Security features and possible attcks on iot

*A. Security Features of IoT*

*1) Confidentiality:* Confidentiality can ensure that the data is only available to authorized users throughout the process, and cannot be eavesdropped or interfered by nonauthorized

users. In IoT, confidentiality is an important security principle, because a large number of measurement devices (RFID, sensors, etc.) can integrated i IoT. Thus, it is critical to ensure that the data collected by a measurement device will not reveal secure information to its neighboring devices. To achieve great confidentiality, enhanced techniques, including

secure key management mechanisms, and others should be developed and used [22].

*2) Integrity:* Integrity can ensure that the data cannot be tampered by intended or un-intended interference during the data delivery in communication networks, ultimately providing

the accurate data for authorized users. Integrity is important for IoT, because if IoT applications receive forged data or tampered data, erroneous operation status can be estimated and wrong feedback commands can be made, which could further disrupt the operation of IoT applications. To achieve acceptable integrity, enhanced secure data integrity mechanisms (false data filtering schemes, etc.) should be developed and applied [143].

*3) Availability:* Availability can ensure that the data and devices are available for authorized users and services whenever the data and devices are requested. In IoT, services are commonly requested in real-time fashion, and services cannot be scheduled and provided if the requested data cannot be delivered in a timely manner. Thus, availability is also an

important security principle. One of the most serious threats to availability is the denial-of-service (DoS) attack, and enhanced techniques (secure and efficient routing protocols, etc.) should be studied and applied to ensure availability in IoT [82].

*4) Identification and Authentication:* Identification can ensure that nonauthorized devices or applications cannot be connected to IoT, and authentication can ensure that the data delivered in networks are legitimate, and the devices or applications that request the data are legitimate as well. In IoT, identifying and authenticating each data and object is difficult, because a arge number of diverse objects comprise an IoT. Thus, designing efficient mechanisms to deal with the authentication of objects or things is critical in IoT [32].

*5) Privacy:* Privacy can ensure that the data can only be controlled by the corresponding user, and that no other user can access or process the data. Unlike confidentiality, which aims to encrypt the data without being eavesdropped and interfered by nonauthorized users, privacy ensures that the user can only have some specific controls based on received data and cannot infer other valuable information from the received data [20], [106], [144], [159]. Privacy is considered as one of important security principles due to a large number of devices,

services, and people sharing the same communication network in IoT.

**Security challenges of IoT**

In this section, security challenges in each layer of IoT architecture are presented in detail. In SoA-based IoT, the service layer is established via extracting the functionality of data services in the network layer and the application layer. Thus, security challenges in the service layer can be attributed to challenges in the network and the application layers. In the

following, only security challenges in the perception layer, the network layer, and the application layer are presented. [4] [5]

*1) Perception Layer:* As the main purpose of the perception layer in IoT is to collect data, the security challenges in this layer focus on forging collected data and destroying perception

devices, which are presented below.

|  |  |  |
| --- | --- | --- |
|  |  |  |
| 1 | Node capture attack | In this attack, the control of the node or device is captured by physically replacing the entire node or tampering the node or device. If a node undergoes this attack, important information like group communication key, radio key, matching key etc. can be exposed. |
| 2 | Malicious code injection attacks | In this case, malicious code is injected into the memory of a node. This node can further grant accesses and have the full control of the system. |
| 3 | False data injection attacks | In this attack, the false data could be injected in the device and this false data is transmitted to the IoT applications. |
| 4 | Replay attacks (or freshness attacks) | To obtain the trust of IoT, adversary uses a malicious node to transmit information to the destination host. This attack is commonly used in the authentication process to destroy the validity of certification |
| 5 | Cryptanalysis attacks and side channel attacks | A cryptanalysis attack can use the obtained cipher text or plaintext to infer the encryption key being used in the encryption algorithm. |
| 6 | Eavesdropping and interference | In an IoT environment, most of the data transfer is through wireless network and it can be eavesdropped by non-authorized users. Noise data can also be used to interfere with the information. |
| 7 | Sleep deprivation attacks | In order to extend the life cycle of the devices and nodes, devices or nodes are programmed to follow a sleep routine to reduce the power consumption. This attack will break the programmed sleep routines to keep the device active all the time. |

*2) Network Layer:* As the main purpose of the network layer in IoT is to transmit collected data, the security challenges in this layer focus on the impact of the availability of network resources. Also, most devices in IoT are connected into IoT networks via wireless communication links. Thus, most security challenges in this layer are related to wireless networks in IoT.

|  |  |  |
| --- | --- | --- |
| 1 | *DoS attacks* | This is considered to be one of the most common attack in which the services of the IoT system becomes unavailable. It attacks the network protocols with huge amount of traffic. |
| 2 | *Spoofing attacks* | In this case, the advisory gains the full access of IoT system and it sends malicious data into the system. IP spoofing is an example to this type of attack wherein the adversary spoof and records th IP address of other authorized devices in the IoT system, further accessing the whole system to send malicious data. |
| 3 | *Sinkhole attacks* | In this type of attack, a node claims to have capabilities so that the neighbouring nodes choose this node as the forwarding node in data routing process. In this way, the compromised node gets large amount of data before it is delivered to the system. this attack will open up many other attacks like DoS. |
| 4 | *Wormhole attacks* | Wormhole attack can be launched  by two cooperative malicious devices or nodes in IoT, in which  the two malicious devices in different locations can exchange  routing information with private links to achieve a false onehop  transmission between them, even if they are located far  away from each other [67]. In a wormhole attack, because  the forwarding hops are reduced, more data will be delivered  through these two malicious devices or nodes. With access  to more delivered data, the wormhole attack can lead to the  similar damage as sinkhole attack. To defend against wormhole  attack, there are some possible defensive techniques.  One technique is to modify the routing protocols to enhance  the security in the route selection process [26], while other  techniques involve deploying secure hardware (GPS, directed  antenna, etc.). |
| 5 | *Man in the middle attack* | In a man in the middle  attack, a malicious device controlled by the adversary  can be virtually located between two communicating devices  in IoT [96]. By stealing the identify information of the  1134 IEEE INTERNET OF THINGS JOURNAL, VOL. 4, NO. 5, OCTOBER 2017  two normal devices, the malicious device can be a middle  device to store and forward all data, which is communicated  between these two normal devices, while the two normal  devices cannot detect the existence of the malicious device,  and instead believe that they directly communicate with each  other. The man in the middle attack can violate the confidentiality,  integrity, and privacy of restricted data in IoT  through monitoring, eavesdropping, tampering, and controlling  the communication between the two normal devices. Unlike  malicious node capture attacks that need to physically tamper  with the hardware of devices, the man in middle attack can  be launched by only relying on the communication protocols  used in IoT networks. Secure communication protocols and  key management schemes, which can ensure the identify and  key information of normal devices not be leaked to the adversary,  can be efficient defense techniques to protect against the  attack [22], [82]. |
| 6 | *Routing information attacks* | Routing information  attacks focus on the routing protocols in IoT systems, in which  the routing information can be manipulated and resent by the  adversary to create route loops in the data transmission of  the network, leading to the extension of source paths and the  increase of end-to-end delay in IoT networks [8]. To defend  against the routing information attack, secure routing protocols  and trust management to establish secure links among devices  in IoT and ensure the identifying information and IP addresses  not to be leaked to the adversary are possible techniques to  be used. |
| 7 | *Sybil attacks* | In a sybil attack, a malicious device,  namely a sybil device, can claim several legitimate identities  and impersonate them in IoT systems [8], [95], [158].  Because a sybil device has several legitimate identities, false  data sent by the sybil device can be easily accepted by their  benign neighboring devices. Also, routes that select sybil  devices as forwarding nodes may consider that several different  intersected paths are determined, but, in fact only  one path is determined and all transmitted data needs to go  through the sybil device, in which jamming and DoS can  be used. To defend against sybil attacks, secure identification  and authentication mechanisms need to be developed for IoT  systems [32]. |
| 8 | *Unauthorized access* | RFID is an important enabling  technology in IoT. Nonetheless, as a large number of RFIDbased  devices are integrated in IoT, and most of the RFID  tags lack proper authentication mechanisms, RFID tags can be  accessed and the information stored in tags can be obtained,  modified, and deleted by the adversary [8], [60]. Thus, authorization  access and authentication mechanisms for RFID-based  devices in IoT is a challenge in need of further development  [56]. |

*3) Application Layer:* The main purpose of the application layer is to support services requested by users. Thus, challenges in the application layer focus on the software attacks. Here, several possible challenges in the application layer of IoT are presented below.

|  |  |  |
| --- | --- | --- |
|  |  |  |
| 1 | *Phishing attack* | In phishing attacks, the adversary  can obtain the confidential data of users, such as identification  and passwords, by spoofing the authentication credentials of  users via the infected e-mails and phishing websites [8], [54].  Secure authorization access, and identification and authentication  can mitigate phishing attacks [8]. Nonetheless, the most  efficient way is for users themselves to always be vigilant  while surfing online. This becomes an issue as most of devices  in IoT are machines, which may lack of such intelligence |
| 2 | *Malicious virus/worm* | A malicious virus/worm is  another challenges to IoT applications [8], [127], [154]. The  adversary can infect the IoT applications with malicious selfpropagation  attacks (worms, Trojan Horse, etc.), and then  obtain or tamper with confidential data. Reliable firewall,  virus detection, and other defensive mechanisms need to be  deployed to combat malicious virus/worm attacks in IoT  applications [110]. |
| 3 | *Malicious scripts* | Malicious scripts represent the  scripts that are added to software, modified in software, and  deleted from software with the purpose of harming the system  functions of IoT [8]. Because all IoT applications are connected  to the Internet, the adversary can easily fool the  customers in running malicious scripts (java attack applets,  active-x scripts, etc.) when requesting services through the  Internet. Malicious scripts can pose the leakage of confidential  data and even a complete system shut down. To defend against  malicious scripts, effective script detection techniques, including  honeypot techniques, static code detection, and dynamic  action detection, need to be deployed in IoT systems. |