-OAS architecture is meant to be flexible, highly configurable, and easy to integrate with existing services. By delegating the authorization functionality, IoT-OAS achieves benefits including lower processing load with respect to solutions (where access control is implemented on the smart object), fine-grained (remote) customization of access policies, and higher scalability (without the need to operate directly on the device).

V. IoT Security at Different Layers

Applying existing Internet standards to smart devices can simplify the integration of the envisioned scenarios in the IoT contexts. However, the security mechanisms in conventional Internet protocols need to be modified or extended to support the IoT applications. In this section, we discuss the security problems and existing solutions in different layers of IoT systems (Fig. 2).

A. IoT Perception Layer Security

IoT system is designed to collect and exchange data from the physical world. Hence, the perception layer contains various types of collecting and controlling modules, such as the temperature sensors, sound sensors, vibration sensors, pressure sensors, etc. The perception layer can be further divided into two parts: perception node (sensors or controllers, etc.), perception network that communicates with transportation network [27]. Perception node is used for data acquisition

and data control, perception network sends collected data to the gateway, or sends control instruction to the controller. Perception layer technologies include WSNs, implantable medical devices (IMDs), radio-frequency identification, global positioning system, etc.

One perception layer security issue is the detection of the abnormal sensor node. This could happen when the node is physically attacked (e.g., destroyed and disabled) or intruded/compromised by cyber attacks. These nodes are named as faulty nodes in general. In order to ensure the quality of service, it is necessary to be able to detect the faulty nodes and take actions to avoid further degradation of the service. Chen *et al.* [28] proposed and evaluated a localized fault detection algorithm to identify the faulty nodes in WSN. Da Silva *et al.* [29] proposed a decentralized intrusion detection system model for the WSN. Wang *et al.* [30] derived the intrusion detection probability in both homogeneous and heterogeneous WSN.

Another perception layer security concern is the cryptography algorithms and key management mechanism to be used. Public key algorithm has been considered convenient for node authentication. It has larger scalability and can better secure the entire network without complicated key management protocol [27]. According to Gaubatz *et al.* [31], three low-power public key encryption algorithms are the most promising candidates for WSNs: Rabin's scheme, NtruEncrypt, and elliptic curve cryptography. Key management includes secret key generation, distribution, storage, updating, and destruction. Existing key distribution scheme can be divided into four groups: 1) key broadcast distribution [32], [33]; 2) group key distribution [34], [35]; 3) master key predistribution; and 4) pairwise key distribution [36], [37].

Some IoT users have privacy concerns when submitting sensitive data to the collection server. It is very important to anonymize the data before submission so that the collector cannot trace back to the submitter. The anonymous data aggregation has been studied in many previous works [38]–[42]. A recent work by Yao *et al.* [43] proposed an efficient anonymous data reporting protocol for the participatory sensing in IoT applications. The protocol consists of a slot reservation stage and a message submission stage. In the slot reservation stage, a group of N users assign each other a message slot in a vector as the message submission schedule, each user's slot is oblivious to others and the aggregator. In the message submission stage, each user transmits an encoded data to the aggregator based on the slot information known only to herself, while the aggregator cannot link the received data to a specific user. With the proposed data reporting protocol, the link between the received data and the contributor is broken, so that user privacy is protected.

IMD is a new type of IoT device that is implanted within human body for diagnostic, monitoring, and therapeutic purposes. It is imperative to ensure the security of IMDs since even a small vulnerability can cause fatal threat to patient's life. However, in recent years, several attacks have been demonstrated to be able to successfully compromise a number of commercial IMD products.

Halperin *et al.* [44] presented the vulnerabilities of a commercial implantable cardioverter defibrillator (ICD). Equipped with an oscilloscope and a software radio, they managed to reverse-engineer the ICD's communications protocol and obtain the personal information of the patient and the ICD. Furthermore, they also launched active attacks to change the therapy settings and drain the battery more rapidly. Similarly, eavesdropping attacks and active attacks can also compromise commercial glucose monitoring and insulin delivery system [45]–[47]. After reverse-engineering the communication protocol and packet format, they were able to impersonate the doctor and alter the intended therapy by replaying and injecting messages with a software radio. A security professional Jack [48] has also revealed serious security flaws in IMDs, and demonstrated how an adversary can remotely take full control of insulin pump, pacemaker, and ICD. The IMD manufacturers should be responsible for the security incidents and vulnerabilities in their products. However, they tend to be unwilling to include strong security mechanisms into their products since these changes will result in an additional monetary cost and a reduction in service life.

In 2014, an independent security researcher Billy Rios discovered 100 vulnerabilities in the communications system of the PCA 3 Lifecare infusion pump, produced by the medical device company Hospira (HSP). These vulnerabilities allow a hacker to tap into the pumps and change the original amount of medication set to dispense. Rios notified HSP, but the company failed to respond to him. HSP stayed silent on the issue until another researcher Jeremy Richards publicly disclosed the threat in April 2015 [49]. Then, the U.S. Food and Drug Administration and the Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team sent out advisories notifying hospitals of the danger of HSP pumps, and encouraging the transition to alternative infusion systems [50].

Many research efforts have been focused on the access control for IMDs [51]–[57] and the mitigation of resource depletion attacks [58], [59].

B. IoT Network Layer Security

For IoT devices in WSN context, it is desirable to extend IPv6 over low power wireless personal area networks (6LoWPAN) to enable IPSec communication with IPv6 nodes. This is beneficial because the existing end-points on the Internet do not need to be modified to communicate securely with the WSN, and the true E2E security is implemented without the need for a trustworthy gateway. Raza *et al.* [60] proposed an E2E secure communication between IP enabled sensor networks and the traditional Internet. Their extension of LoWPAN supports both IPSec's authentication header and encapsulation security payload (ESP), so that the communication endpoints are able to authenticate, encrypt and check the integrity of messages using standardized and established IPv6 mechanisms. They extended their previous work in [61]. They described ESP for 6LoWPAN/IPSec in detail, and compared the 6LoWPAN/IPSec solution with the commonly employed 802.15.4 link-layer security. A thorough testbed performance evaluation of the 6LoWPAN/IPSec solution and 802.15.4 security is built, which reuses the crypto hardware within existing IEEE 802.15.4 transceivers for 6LoWPAN/IPSec.

Granjal *et al.* [6] proposed a new secure interconnection model and security mechanisms to enable the secure integration of IP enabled WSNs with the Internet, and allow for E2E security. Their model introduces 6LoWPAN security headers to enable E2E security between sensor nodes and hosts on the Internet, while also providing mechanisms to selectively control the energy expended with security operations on the WSN.

Jara *et al.* [62] provided an analysis of the requirements and desirable features for the mobility support in the IoT, and proposed an efficient solution for constrained environments based on Mobile IPv6 and IPSec. This paper has considered the suitability of Mobile IPv6 and IPSec for constrained devices, and analyzed, designed, developed, and evaluated a lightweight version of Mobile IPv6 and IPSec. The proposed solution of lightweight Mobile IPv6 with IPSec is aware of the requirements of the IoT and presents the best solution for dynamic ecosystems in terms of efficiency and security adapted to IoT-devices capabilities.

C. IoT Transport Layer Security

Kothmayr *et al.* [63] presented the first fully implemented two-way authentication scheme for the IoT system, based on existing Internet standards, especially the DTLS protocol. The proposed security scheme is performed during a fully authenticated DTLS handshake and based on an exchange of X.509 certificates containing RSA keys. It can work over standard communication stacks that offer UDP/IPv6 networking for 6LoWPANs.

Raza *et al.* [64] proposed 6LoWPAN header compression for DTLS. They linked the compressed DTLS with the 6LoWPAN standard using standardized mechanisms. The proposed DTLS compression significantly reduces the number of additional security bits. For example, only for the DTLS Record header that is added in every DTLS packet, the number of additional security bits can be reduced by 62%. In their follow-up work [65], an integration of DTLS and CoAP is proposed for the IoT, named Lithe. They also proposed a novel DTLS header compression scheme that aims to significantly reduce the energy consumption by leveraging the 6LoWPAN standard. The proposed DTLS header compression scheme does not compromise the E2E security properties provided by DTLS, and can considerably reduce the number of transmitted bytes while maintaining DTLS standard compliance.

Brachmann *et al.* [66] pointed out that security protocols such as TLS or DTLS adopted on the Internet does not necessarily mean that the same security levels can be achieved in low-power and lossy network (LLN), which is still vulnerable to resource exhaustion, flooding, replay, and amplification attacks, since the 6LoWPAN border router typically does not perform any authentication. The authors presented two approaches to mitigate such attacks. The first is to map the TLS to DTLS protocol to ensure E2E security at the application layer. The second approach is to use DTLS-DTLS tunnel to protect the LLN.

Hummen *et al.* [67] investigated the use of certificates for peer authentication in the Web of things. Preliminary overhead estimations are conducted for the certificate-based DTLS handshake. The authors proposed three design ideas to reduce the overheads of the DTLS handshake, based on prevalidation, session resumption, and handshake delegation, respectively.

D. IoT Application Layer Security

IoT has a wide variety of applications, including but not limited to smart home (e.g., learning thermostat, smart bulb), medical and healthcare (e.g., real-time health monitoring system), smart city (e.g., smart lighting, smart parking), energy management (e.g., smart grids, smart metering), environmental monitoring (e.g., climate monitoring, wildlife tracking), industrial Internet, and connected vehicle.

Most modern IoT devices contain configurable embedded computer systems. Some are even running complex software and resembling general-purpose computers, hence they face the same security risks as that of general-purpose computers. When connected to the Internet, they could get infected by computer virus like trojan.

The IoT is creating a new environment where malware can be used to create powerful botnets. Mirai [68], a newly discovered piece of Linux malware, is being used to rope IoT devices into botnets. Mirai can gain shell access using the default password of the telnet or SSH accounts. After it obtains access to the account, it can create delayed processes, delete files, and even install other malware on the system. The infected devices were secretly under Mirai's control and awaiting orders to strike in the form of a DDoS attack. The vast Internet outage in October 2016 was caused by the DDoS attack using compromised IoT devices running the Mirai malware.

Later, security researchers at MalwareMustDie have discovered another malware family IRCTelnet, also designed to infect Linux-based insecure IoT devices and turn them into a botnet to carry out massive DDoS attacks [69]. Similar to Mirai malware, IRCTelnet also relies on default hard-coded passwords. It compromises an IoT device by brute-forcing its Telnet ports and infecting the device's operating system. Then, the IoT device becomes a node of the botnet network, which can be controlled through Internet relay chat, an application layer protocol that enables communication in text. The DDoS attacks in IoT and WSN contexts have been well-studied in [19] and [70]–[74].

VI. Conclusion

In this survey, we have presented the security and privacy issues in IoT applications and systems. We presented the limitations of IoT devices in battery and computing resources, and discussed possible solutions for battery life extension and lightweight computing. We also studied existing classification approaches for IoT attacks and security mechanisms. Then, we reviewed the recently proposed IoT authentication schemes and architectures. The last part of this paper analyzed the security issues and solutions in four layers, including the perception layer, network layer, transport layer, and application layer.

Overall, the safety of commercial IoT devices today depends on the technologies, protocols, and security mechanisms implemented by each individual manufacturer. Based on the specific case, all IoT devices could be vulnerable to certain types of attacks. This indicates the urgent needs of developing general

security policy and standards for IoT products. IoT manufacturing industry has to work closely with the supervisory agencies, such as FSA and DHS, and the standardization organizations to tackle newly emerged threats as well as to develop strong and robust security standards for IoT devices and systems.

REFERENCES

[1] IoT Analytics. (2014). *Why the Internet of Things Is Called Internet of Things: Definition, History, Disambiguation*. [Online]. Available: https://iot-analytics.com/Internet-of-things-definition/

[2] I. Saif, S. Peasley, and A. Perinkolam. (2015). *Safeguarding the Internet of Things: Being Secure, Vigilant, and Resilient in the Connected Age*. [Online]. Available: https://dupress.deloitte.com/dup-us-en/deloitte-review/issue-17/Internet-of-things-data-security-and-privacy.html

[3] M. Rouse. (2013). *IoT Security (Internet of Things Security)*. [Online]. Available: http://internetofthingsagenda.techtarget.com/definition/IoT-security-Internet-of-Things-security

[4] B. Lam and C. Larose. (2016). *How Did the Internet of Things Allow the Latest Attack on the Internet?* [Online]. Available: https://www.privacyandsecuritymatters.com/2016/10/how-did-the-Internet-of-things-allow-the-latest-attack-on-the-Internet/

[5] Talkin Cloud. (2016). *IoT Past and Present: The History of IoT, and Where It's Headed Today*. [Online]. Available: http://talkincloud.com/cloud-computing/iot-past-and-present-history-iot-and-where-its-headed-today?page=2

[6] J. Granjal, E. Monteiro, and J. S. Silva, "A secure interconnection model for IPv6 enabled wireless sensor networks," in *Proc. IFIP Wireless Days*, Venice, Italy, Oct. 2010, pp. 1–6.

[7] S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Comput. Netw.*, vol. 76, pp. 146–164, Jan. 2015.

[8] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed Internet of Things," *Comput. Netw.*, vol. 57, no. 10, pp. 2266–2279, 2013.

[9] W. Trappe, R. Howard, and R. S. Moore, "Low-energy security: Limits and opportunities in the Internet of Things," *IEEE Security Privacy*, vol. 13, no. 1, pp. 14–21, Jan./Feb. 2015.

[10] H. Shafagh, A. Hithnawi, A. Droescher, S. Duquennoy, and W. Hu, "Poster: Towards encrypted query processing for the Internet of Things," in *Proc. 21st Annu. Int. Conf. Mobile Comput. Netw. (MobiCom)*, Paris, France, 2015, pp. 251–253.

[11] R. Kotamsetty and M. Govindarasu, "Adaptive latency-aware query processing on encrypted data for the Internet of Things," in *Proc. 25th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Aug. 2016, pp. 1–7.

[12] S. A. Salami, J. Baek, K. Salah, and E. Damiani, "Lightweight encryption for smart home," in *Proc. 11th Int. Conf. Availability Reliability Security (ARES)*, Salzburg, Austria, Aug. 2016, pp. 382–388.

[13] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Larnaca, Cyprus, Jul. 2015, pp. 180–187.

[14] E. Ronen and A. Shamir, "Extended functionality attacks on IoT devices: The case of smart lights," in *Proc. IEEE Eur. Symp. Security Privacy (EuroS P)*, Saarbrücken, Germany, Mar. 2016, pp. 3–12.

[15] O. Salman, S. Abdallah, I. H. Elhajj, A. Chehab, and A. Kayssi, "Identity-based authentication scheme for the Internet of Things," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Messina, Italy, Jun. 2016, pp. 1109–1111.

[16] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, "Pauthkey: A pervasive authentication protocol and key establishment scheme for wireless sensor networks in distributed IoT applications," in *Int. J. Distrib. Sensor Netw.*, vol. 10, Jul. 2014, Art. no. 357430.

[17] G. Ho *et al.*, "Smart locks: Lessons for securing commodity Internet of Things devices," in *Proc. 11th ACM Asia Conf. Comput. Commun. Security (ASIA CCS)*, Xi'an, China, 2016, pp. 461–472.

[18] Y. Sharaf-Dabbagh and W. Saad, "On the authentication of devices in the Internet of Things," in *Proc. IEEE 17th Int. Symp. World Wireless Mobile Multimedia Netw. (WoWMoM)*, Coimbra, Portugal, Jun. 2016, pp. 1–3.

[19] C. Zhang and R. Green, "Communication security in Internet of Thing: Preventive measure and avoid DDoS attack over IoT network," in *Proc. 18th Symp. Commun. Netw. (CNS)*, San Diego, CA, USA, 2015, pp. 8–15.

[20] I. Bouij-Pasquier, A. A. Ouahman, A. A. E. Kalam, and M. O. de Montfort, "Smartorbac security and privacy in the Internet of Things," in *Proc. IEEE/ACS 12th Int. Conf. Comput. Syst. Appl. (AICCSA)*, Marrakesh, Morocco, Nov. 2015, pp. 1–8.

[21] G. L. dos Santos, V. T. Guimaraes, G. da Cunha Rodrigues, L. Z. Granville, and L. M. R. Tarouco, "A DTLS-based security architecture for the Internet of Things," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Larnaca, Cyprus, Jul. 2015, pp. 809–815.

[22] S. Jebri, M. Abid, and A. Bouallegue, "An efficient scheme for anonymous communication in IoT," in *Proc. 11th Int. Conf. Inf. Assurance Security (IAS)*, Marrakesh, Morocco, Dec. 2015, pp. 7–12.

[23] K. Yoshigoe, W. Dai, M. Abramson, and A. Jacobs, "Overcoming invasion of privacy in smart home environment with synthetic packet injection," in *Proc. TRON Symp. (TRONSHOW)*, Tokyo, Japan, Dec. 2015, pp. 1–7.

[24] L. Seitz, G. Selander, and C. Gehrmann, "Authorization framework for the Internet-of-Things," in *Proc. IEEE 14th Int. Symp. World Wireless Mobile Multimedia Netw. (WoWMoM)*, Madrid, Spain, Jun. 2013, pp. 1–6.

[25] M. Vučinić *et al.*, "OSCAR: Object security architecture for the Internet of Things," in *Proc. IEEE Int. Symp. World Wireless Mobile Multimedia Netw.*, Jun. 2014, pp. 1–10.

[26] S. Cirani, M. Picone, P. Gonizzi, L. Veltri, and G. Ferrari, "IoT-OAS: An OAuth-based authorization service architecture for secure services in IoT scenarios," *IEEE Sensors J.*, vol. 15, no. 2, pp. 1224–1234, Feb. 2015.

[27] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: Perspectives and challenges," *Wireless Netw.*, vol. 20, no. 8, pp. 2481–2501, 2014.

[28] J. Chen, S. Kher, and A. Somani, "Distributed fault detection of wireless sensor networks," in *Proc. Workshop Dependability Issues Wireless Ad Hoc Netw. Sensor Netw. (DIWANS)*, 2006, pp. 65–72.

[29] A. P. R. da Silva *et al.*, "Decentralized intrusion detection in wireless sensor networks," in *Proc. 1st ACM Int. Workshop Qual. Service Amp Security Wireless Mobile Netw. (Q2SWinet)*, Montreal, QC, Canada, 2005, pp. 16–23.

[30] Y. Wang, X. Wang, B. Xie, D. Wang, and D. P. Agrawal, "Intrusion detection in homogeneous and heterogeneous wireless sensor networks," *IEEE Trans. Mobile Comput.*, vol. 7, no. 6, pp. 698–711, Jun. 2008.

[31] G. Gaubatz, J.-P. Kaps, E. Ozturk, and B. Sunar, "State of the art in ultra-low power public key cryptography for wireless sensor networks," in *Proc. 3rd IEEE Int. Conf. Pervasive Comput. Commun. Workshops*, Mar. 2005, pp. 146–150.

[32] S. C.-H. Huang and D.-Z. Du, "New constructions on broadcast encryption key pre-distribution schemes," in *Proc. IEEE 24th Annu. Joint Conf. Comput. Commun. Soc.*, vol. 1. Miami, FL, USA, Mar. 2005, pp. 515–523.

[33] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Proc. Symp. Security Privacy*, Berkeley, CA, USA, May 2003, pp. 197–213.

[34] F. M. Al-Turjman, A. E. Al-Fagih, W. M. Alsalih, and H. S. Hassanein, "A delay-tolerant framework for integrated RSNs in IoT," *Comput. Commun.*, vol. 36, no. 9, pp. 998–1010, 2013.

[35] H. Liu, M. Bolic, A. Nayak, and I. Stojmenovic, "Taxonomy and challenges of the integration of RFID and wireless sensor networks," *IEEE Netw.*, vol. 22, no. 6, pp. 26–35, Nov./Dec. 2008.

[36] H. Chan and A. Perrig, "PIKE: Peer intermediaries for key establishment in sensor networks," in *Proc. IEEE 24th Annu. Joint Conf. Comput. Commun. Soc.*, vol. 1. Miami, FL, USA, Mar. 2005, pp. 524–535.

[37] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proc. 9th ACM Conf. Comput. Commun. Security (CCS)*, Washington, DC, USA, 2002, pp. 41–47.

[38] H. Corrigan-Gibbs and B. Ford, "Dissent: Accountable anonymous group messaging," in *Proc. ACM CCS*, Chicago, IL, USA, 2010, pp. 340–350.

[39] D. I. Wolinsky, H. Corrigan-Gibbs, B. Ford, and A. Johnson, "Dissent in numbers: Making strong anonymity scale," in *Proc. USENIX OSDI*, 2012, pp. 179–192.

[40] H. Corrigan-Gibbs, D. I. Wolinsky, and B. Ford, "Proactively accountable anonymous messaging in verdict," in *Proc. USENIX Security*, Washington, DC, USA, 2013, pp. 147–162.

[41] H. Corrigan-Gibbs, D. Boneh, and D. Mazières, "Riposte: An anonymous messaging system handling millions of users," in *Proc. IEEE S P*, San Jose, CA, USA, 2015, pp. 321–338.

[42] X. Zhao, L. Li, G. Xue, and G. Silva, "Efficient anonymous message submission," in *Proc. IEEE INFOCOM*, Orlando, FL, USA, Mar. 2012, pp. 2228–2236.

[43] Y. Yao, L. T. Yang, and N. N. Xiong, "Anonymity-based privacy-preserving data reporting for participatory sensing," *IEEE Internet Things J.*, vol. 2, no. 5, pp. 381–390, Oct. 2015.

[44] D. Halperin *et al.*, "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," in *Proc. IEEE S&P*, Oakland, CA, USA, 2008, pp. 129–142.

[45] C. Li, A. Raghunathan, and N. K. Jha, "Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system," in *Proc. IEEE HealthCom*, Columbia, MO, USA, 2011, pp. 150–156.
[46] J. Radcliffe, "Hacking medical devices for fun and insulin: Breaking the human SCADA system," in *Proc. Black Hat USA*, 2011, pp. 1–12.
[47] E. Marin, D. Singelée, B. Yang, I. Verbauwhede, and B. Preneel, "On the feasibility of cryptography for a wireless insulin pump system," in *Proc. 6th ACM Conf. Data Appl. Security Privacy (CODASPY)*, New Orleans, LA, USA, 2016, pp. 113–120.
[48] B. Jack. (2015). *Implantable Medical Devices: Hacking Humans*. [Online]. Available: https://en.wikipedia.org/wiki/Barnaby_Jack#cite_note-medcity-11
[49] D. Goldman. (2013). *A Hacker Can Give You a Fatal Overdose*. [Online]. Available: http://money.cnn.com/2015/06/10/technology/drug-pump-hack/
[50] *Two Safety Communications on the Cybersecurity Vulnerabilities of Two Hospira Infusion Pump Systems*, FDA, Silver Spring, MD, USA, 2015. [Online]. Available: http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/default.htm
[51] K. B. Rasmussen, C. Castelluccia, T. S. Heydt-Benjamin, and S. Capkun, "Proximity-based access control for implantable medical devices," in *Proc. ACM CCS*, Chicago, IL, USA, 2009, pp. 410–419.
[52] X. Hei and X. Du, "Biometric-based two-level secure access control for implantable medical devices during emergencies," in *Proc. IEEE INFOCOM*, Shanghai, China, 2011, pp. 346–350.
[53] F. Xu, Z. Qin, C. C. Tan, B. Wang, and Q. Li, "Imdguard: Securing implantable medical devices with the external wearable guardian," in *Proc. IEEE INFOCOM*, Shanghai, China, 2011, pp. 1862–1870.
[54] M. Rostami, A. Juels, and F. Koushanfar, "Heart-to-heart (H2H): Authentication for implanted medical devices," in *Proc. ACM CCS*, Berlin, Germany, 2013, pp. 1099–1112.
[55] X. Hei, X. Du, S. Lin, and I. Lee, "PIPAC: Patient infusion pattern based access control scheme for wireless insulin pump system," in *Proc. IEEE INFOCOM*, Turin, Italy, 2013, pp. 3030–3038.
[56] X. Hei, X. Du, and S. Lin, "Poster: Near field communication based access control for wireless medical devices," in *Proc. ACM MobiHoc*, Philadelphia, PA, USA, 2014, pp. 423–424.
[57] G. Zheng, G. Fang, M. A. Orgun, and R. Shankaran, "A non-key based security scheme supporting emergency treatment of wireless implants," in *Proc. IEEE ICC*, Sydney, NSW, Australia, 2014, pp. 647–652.
[58] X. Hei, X. Du, J. Wu, and F. Hu, "Defending resource depletion attacks on implantable medical devices," in *Proc. IEEE GLOBECOM*, Miami, FL, USA, 2010, pp. 1–5.
[59] J. Liu, M. A. Ameen, and K. S. Kwak, "Secure wake-up scheme for WBANs," *IEICE Trans. Commun.*, vol. 93-B, no. 4, pp. 854–857, Apr. 2010.
[60] S. Raza *et al.*, "Securing communication in 6LoWPAN with compressed IPsec," in *Proc. Int. Conf. Distrib. Comput. Sensor Syst. Workshops (DCOSS)*, Barcelona, Spain, Jun. 2011, pp. 1–8.
[61] S. Raza, S. Duquennoy, J. Hoglund, U. Roedig, and T. Voigt, "Secure communication for the Internet of Things—A comparison of link-layer security and IPsec for 6LoWPAN," *Security Commun. Netw.*, vol. 7, no. 12, pp. 2654–2668, 2014.
[62] A. J. Jara, D. Fernandez, P. Lopez, M. A. Zamora, and A. F. Skarmeta, "Lightweight MIPv6 with IPsec support," *Mobile Inf. Syst.*, vol. 10, no. 1, pp. 37–77, 2014.
[63] T. Kothmayr, C. Schmitt, W. Hu, M. Brünig, and G. Carle, "DTLS based security and two-way authentication for the Internet of Things," *Ad Hoc Netw.*, vol. 11, no. 8, pp. 2710–2723, Nov. 2013.
[64] S. Raza, D. Trabalza, and T. Voigt, "6LoWPAN compressed DTLS for CoAP," in *Proc. IEEE 8th Int. Conf. Distrib. Comput. Sensor Syst.*, Hangzhou, China, May 2012, pp. 287–289.
[65] S. Raza, H. Shafagh, K. Hewage, R. Hummen, and T. Voigt, "Lithe: Lightweight secure CoAP for the Internet of Things," *IEEE Sensors J.*, vol. 13, no. 10, pp. 3711–3720, Oct. 2013.
[66] M. Brachmann, S. L. Keoh, O. G. Morchon, and S. S. Kumar, "End-to-end transport security in the IP-based Internet of Things," in *Proc. 21st Int. Conf. Comput. Commun. Netw. (ICCCN)*, Munich, Germany, Jul. 2012, pp. 1–5.
[67] R. Hummen, J. H. Ziegeldorf, H. Shafagh, S. Raza, and K. Wehrle, "Towards viable certificate-based authentication for the Internet of Things," in *Proc. 2nd ACM Workshop Hot Topics Wireless Netw. Security Privacy (HotWiSec)*, Budapest, Hungary, 2013, pp. 37–42.
[68] Wikipedia. (2016). *Mirai*. [Online]. Available: https://en.wikipedia.org/wiki/Mirai_(malware)
[69] S. Khandelwal. (2016). *New IoT Botnet Malware Discovered; Infecting More Devices Worldwide*. [Online]. Available: http://thehackernews.com/2016/10/linux-irc-iot-botnet.html
[70] Z. A. Baig, M. Baqer, and A. I. Khan, "A pattern recognition scheme for distributed denial of service (DDoS) attacks in wireless sensor networks," in *Proc. 18th Int. Conf. Pattern Recognit. (ICPR)*, vol. 3. Hong Kong, 2006, pp. 1050–1054.
[71] X. Du, M. Guizani, Y. Xiao, and H.-H. Chen, "Defending DoS attacks on broadcast authentication in wireless sensor networks," in *Proc. IEEE Int. Conf. Commun.*, Beijing, China, May 2008, pp. 1653–1657.
[72] K. Gill and S.-H. Yang, "A scheme for preventing denial of service attacks on wireless sensor networks," in *Proc. 35th Annu. Conf. IEEE Ind. Electron.*, Porto, Portugal, Nov. 2009, pp. 2603–2609.
[73] R. Nanda and P. V. Krishna, "Mitigating denial of service attacks in hierarchical wireless sensor networks," *Netw. Security*, vol. 2011, no. 10, pp. 14–18, 2011.
[74] K. Sonar and H. Upadhyay, *An Approach to Secure Internet of Things Against DDoS*. Ahmedabad, India: Springer, 2016, pp. 367–376.

Yuchen Yang received the B.S. degree in computer software theory from Harbin Engineering University, Harbin, China, in 2011, where he is currently pursuing the Ph.D. degree in computer application technology.

He had been involved with E-government modeling and simulation with the National Engineering Laboratory, Glasgow, U.K., since 2009. His current research interests include E-government modeling and simulation, organization, and management in big data.

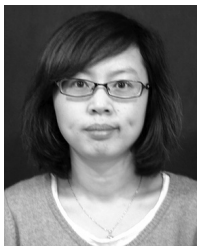
Longfei Wu received the B.E. degree in communication engineering from the Beijing University of Posts and Telecommunications, Beijing, China, in 2012. He is currently pursuing the Ph.D. degree at the Department of Computer and Information Sciences, Temple University, Philadelphia, PA, USA, under the supervision of Dr. X. Du.

His current research interest includes security and privacy issues of modern computing systems and devices including mobile devices, medical devices, and Internet-of-Things.

Guisheng Yin was born in Taixing, China, in 1964.

He is a Professor and the Ph.D. Supervisor with the Harbin Engineering University, Harbin, China. His current research interests include data mining, computational intelligence, and information security.

Dr. Yin is a Senior Member of the China Computer Federation.



Lijie Li received the M.S. degree from the College of Computer Science and Technology, Harbin Engineering University, Harbin, China, in 2006, and the Ph.D. degree from the College of Automation, Harbin Engineering University, in 2012.

She is currently a Lecturer with the College of Computer Science and Technology, Harbin Engineering University. Her current research interests include privacy protection, social network, and pattern recognition.

Hongbin Zhao received the Ph.D. degree in automation from Harbin Institute University, Harbin, China.

He is a Post-Doctoral Fellow with the College of Computer Science and Technology, Harbin Engineering University. He has authored or co-authored over ten publications as edited books and proceedings, invited book chapters, and technical papers in refereed journals and conferences. His current research interests include data security and privacy, mobile computing, and distributed and networked systems.