A Survey on Next generation Computing IoT Issues and Challenges

Anurag Shukla
Department of Computer Science & Engineering
National Institutes of Technology
Raipur, India
anurag672@yahoo.com

Sarsij Tripathi
Department of Computer Science & Engineering
National Institutes of Technology
Raipur, India
stripathi.cs@nitrr.ac.in

Abstract—With the popularity of the Internet of things (IoT), an enormous number of sensors and smart objects, which is heterogeneous in nature deployed into a network, send/receive data through the internet on the web. It is tedious to secure the communicated data and the device identity otherwise it cannot be adopted by their natives. But, existing security techniques that are very popular on the Internet are too complex to integrate on small, constrained objects. While initiating security through some protocol and techniques, the life of battery operated sensor can be reduced, so there is need to provide a proper balance between security and energy. This paper presents a survey of existing security protocols applied on IoT, their comparison and possible solution for various attacks.

Keywords—Internet of Things (IoT), Challenges and Issues, Security, Possible Solutions, Energy and Quality of Services (QoS).

I. INTRODUCTION

With the progress in wireless communication, Pervasive computing and mobile computing, resulted in a new model known as the Internet of things (IoT). IoT is attracting a lot of researchers and industrial innovation. The definition for the IoT could be as the ubiquitous and global networks, which offer various applications for controlling and monitoring the physical world activities of the information collection, data cleaning, processing and analysis of data generated by IoT sensors. These IoT devices have in built computation and sensing capabilities such as RFID, GPS, actuators, LAN and wireless LAN (Zhao & Ge, 2013). These "things" could interact with each other (machine-to-machine (M2M) communication) by making request and response for data and sensing the real world attributes like temperature, pressure, etc. These devices can be bind to the internet and could be managed and operated remotely (Xu, Ding, Zhao, Hu & Fu, 2013; Wei & Qi, 2011).

It can be seen as a network of wide-range devices that introduces not only the various security issues available in sensor devices, mobile communication, and the internet, but also some abnormal and accentuated issues like user and network privacy, sensor life cycle (energy consumption), secure routing and quality of service among these devices (Zhao & Ge, 2013).

In the last few years, IoT became a hot topic in industry and academic research. IoT is expanding everywhere and supports a complete view of the real world and high level of interaction with the physical world (Atzori, Iera & Morabito, 2010; Gubbi, Buyya & Marusic, 2010). Such areas are smart transportation system; Energy monitoring system, e-healthcare is just a few examples where IoT will be applicable. The reorganization of IoT will largely depend on reliable communication, network, system architecture, data computation, resource allocation, and pervasive computing technology, which provides efficient, secure, and physically as well as cyber interconnectivity. The main agenda of it is the device interconnection within the network, routing between the networks, and specifically the last one dynamic security level mechanism for the various nodes according their real need by considering various parameters: energy and computation capabilities. With increasing number of interconnected devices on the internet (as shown in figure 2), the daunting challenge is to secure the node network from possible threats and attacks. People will feel insecure to migrate their devices on the internet if there is a possibility of being controlled or attacked from unauthorized person or machine over the network (Ericsson, 2011).
Figure 1. Internet of Things and It’s Popular Application

Continue with our discussion, device communication and routing is a critical part of it due to the need of maintaining consistency while data or packet is transmitted between IoT nodes across various network topologies. The processes of making secure communication and maintaining a QoS even more tedious (Gubbi et al., 2010). In it, various Sensor nodes have different computation capabilities, and it is running on battery power. Consider via the above factor’s; there is an essential need of a real-time security model so that system can assign the different level of security techniques according to node characteristics like energy, computation power, etc. for securing the data and routing process across IoT nodes.

II. DEFINITIONS, HISTORY & TRENDS

A. Definitions

Atzori et al. (2010) defined, IoT can be combined into three parts—internet (middleware), things (sensors) and semantic (knowledge/data analysis). Although this type paradigm is required due to the subject nature, the IoT requirement can be expanded only in the service domain.

Figure 2. A forecast of more than 50 billion interconnected devices by 2020. (Adapted from [CISCO, 2011]).

The IoT architecture (indicated in figure 3) is being organized into three layers: perception, network, and application layer (Zhao et al., 2013). The support layer (such as cloud computing, intelligent computing) is also included in some system architecture for the support of the application layer (Suo, Wan, Zou, & Liu, 2012). In this survey, we have considered three-layer architectures, which have been reported frequently by other researcher. In this article, we explore the IoT protocol, which works on network and application layer and their vulnerability of being attacked during communication.

The Rest of the article is organized into three sections. In the first section we cover, the various definitions related to IoT and their history followed by IoT application, in the very next section, we provide the various IoT related challenges and their issues: Security, Energy, and Quality of Service (QoS). In the next section, we give the protocol stack corresponding IoT layers and provide a comparison between them. In the last section we analyze various IoT related security work which is isolated from the standard protocols and categorize them according to their key cryptographic techniques, we summarize all these techniques and provide a comparison table between them by considering their provide solution against security threats.

According to the RFID group, the definition of IoT is: The worldwide-interconnected network of different objects uniquely identified based on an address scheme through standard protocols.

The Clusters of European research projects on IoT (Sundmaeker, Guillemin, Friess, & Woelflê, 2010): “Things” can participate actively in social and business process where they able to interact and communicate with each other by transmitting the data and sensed value about the physical world, while responding autonomously without any human interaction to real/physical world events and trigger some actions and offer the service.

Figure 3. Security Architecture (Suo, Wan, Zou, & Liu, 2011; Zhao & Ge, 2013)
By Forrester, Smart environment (Bélissent, 2010): Uses of information, communication technologies, and protocols for developing an infrastructure to serve the society, cities administrates transportation, health care and education more efficient, interactive and better.

In our definition, we believe in the theory that a common static architecture cannot be a blueprint for all applications, so we should make it more flexible to support scalability and do not restrict to any standard protocol. Our definition of IoT is Interconnection of devices in IoT networks is achieved through some standards or protocols. Day by day new devices are introduced into a market, for instance, some couple of years ago no one wonders about a mobile phone. Now, these days the mobile phone is smarter as computer and cheaper too. Therefore, we are suggesting here, Standards or protocols, which are used for developing the IoT network, should be open. When new devices are introduced in a network, standards can be modified according to their need.

B. IoT History

The term IoT is around 17 years old, but the real idea about connecting devices had been longer, around since 1970. At that time, the idea was often called “pervasive computing” or “embedded internet”. The term, IoT was actually invented by Kevin Ashton at Procter & Gamble during his work. In 1999 “internet” was a hot topic and Kevin Ashton was working in supply chain optimization, wanted to collaborate two technologies: internet and RFID so that he can attract the senior management team. He called his presentation “Internet of Things”. Even he got successes, but then it was remained untouched for next 10 years.

In the table 1, we give the brief history about IoT and cover the important events year by year, which can help to know that how IoT came into existence from other areas and what is the required technology, which can help in shaping the IoT world.

<table>
<thead>
<tr>
<th>Year</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>1967</td>
<td>Remotely Monitored Battlefield Sensor System (REMBASS)</td>
</tr>
<tr>
<td>1978</td>
<td>Aircraft Detection through Distributed Sensor Networks at Lincoln Labs</td>
</tr>
<tr>
<td>1994</td>
<td>Low Power Wireless Integrated Micro sensors (LWIM) - Bill Kaiser</td>
</tr>
<tr>
<td>1999</td>
<td>1999: The term Internet of Things (IoT) is introduced by K. Ashton, Executive Director of the Auto-ID Center in MIT (Massachusetts Institute of Technology). First time N. Gershenfeld share his ideas about IoT in his book entitled “When Things Start to Think”. MIT Auto-ID Lab, originally founded by K. Ashton, D. Brock and S. Sharma. They introduced the Electronic Product Code (EPC), a global RFID-based item identification system intended to replace the UPC bar code.</td>
</tr>
<tr>
<td>2000</td>
<td>LG shared his idea and plans on internet refrigerator.</td>
</tr>
<tr>
<td>2002</td>
<td>The Ambient Orb created by David Rose and others in a spin-off from the MIT Media Lab is released into wild with NY Times Magazine naming it as one of the Ideas of Year. The Orb monitors the Dow Jones, personal portfolios, weather and other data sources and changes its color based on the dynamic parameters.</td>
</tr>
<tr>
<td>2003-2004</td>
<td>RFID is deployed on large number by the Department of Defense (US) in their Savi program and Wal-Mart in the commercial world.</td>
</tr>
<tr>
<td>2005</td>
<td>The UN’s International Telecommunications Union (ITU) published its first report on the IoT’s topic.</td>
</tr>
<tr>
<td>2008</td>
<td>Identified by the EU and the First IoT European conference is held. Group of companies launched the IPSO Alliance to encourage the use of IP in “Smart Objects” networks and to enable the IoT.</td>
</tr>
</tbody>
</table>

C. Trends

IoT is known as one of the emerging technology in research and it’s industry. People’s interest about different paradigms varied with respect to time. According to Google search (2017) trends, the web search popularity during the last 13 years for the terms IoT, wireless sensor network and ubiquitous computing is given in figure 4. It can be clearly observed that the popularity of it is increasing day by day with the downturn of the wireless sensor network.
The FCC voted to approve and launching the ‘white space’ spectrum. IoT was listed as one of the 6 “Disruptive Civil Technologies” by US Intelligence Council, with Potential impacts on US interests out to 2025. According to Cisco’s Business Solutions Group in 2008-2009, IoT was born. Chinese Premier Wen Jiabao calls IoT as a key for China industry and has plans to major investments in IoT industry.

2010 IPv6 public launch- The new protocol allows approximately for $2^{128}$ addresses to support IoT.

III. APPLICATION

IoT has the ability and can take the society to another level, where things can be very systematic and easy to operate from anytime or anywhere. IoT allows the device for making smart decisions and appropriate action without any human interaction. IoT concepts have been revealed in various domains ranging from transport, logistics, object tracking, agriculture, smart environment (home, office, city) to energy and defense.

According to Fleisch (2010), IoT is appropriate in every phase and everywhere. He considered 100 existence and emerging application that leveraging the IoT concept. He identified seven primary value drivers. Starting four applications are based on machine-to-machine communication (M2M) and rest of three based on user participation.

1. Simplified manual proximity trigger: IoT nodes can transmit their name or identity when they are in reach of sensor range. As soon as the node is close, enough into sensing space, a particular activity or transaction will be triggered automatically.
2. Automatic proximity trigger: It triggered an automatic action when the physical distance between two nodes under below to some particular value (threshold).
3. Automatic sensor triggering: A smart device can collect data through various types of sensors, including brightness, temperature, smell, acceleration, vibration, noise, chemical composition, humidity, and vision and life signals. Devices sense these data and communicate with the server and action will trigger based on pre-program rules.
4. Automatic product security: A IoT nodes can provide security based on the QR code, and its cyber representation (Bind a specific URL corresponding to every QR code).
5. Simple and direct user feedback: IoT nodes contain simple mechanism and can give feedback to an authenticate person present in the domain either in audio format (small beep) or visual signal (flashlight).
6. Extensive user feedback: IoT nodes can offer a service to the user (node is linked to a service through some gateway device). Augmented service is an appropriate example of this kind of application.
7. Mind changing feedback: The combination of virtual world and the real world might be a reason of new levels of change in the human behavior. Fleisch’s seven drivers can be suitable for real IoT applications.

By integrating subsystem (smart home, smart city, and transportation system) will form a smart environment that is shown in Table 2 and their specification on technical perspective is listed there. We identified some IoT application and grouped them according to their domain in Table 3.

<table>
<thead>
<tr>
<th>Network size</th>
<th>Users</th>
<th>Energy source</th>
<th>Communication</th>
<th>Data storage</th>
<th>IoT device</th>
<th>Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smart office / Home (Kidd et al., 1999)</td>
<td>Smart city (Murty et al., 2008)</td>
<td>Smart Forest/ Agriculture (Aun , 2000)</td>
<td>Smart Parking / Transportation (Lin et al., 2005)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Small</td>
<td>Medium/Large</td>
<td>Medium</td>
<td>Small/Large</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Very few</td>
<td>Many/Policy maker/General Public</td>
<td>Few/Landowner</td>
<td>General Public/ Many</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rechargeable battery</td>
<td>Energy harvesting</td>
<td>Energy harvesting</td>
<td>Rechargeable battery/ Energy harvesting</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wi-Fi/3G/4G LTE</td>
<td>Wi-Fi/3G/4G LTE</td>
<td>Wi-Fi/ Satellite</td>
<td>Wi-Fi/ Satellite</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local Server</td>
<td>Shared Server</td>
<td>Local Server/Shared Server</td>
<td>Shared Server</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RFID/ WSN</td>
<td>RFID/ WSN</td>
<td>WSN</td>
<td>RFID/WSN</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Small</td>
<td>Large</td>
<td>Medium</td>
<td>Medium/ Large</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 3. IoT Application Domains - Description and Examples.

<table>
<thead>
<tr>
<th>Domain</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industry</td>
<td>Application on automation industry and commercial or financial transactions between companies and various organizations.</td>
<td>Public sector, water infrastructure, manufacturing, logistic, transport, etc.</td>
</tr>
<tr>
<td>Environment</td>
<td>Applications for monitoring, protection and efficient utilization of all natural resources.</td>
<td>Agriculture, forest, energy management, environmental management services, recycling etc.</td>
</tr>
<tr>
<td>Society</td>
<td>Activities regarding the development and serve better societies, nation, and peoples.</td>
<td>Government services towards society and citizens (e.g., Smart traffic control system, health monitoring system, smart city).</td>
</tr>
</tbody>
</table>

IV. CHALLENGES AND ISSUES

The heterogeneous nature in its network is rising different challenges with respect of security, resource availability and functionality. A safe IoT system must overcome to all challenges given in table 4.

A. Security and Privacy

In IoT, two major issues are the privacy (user related information) and security about the sensed data and business processes. The heterogeneity in IoT nodes, large scale of deployment, resource constraints, and their mobility make it harder to secure the network. There are a large number of techniques for ensuring the confidentiality. However, the primary task is to execute this algorithm faster to match the constraint of real time and should be less energy consuming. In addition, for making encryption technique secure, an efficient key distribution should be used. In the small-scale system, key distribution can be possible at the time of deployment, but at a large level, only novel key distribution schemes can be used for ensuring the privacy. Data anonymity can be a solution for privacy, but it is supported by equipment like high computation power and large bandwidth which is just contradict to IoT requirements (Miorandi, Sicari, De Pellegrini & Chlamtac 2012).

Security is a critical component for adopting the IoT at a global level, and without any guarantee, regarding authenticity, confidentiality, integrity and non-repudiation the related party is unlikely to adopt on a large scale. We will explore these key points in this section.

1. Availability

Availability is the consistency of every layer services of a network to the devices and makes sure the survivability of network service even in the presence of attacks. IoT services will apply to commercial and real-time applications, so security in respect of availability should be on top.

2. Authenticity

A Process, where a user or node needs to prove their identity to use some services. Authentication is required to protect the system from impersonating nodes, which can breach the safety of the entire network. In IoT, many node support heterogeneous communication in a network, authentication is necessary to avoid illegal accesses.

3. Confidentiality

Data confidentiality is relevant to the business application, where an only authorized person can access or modify the data. In the context of IoT, data confidentiality addressing two important aspects: first is about the data access mechanism and a second are about object authentication processes. While data is transmitted, routing and encryption are precious to provide safety during communication.

4. Integrity

It provides an assurance that received data to the destination node should be original as sender sent, it should not be damaged or modified either from collision or through a third party (hacker).

5. Non-repudiation

Non-repudiation is an assurance that someone cannot deny to anything; as like source node send their data to the destination and should acknowledge the same. Non-repudiation is important to identify and some untrusted node can send the wrong information to some other nodes in a network and can deny, they never posted such information.

Table 4. IoT Challenges.

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interoperability</td>
<td>Incorporate of security techniques in IoT network should not obstruct the functionality of the heterogeneous devices.</td>
</tr>
<tr>
<td>Fault tolerance</td>
<td>The system should avoid even a single failure in the network, so infected node will not affect the entire system. Apart from that network must also avoid resource exhaustion attack against limited resource device.</td>
</tr>
<tr>
<td>Limitation of resource</td>
<td>Most of the IoT devices are restricted with respect to computation power, energy resources (battery operated), memory and bandwidth (linked to each other on low bandwidth). Therefore, it is tough to apply on internet security protocols directly in the context of IoT network. Hence, the standard security techniques need to redesign to full fill...</td>
</tr>
</tbody>
</table>
B. Energy

Many of IoT node runs on battery operated power and energy efficiency is most crucial for availability and proper functionality of the network. Energy efficiency in IoT sensor nodes is an active research area (Yoo, Wu, & Qiao, 2015; He, Chen, Yau & Sun, 2012). Most of it nodes are running on non-chargable energy source and communication between heterogeneous nodes is more energy consuming. Deployment of complex security protocols in an IoT network can consume more energy, so it is advisable that in its network, we need a mechanism where a level of security can assign while considering the parameters like energy and probability of actual threads at a particular node.

C. Quality of Services (QoS)

While developing an IoT network, various challenges exist for a developer, one of them a quality of service (QoS) in respect of sensing data quality, resource consumption, data drop and so on. The QoS deal with all the parameters, which can directly or indirectly affect the reliability, performance and availability of the network. Considering some of the points (European Commission, 2014) under this category are:

- Bandwidth, Capacity and Throughput
- Trustworthiness
- Latency
- Resource Optimization and Cost Efficiency
- Scalability

V. Related Work About IoT Protocols

In this section, we will discuss about various IoT protocols and try to identify their benefits as well as limitations. The discussion includes perception layer, network layer and application layer protocols. Network layer functionality is further divided into two parts.

A. IoT perception layer protocol

In this section, we will discuss different communication protocols for IoT device. In IoT, all types of sensors, actuator devices and communication technology or protocols between them will reside in this category only. ZigBee and Bluetooth are most commonly used in IoT network. In this layer, we will discuss various protocol standards. On the other hand, IEEE 801.11ah can be used easily due to the existing and globally spread infrastructure of IEEE 802.11 in a wireless application. In some application, reliability is preferable hence; they use Home Plug for LAN connectivity.

1. IEEE 802.15.4

IEEE 802.15.4 is most used standard in IoT for medium access control. It includes device communication, a header with source and destination address and frame format. The traditional network frame format does not use in IoT network due to their overhead so, in 2008 IEEE 802.15.4e was introduced to upgrade IEEE 802.15.4 to support less power energy. It is highly reliable because it uses channel hopping and time synchronization method.

2. IEEE 802.11ah

IEEE 802.11ah runs on low energy and apart from that, it is same as IEEE 802.11. IEEE 802.11 standard are not appropriate for IoT due to high power requirements and frame overhead, so it is a redesigned version of IEEE 802.11 to meet IoT requirements with less overhead and less power communication for motes and sensors. IEEE 802.11 (known as Wi-Fi) is very popular wireless standard and mostly used in Laptops, mobile phones, etc (Park, 2015).

Table 5. Protocol Stack for IoT Layer.

<table>
<thead>
<tr>
<th>Encapsulation</th>
<th>Routing</th>
<th>Perception</th>
</tr>
</thead>
<tbody>
<tr>
<td>(MQTT, SMQT, DDS, XMPP, AMQP CoRE, CoAP)</td>
<td>(RPL, CORPL, CARP…)</td>
<td>(WiFi, Bluetooth, Zigbee smart, DECT/ ULE, Weightless, Z-wave, DASH7, 3G/LTE, Home Plug GP, LoRaWAN, LTE-A, G.9959, 802.11ah, 802.15.4e…)</td>
</tr>
</tbody>
</table>
encrypt data and maintain integrity, so it is a secure and reliable protocol. This protocol ensures security source to destination (End to End security mechanism) and peer-to-peer as well (Raza, & Voigt, 2010; Kim, Hekland, Petersen & Doyle, 2008).

4. **Z-Wave**

   This protocol comes under MAC protocol and very popular for home automation. Its range up to 30-meter, appropriate for a small message and low power protocol and used for communication in smart home or office. Z-Wave follows master-slave architecture and master control the entire network and instructs the slaves through commands. It acknowledges the message to ensure reliability and uses CSMA/CA for collision detection (He, Chen, Yau, & Sun, 2012).

5. **Bluetooth Low Energy**

   Bluetooth is used for short distance communication and consume ten times less energy with 15 times more latency than classical Bluetooth. It works on master-slave architecture and uses two types of frame: data frame and advertising. Slaves send the advertising frame on one or more dedicated link. The master continues to sense these links, find them and connect with slaves. Nodes are mostly in an inactive state to make an efficient source of resource and awake only when they communicate with each other (Decuir, 2010; Hasan, Hossain, & Niyato, 2013).

6. **Zigbee Smart Energy**

   Zigbee supports a large range of communication and can be used in a healthcare system, remote controls or in smart office. It supports different network topologies like peer to peer, star, tree soon. ZigBee standards divide in two profiles: ZigBee and ZigBee Pro. ZigBee. These protocols work with different applications and support implementation with low computational power and memory. ZigBee Pro includes more features like efficiency through many to one routing techniques, security through symmetric key exchange and scalability (ZigBee Standards Organization, 2008).

7. **DASH7**

   It is wireless communication protocol and for RFID and employ globally on ISM Band (Industrial, scientific and medical) and appropriate for IoT applications. It supports high range, scalable and offers higher data rate than ZigBee. It is designed to support lightweight, low cost to support encryption and follow IPv6 addressing (LoRa Alliance, 2015).

8. **HomePlug**

   Homeplug is a MAC protocol and used in a home automation system. It comes in three versions: Home plug-AV, HomePlug AV2, and HomePlugGP. HomePlugGP is a redesigned version of HomePlugAv for ensuring low power and cost; it is specially designed for its applications (smart home). HomePlugGP uses Orthogonal Frequency Division coding Multiplexing (OFDM) coding for reliable communication. HomePlugGP use CDMA and TDMA techniques for medium accesses while HomePlugAV used only CSMA as a MAC protocol. HomePlugGP synchronizes the sleeping time and wakes up only when in requires, so it operates on less power than HomePlug9) G.9959 (HomePlug Alliance, 2012).

9. **Long Term Evolution-Advances (LTE-A)**

   Long Term Evolution Advances (LTE-A) is a set of standards, introduced for communication between M2M (machine to machine) or IoT devices in a cellular network. Compared to other cellular protocols, LTE supports scalability and low power. LTE-A divide the frequency into independent band and can them separately (Orthogonal Frequency Division Multiple Access). LTE-A architecture consists of a Core network- responsible for to track IPs and to control the mobile nodes; 2nd one is Radio accesses network to deal with access control, wireless connectivity, and data plan and the last one is mobile nodes (Hasan, Hossain, & Niyato, 2013).

10. **LoRaWAN**

    LoRaWAN is a new and emerging wireless technology, with low energy, low cost, secures and supports full duplex communication. It is designed to support large or scalable with million numbers of devices. It supports the future needs of IoT like energy harvesting, mobility, operated at low power and redundant operation (LoRa Alliance, 2015).

11. **Weightless**

    It is a wireless area network technology and designed by Special Interest Group (SIG) -Nonprofit organization. It supports two standards Weightless-N and Weightless-W. Weightless introduced earlier, support low cost and consumed less energy and communicating between machine to machine using TDM access. Weightless- W offers above features too, but uses only television band frequencies (Poole, 2014).

12. **Digital Enhanced Cordless Telecommunications (DECT) / Ultra Low Energy (ULE)**

    It is the European standard for cordless phones. Digital Enhanced Cordless Telecommunications (DECT) / Ultra Low Energy (ULE) is an improved version of DECT. It operates on low power and less cost air interface technique so it can be use
Table 6. Perception Layer Protocols Comparison

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Energy Efficient</th>
<th>Reliability</th>
<th>Remark: Techniques for ensuring the reliability</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE 802.15.4</td>
<td>High</td>
<td>High</td>
<td>Channel hopping, time synchronization</td>
</tr>
<tr>
<td>IEEE 802.11 AH</td>
<td>High</td>
<td>Less</td>
<td></td>
</tr>
<tr>
<td>Wireless HART</td>
<td>Less</td>
<td>High</td>
<td>Advance encryption</td>
</tr>
<tr>
<td>Z-Wave</td>
<td>High</td>
<td>High</td>
<td>Acknowledge system, CSMA/CD</td>
</tr>
<tr>
<td>Bluetooth Low</td>
<td>Very High</td>
<td>High</td>
<td>Encryption</td>
</tr>
<tr>
<td>Energy Zigbee Smart</td>
<td>High</td>
<td>High</td>
<td>Symmetric key</td>
</tr>
<tr>
<td>Energy DASH7</td>
<td>High</td>
<td>Average</td>
<td>Encryption</td>
</tr>
<tr>
<td>HomePlug</td>
<td>High</td>
<td>High</td>
<td>OFDM</td>
</tr>
<tr>
<td>LTE-A</td>
<td>High</td>
<td>Less</td>
<td></td>
</tr>
<tr>
<td>LoRaWAN</td>
<td>Very High</td>
<td>High</td>
<td>Acknowledgement, time-synchronization mechanisms at regular fixed intervals</td>
</tr>
<tr>
<td>Weightless</td>
<td>High</td>
<td>Less</td>
<td></td>
</tr>
<tr>
<td>DECT/ULE</td>
<td>High</td>
<td>High</td>
<td>Congestion free</td>
</tr>
</tbody>
</table>

in IoT applications. It communicates through the dedicated channel, so it is free from congestion. DECT/ULE uses FDMA and TDMA, which were not supported by DECT (Bush, 2015).

B. IoT Network layer protocol

We divide the network layer functionality into two parts: Routing and Encapsulation. In this section, we will discuss various routing and encapsulation protocols.

1. IoT Network layer Routing protocol

In this section, we will discuss IoT routing protocol, which is responsible for delivering the packets from source to target device.

a. Routing Protocol (RPL)

RPL (Routing Protocol) is a distance vector routing protocol that can support various communication protocols, which we discuss in an upper section of perception layer. It constructs Destination-oriented direct acyclic graph (DODAG) that has one and unique route from the root to all leaf nodes. Firstly, each node advertises him as a root node by sending an advertisement message. This message will spread in a network, and the entire DODAG will slowly build. When communicating, root sends a DAO (Destination Advertisement Object) to its parents, like this it’s will propagate to root, and root will decide according to the destination address that’s where it has to send. When any new node wants to join a network, it will request, through the DODAG Information Solicitation (DIS), and root gives acknowledge through DAO Acknowledgment (DAO-ACK). RPL node can be stateless and stateful, the stateful node used commonly and node keeps track of parents only. Root has complete knowledge of entire DODAG so communication will go through root only. Stateful node keeps information about the parents as well as children where communication will go through it does not need to go through the root (Winter, 2012).

b. Cognitive RPL (CORPL)

CORPL (Cognitive RPL) is an extension of RPL protocol, used DODAG topology and designed for the cognitive network. CORPL comes with two modifications of RPL that is it forwards the packet to best hope by choosing multiple forwarders from forwarder set. Each node maintains their forwarder set in place of its parent and use DIO message to update their neighbors when there is any change. Each node changes neighbor’s priorities corresponding these updates to create forwarder set (Aijaz, & Aghvami, 2015).

c. Content-aware routing protocol (CARP)

CARP (Content-aware routing protocol) is used in underwater communication, and it considers link reliability based on the successful communication by neighbor sensor history. It is a distributed routing protocol and uses a lightweight packet mechanism so that we can use in IoT application. It works based on two scenarios: network initialization and data forwarding. In first scenario: hello message will broadcast from the source to each available node in a network. In second scenario: packet will be routed in the network hop by hop. Each hop identifies independently. The main drawbacks with the CARP protocol are that it does not maintain the previously sensed data means if there is significant change is sensor data and if an application requires the previous one, in this kind of situation CARP is not applicable. E-CARP is an extended version of CARP with allowing to node save the previous data (Zhou, Yao, Xing, Shu, & Bu, 2015).
2. Network Layer Encapsulation Protocols

Ericsson (2011) estimated that up to 2020 there will be 50 billion devices on the Internet, so to support the unique addressing mechanism IPv6 protocol is used on its network. Now one problem is that, IoT data link frame format relatively small to store IPv6 addresses. Therefore, to handle this kind of situation IETF (Internet Engineering Task Force) working on a set of standards to enclose the IPv6 datagram’s into IoT data link layer frames. In this section, we will discuss this mechanism in brief.

Table 7. Network Layer Routing Protocols Comparison.

<table>
<thead>
<tr>
<th>Protocols</th>
<th>Energy Efficient</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>RPL</td>
<td>×</td>
<td>✓</td>
</tr>
<tr>
<td>CORPL</td>
<td>✓</td>
<td>×</td>
</tr>
<tr>
<td>CARP</td>
<td>✓</td>
<td>×</td>
</tr>
</tbody>
</table>

a. 6LoWPAN
IPv6 over low power wireless area network (6LoWPAN) is most popular protocol under this category. It encapsulates long header of IPv6 protocol in IEEE 802.15.4 packets which maximum size is 128 bytes. This standard introduces compression techniques to decrease transmission overhead, support multi hop delivery and fragmentation support to maintain maximum frame size of 128 bytes. Four types of header supported by 6LoWPAN frame: 6LoWPAN, mess, fragment and dispatcher header. If any frame does not follow specialization of 6LoWPAN network, then it will reject. Mess is used for broadcasting, the fragment is used to break the large IPv6 header to fit into 128-byte size and dispatcher is used for multicast and compression over IPv6 header (Jain, 2015).

b. 6TiSCH
It is a working group of Internet Engineering Task Force (IETF) developing a mechanism to distribute channel in TSCH (Time-Slotted Channel Hopping) mode. It consists a matrix where column represents the available frequencies and rows available time slots for network scheduling and the channel will be distributed according to this matrix. The matrix is partitioned into many chunks and known to all nodes in a network. There is a possibility that some nodes can have the same parameters, so to avoid this kind of situation node will negotiate so that each node will get a chance. This standard will not specify the scheduling techniques, so according to application requirements allow maximum flexibility to IoT application. The scheduling can be distributed or centralized depending on topology or application (Dujovne, Watteyne, Vilajosana, & Thubert, 2014).

c. IPv6 over G.9959
G.9959 supports a frame format, where 32 bits reserved for the network identifier (home network) that is given by a controller and 8 bit for node identifier that is assigned to each node. RFC 7428 introduce a frame format to transmit IPv6 packet over G.9959 packet, and support a level of security through shared key mechanism for encryption, but some applications required end-to-end encryption mechanism for maintaining the high level of security.
d. IPv6 over Bluetooth Low Energy
The Bluetooth Special Interest Group (BSIG) in Bluetooth v4.0 and an enhanced version in v4.1 introduced Bluetooth low energy. It is a radio technology, which is run on low power, such as battery power and it, attracts IoT applications such as environmental sensing, health monitoring, etc. Bluetooth LE using the same compression method as 6LowPAN and fragmentation feature is different from a 6LowPAN standard. It is achieved through sub layer L2CAP (Logical Link Control and Adaptation Protocol) which reassemble the large payload packet into 27 bytes. Bluetooth LE can use over small messages with low power (Niemänen, Savolainen, Isomaki, Patil, Shelby & Gomez, 2015).

Table 8. Network Layer Encapsulation Protocols Comparison

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Energy Efficient</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>6LoWPAN</td>
<td>✓</td>
<td>×</td>
</tr>
<tr>
<td>6TiSCH</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>IPv6 over G.9959</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>IPv6 over Bluetooth Low Energy</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
self to broker in the setup phase and get a key from the developer of an application according to required security level. When new data are formed, it is encrypted, published and send them to a subscriber by a broker. The encryption algorithm and set of keys are not standardized; SMQTT is introduced just to add the security feature in MQTT (Singh, Rajan, Shivraj, & Balamuralidhar, 2015).

3. **Advance Message Queue Protocol (AMQP)**
The Advance Message Queue Protocol (AMQP) is a session layer protocol, which in introduced for financial applications. It follows the same architecture (Publisher/subscriber) as MQTT and runs over TCP/IP protocol. In AMQP, broker functionality is divided into two parts: exchange and queue. The exchange processes the publisher message and organizes them into a queue according to roles and condition, which is predefined into the queue. Queues corresponding to the subscriber and the topics, whenever the data available in the queue then will get (OASIS, 2012).

4. **Constrained Application Protocol (CoAP)**
The Constrained Application Protocol (CoAP) is developed by the IETF working group to provide a lightweight interface. It is an application-layer protocol. REST (representational state transfer protocol) is a standard interface work between HTTP client and interface. As compared to light it application requirements, REST consumes more power and significantly overhead. The CoAP is introduced to match the IoT requirements such as low power overhead to operate sensors. CoAP architecture, functionality divided into two layers: messaging and request/response. The first sub layer is ensured the reliability and deal with the duplicity of the packet and request/response sub layer for communication. CoAP has four messaging nodes - conformable, non-conformable, piggyback and separate. Reliable and unreliable transmission represent by conformable and unconformable modes respectively, while piggyback used in the client/server model, where the server get a message sends the response directly with acknowledged the message. On the other side, the separate mode will use when server response within the message separate from the acknowledgment (Karagiannis, Chatzimisios, Vazquez-Gallego & Alonso-Zarate, 2015; Shelby, Hartke, & Bornmann, 2014).

XMPP was introduced for chatting and message exchange purpose and standardized by IETF many years ago. It is a standard and efficient protocol over the internet. Now, it is reusing the same standards because of its use XML, which make it easily extensible. It is a very efficient protocol over the internet and has been raised over the IoT application. XMPP can work on request/response, or publisher/subscriber architecture and developer can choose according to the development application. It is developed for near real-time application and provides efficient support for a small message. It does not provide any support for QoS. Therefore, it does not take place in M2M communication. Furthermore, XML involves a lot of tag format and headers, which cause for more power consumption. So, it is rarely used in IoT applications (Karagiannis, Chatzimisios, Vazquez-Gallego & Alonso-Zarate, 2015; Saint-Andre, 2011).

<table>
<thead>
<tr>
<th>Protocols</th>
<th>Security</th>
<th>QoS</th>
</tr>
</thead>
<tbody>
<tr>
<td>MQTT</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>AMQP</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>CoAP</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>DDS</td>
<td>×</td>
<td>✓</td>
</tr>
<tr>
<td>XMPP</td>
<td>✓</td>
<td>×</td>
</tr>
</tbody>
</table>

**V. COMPARISON AND CLASSIFICATION OF IOT RELATED SECURITY ATTACKS**

In this section, existing IoT related security work analyzed and categorized into two types: techniques that work on asymmetric key schemes and symmetric pre-distribution schemes. These techniques are isolated from standard IoT protocols, which are covered in the above section. In figure 5 taxonomy of security techniques according to cryptography schemes.

In table 10, we compare all these security techniques by considering the various attributes: energy, latency, complexity and bandwidth utilization. We use simple notations to compare the security techniques: '✓'—supported, 'blank means' – not applicable or not comparable and '×'—not supported.

In table 11 we consider six metrics to evaluate the solutions: Privacy, Authentication, Confidentiality, Denial-of-service (DOS), Integrity and end-to-end (E2E) Security. We define simple notations to evaluate the security services: '✓'—supported, 'blank means' – not supported.

**VI. RESEARCH CHALLENGES**

The concept of IoT has been extended to various domains of real life in order to solve various problems. It can be viewed as a combination of heterogeneous devices, sensor, actuator, etc. communicating with each other without very less human intervention and providing meaningful information to control and monitor situation for example: Patient monitoring, energy management, and traffic monitoring System. The applications of IoT can be constrained by resource limitation such as less computation power, limited energy, limited bandwidth, limited memory etc. Apart from above, challenges the applications developed using IoT concept are prone to security and privacy attack. The computing nodes/sensors are deployed in open environment and their communication is limited but vulnerable to attack. Further, the sensed data is collected at one key node and forwarded for analysis and monitoring purpose. This involves use of Internet quite often. So, in view of above scenarios a security framework or model for IoT application is desirable, where it has to be ensured that privacy and security of data cannot be compromised.
As mostly IoT applications are Real time and Energy constrained, the challenge to provide security to applications needs a balancing approach. The strategy for providing security should be adaptive in nature which changes according to the applications parameter such as energy, Timeliness, attack level, security level, Load in the system etc.

In IoT, standard is an important part. The standard development process and protocol should be open accesses to all, so that when new devices will introduce in network, existing standard can be modified to support new object and application. In today’s network paradigm, global standards are typically more applicable than any local agreements.

Therefore, it becomes an open and viable area of research and effort is required to develop a comprehensive security aware framework where the security level can be flexible and it is decided only after analyzing the network nodes parameters: Energy, Computation power, Attack level, Security level such that QoS feature of things and node-integrated network can be ensured.

VII. CONCLUSIONS

The objective of this survey is to present an explicit analysis of the traditional IoT security protocols, modified techniques, their approach and possible challenges over various attacks. There are numerous issues in IoT, such as user privacy, authentication, data confidentiality, DOS, integrity and end-to-end (E2E) security across network that must be resolve by IoT security techniques. Still, there are multiple security threats, which will be place in the Future IoT. Additionally, In IoT networks most of the devices are resource restricted and it is not only recommended to assure the security in network, but also to implement efficient techniques which balancing the requirements like computation power, energy, and QoS features of things and network, so that these techniques can be applicable to the real world scenarios.

This survey paper also provides a classification of existing security techniques and protocols relying on their key-based cryptography approach for assuring reliability in the IoT network. These techniques and protocols are examine for identify their advantages and limitation over energy and QoS features. Apart from that, this article also identify some research challenges for Future IoT so that organizations and researchers should tackle these problem and further research can be carried out in this direction.
Figure 5 Taxonomy of cryptography key classification.

Classification of cryptographic keys

Asymmetric key schemes

Symmetric key predistribution scheme

<table>
<thead>
<tr>
<th>Key transport based on public key encryption</th>
<th>Key agreement based on asymmetric techniques</th>
</tr>
</thead>
<tbody>
<tr>
<td>Raw public key encryption</td>
<td></td>
</tr>
<tr>
<td>Certification based encryption</td>
<td></td>
</tr>
<tr>
<td>Identity based encryption</td>
<td></td>
</tr>
</tbody>
</table>

Deterministic key distribution

Probabilistic key distribution

Offline key distribution

Server assisted server

External assisted server

Proxy-based assisted server

(Sarikaya et al., 2012)
(IoT (Raza et al., 2013) (Hummen et al., 2013)
(Szczechow uak et al., 2009) (Yang et al., 2013) (Nicanfar et al., 2011)
(Yang et al., 2013) (Meslenauer et al., 2008) (Moskowitz et al., 2012)(Gos wami et al., 2014)
(Eschenauer et al., 2012)
(Du et al., 2006; Blom et al., 1984)
(Raza et al., 2011)
(Bhattacharyya et al., 2015)
(Saied et al., 2012)
(Hussen et al., 2013)
(Vucinic et al., 2015)
Table 10. Summary of Proposed Security work and their key Techniques for IoT.

<table>
<thead>
<tr>
<th>Protocol/References</th>
<th>Briefdescription</th>
<th>Energy Efficiency</th>
<th>Latency</th>
<th>Complexity</th>
<th>B.W. utilization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Bootstrapping Solutions for Resource-Constrained Devices</td>
<td>This document give an idea how to securely configure the resource constrained device networks at initial stage and bootstrapping architecture, security methods and communication channel are described.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>A lattice based authentication for low-cost RFID (Moustaine et al., 2012)</td>
<td>Author proposes an NTRU-based scheme for RFID tag (low-cost), and a lightweight mutual authentication protocol based on pre-NTRU’s adaptation. This solution covers the security and privacy related requirements for RFID systems.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Lightweight secure CoAPs for the IoT: Lithe (Raza et al., 2013)</td>
<td>Author presents Lightweight Secure CoAP for the IoT (Lithe) — a combination of DTLS and CoAP for the IoT. With Lithe, additionally give a novel DTLS header compression scheme that aims to decrease the energy consumption by leveraging the 6LoWPAN standard. DTLS header compression scheme does not compromise the end-to-end security properties. Simultaneously, it greatly reduces the number of data bytes while maintaining DTLS standard compliance.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Certificate-based authentication for the IoT (Hummen et al., 2013)</td>
<td>Author proposes these methods to decrease the overheads of the DTLS handshake. These methods are based on pre-validation, handshake delegation and session resumption.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Establishment of ECC-based initial secrecy usable for IKE implementation (Ray et al., 2012)</td>
<td>Author proposes a new flexible approach for reducing the complexity and security improvement of the IKE implementation.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Identity-based encryption for heterogeneous sensor networks: TinyIBE (Szczechowiak et al., 2009)</td>
<td>Author proposes an efficient security bootstrapping mechanism for heterogeneous Sensor Networks that base on Identity-Based Encryption and exploits the enhanced capabilities of high-end cluster heads. Propose asymmetric security scheme provides authenticated key distribution without using expensive certificates.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Authenticated Pair-wise Key using Identity-based Cryptography (Yang et al., 2013)</td>
<td>This technique stand on the elliptic curve Diffie-Hellman (ECDH). It can effectively protect from various attacks: man-in-the-middle attacks and node-capture attacks through encrypting the exchanged parameters using identity-based encryption.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Elliptic Curve Diffie-Hellman - Elliptic Curve Digital Signature Algorithm (ECDH-EDDSA) (Meulenaer et al., 2008)</td>
<td>Author verify the energy cost of cryptographic protocols, both from a computation point and a communication of view based on practical measurements on the MICAz and TelosB sensors. Author focus on the cost of two key agreement protocols: Kerberos and Elliptic Curve Diffie-Hellman key exchange with authentication provided by the Elliptic Curve Digital Signature Algorithm (ECDH-EDDSA).</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>HIP Diet EXchange (DEX) (Moskowitz, 2012)</td>
<td>HIP is introduced to provide secure authentication of hosts. HIP also explore to limit the exposure of the host to various attacks denial-of-service and man-in-the-middle (MitM).</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
### Key-Management Scheme for Distributed Sensor Networks

**Eschenauer et al., 2002**

Author presents a key-management scheme designed to satisfy both operational and security requirements of DSNs. The scheme includes selective distribution and revocation of keys to sensor nodes as well as node re-keying without substantial computation and communication capabilities. It relies on probabilistic key sharing among the nodes of a random graph and uses simple protocols for shared key discovery and path key establishment, and for key revocation, re-keying, and incremental addition of nodes.

### A Key Predistribution Scheme for Sensor Networks Using Deployment Knowledge

**Du et al., 2006**

Author proposes a novel random key pre-distribution scheme that exploits deployment knowledge and avoids unnecessary key assignments and the performance including memory usage, connectivity and network resilience against node capture of sensor networks can be substantially improved with the use of our proposed scheme.

### An Optimal Class of Symmetric Key Generation Systems

The purpose of this paper is to provide a class of SKGS for which the amount of secret information needed by each user to generate his keys is the least possible while at the same time a certain minimum number of users have to cooperate to resolve the uncertainty of unknown keys.

### D-HIP: a distributed key exchange scheme for HIP-based IoT

**Saied et al., 2012**

Author proposes a distributed lightweight key exchange protocol designed to reduce the requirements of HIP Base Exchange, in order to be supported by resource-constrained nodes.

### SAKES: secure authentication and key establishment scheme

**Husson et al., 2013**

Author proposes Secure Authentication and Key Establishment (SAKES) scheme for the machine-to-machine (M2M) communication in the 6LoWPAN. SAKES light weight public key during the session establishment processes and pairwise key for node authentication.

### BROSK (Lai et al., 2002)

BROSK protocol: To make link dependent keys by broadcasting key negotiation messages.

### An Measurement Transmission Scheme for Privacy Protection

**Li et al., 2013**

Author proposed a Ring Communication Architecture (RCA). This technique which assure customers’ privacy by using the ortho code.

### Energy-efficient Physical Layer Packet Authenticator

**Bartoli et al., 2013**

In this method, verification test will conduct at Physical layer to challenge exhaustion DoS attacks and this technique is able to reject non-intended packets without the need to their total reception.

### Lightweight Establishment of Secure Session

**Bhattacharyya et al., 2015**

This is a novel lightweight cross layer approach for session establishment and interchange of application layer message through a secure channel.

### Object Security Architecture

**Vucinic et al., 2015**

OSCAR: Architecture provides End-to-End security in IoT network and work on the concept of object security and relative security with the application payload.

### Securing Communication in 6LoWPAN with Compressed IPSec

**Raza et al., 2015**

This technique offer secure communication (End-to-End) between the internet and IP enabled sensor network in 6LoWPANs.
Securing Intra-Communication in 6LoWPAN: A PKI Integrated Scheme (Goswami et al., 2014)

A public key infrastructure (PKI) enabled scheme with database system, which contains the required keying information about all the network nodes.

Smart Grid Authentication Scheme (SGAS-I) Authentication and Smart Grid Key Management (SGKM-I) for Unicast and Multicast Communications (Nicanfar et al., 2011)

A novel key management and mutual authentication protocol for establish a link between the utility server and customers smart meters so that communication can take place. This protocol secure from various attacks like Brute-force, DoS and Man-In-The-Middle Replay attacks.

<table>
<thead>
<tr>
<th>Author</th>
<th>Privacy</th>
<th>Authentication</th>
<th>Confidentiality</th>
<th>DDoS</th>
<th>Integrity</th>
<th>E2E Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sarikaya et al., 2011</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Moustaine et al., 2012</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✔</td>
</tr>
<tr>
<td>Hummon et al., 2013</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✔</td>
</tr>
<tr>
<td>Rana et al., 2013</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✔</td>
</tr>
<tr>
<td>Kay et al., 2012</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✔</td>
</tr>
<tr>
<td>Szczesniak et al., 2012</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Yang et al., 2013</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>De Meulenaar et al., 2006</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Moskowitz et al., 2012</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Eschenauer et al., 2002</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>De et al., 2006</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Du et al., 2006 , Huang et al., 1984</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Saito et al., 2012</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Huang et al., 2013</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Lai et al., 2002</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Li et al., 2013</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Rautkari et al., 2013</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Venter et al., 2015</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Rana et al., 2018</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Goswami et al., 2014</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Nicanfar et al., 2011</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✔</td>
</tr>
</tbody>
</table>

Table 11. Summary of Proposed Security Methods for IoT.

Low: •

High: ✫
References


[73] Zhao, K., & Ge, L. (2013, December). A survey on the internet of things security. In Computational Intelligence and Security (CIS), 2013 9th International Conference on (pp. 663-667). IEEE.


