CHAPTER 2

BACKGROUND AND LITERATURE SURVEY

This chapter explains the background study of secure RPL routing over IoT. It also classifies and compares the routing techniques and various types of RPL attacks in IoT. Further, it comprehensively surveys the papers related to secure RPL routing in IoT.

2.1 Fundamentals of IoT

Initially, the IoT is named the Internet of Everything (IoE) (Jorge et al., 2015) (Ibarra et al. 2017). The IoT devices are unique identifiers that can transmit data over a network by enabling internet assisted communication among physical and virtual things with or without human interactivity. The IoT also offers an efficient way to learn the interaction between devices that are interconnected through the internet (Rolf and Romana, 2010). The IoT devices are mostly sensors, intelligent vehicles, actuators, and other smart devices. Thus, the IoT extensively interconnects the devices for offering more intelligent services in the smart world. The IoT is not a solitary technology in which diverse technologies are agglomerated and perform the network task in a tandem manner. The widely interconnected devices create a wide variety of short-range networks that are vehicular ad hoc, wireless sensor, radio frequency identification, wireless fidelity, Zigbee, and Bluetooth (Bandyopadhyay and Sen 2011). Hence, it is essential to build efficient IoT architecture for providing a sequence of communication among such devices. The IoT devices are heterogeneous, and the resources of such devices such as memory, battery power, and processor capability also heterogeneous. Due to the nature of heterogeneity, the IoT offers diverse communications such as device to device and device to human. The communicating range of IoT devices is limited and the data is delivered in a single or multi-hop manner. In single-hop communication, the communicating devices are within the range and there is no need to relay the devices for data delivery. In contrast, the devices out of communication

range necessitate relay devices for successful data delivery (Mercy and Pravin, 2014). Also, the retrieved data in IoT also heterogeneous and it is crucial to deliver the data in an intelligent way.

2.1.1 IoT Architecture

Due to the heterogeneity and different kinds of large scale technologies, there is no globally agreed consensus architecture for IoT (Ning and Wang, 2011). Various researchers present diverse kinds of architecture (Mashal et al., 2015) (Said and Masud, 2013). The fundamental IoT architecture is the three-layer architecture. The three-layer architecture incorporates the physical, network, and application layers (Wu et al., 2010) (Khan, 2012). Such architecture only defines the IoT basic structure, but it is not enough for providing smart services to the IoT. For that, the five-layer IoT architecture includes two additional layers named as processing and business. Typical five-layer IoT architecture is depicted in figure 1.

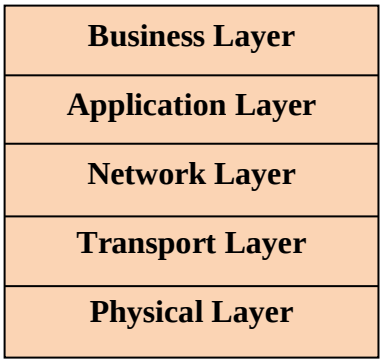

Figure 2.1: Layered IoT Architecture

In IoT architecture, the first layer is the physical layer that includes smart devices like a sensor to monitor the environmental activities. It finds the physical parameters in the environment. The transport layer transmits the observed data of the physical layer to the network layer through any one of wireless technologies like local area networks, Bluetooth, and other short-range networks. The network layer connects the smart devices and servers for processing and forwarding the observed data. Consequently, the application layer delivers the user-defined smart application services like smart homes, healthcare, and modern cities. Finally, the business layer is

responsible for managing the entire IoT system, such as application services and user personal information preservation.

2.1.2 IoT Technologies

IoT technology comprises a large number of heterogeneous devices, and they involve many technologies to deploy and manage IoT devices (Zeng et al., 2011). Diverse IoT technologies are utilized in real-time and such technologies promote the IoT evaluation significantly. Some of the IoT technologies are as follows.

Internet Protocol Version 6 (IPV6): It is an excellent enabler for an IoT which is evaluated over Internet Protocol Version 4 (IPV4) (Savolainen et al., 2013). The IPV6 protocol offers Internet Protocol (IP) address of the IoT devices. In recent years, most of the IoT devices support IPV6. The IPV6 is a 128-bit addressing protocol, and it abundantly handles a considerable amount of IoT devices.

Radio Frequency Identification (RFID): It is a type of IoT technology utilized to determine the device and people (Liu et al., 2008) (Mitrokotsa and Douligeris, 2009). It is also used to label the devices, and the RFID includes tags, software drivers, and applications.

Wireless Sensor Network (WSN): It is a network that is formed by sensor nodes with the ability to monitor the environmental conditions such as pressure, humidity, temperature, pollution levels, wind speed, intensity levels of various parameters, and vital body statistics (Lazarescu, 2016) (Jiang, 2013) (Al-Turjman and BD, 2019).

Wireless Fidelity (Wi-Fi): It is a short-range wireless technology that connects the smart devices to the internet wirelessly and locally. In the modern world, Wi-Fi connects smart phones, computers, digital cameras, laptops, and personal digital assistants to internet access points through wireless connections (Tozlu et al., 2012).

Bluetooth: It is an IoT technology that is enabled in different mobile operating systems such as android, windows, Linux, and blackberry (Chang, 2014). It is a better technology for IoT, as it enables the devices with lower energy consumption and also offers a better-quality level in communication.

Zigbee: It is a type of IEEE standard interface which is suitable for high-level communication routing protocols that are utilized to design Personal Area Networks (PAN). The Zigbee is a basic of IoT, and it offers features such as self-regulating, low power, and low cost (Han and Lim, 2010) (Hancke et al., 2012).

2.1.3 IoT Applications

The IoT offers several types of smart applications that make the human lifestyle better. The IoT applications are smart homes, smart cities, smart water, social life and entertainment, healthcare systems, smart agriculture, and energy conservation.

Smart Homes: It has become prevalent in today's world, as the sensor network embedded for home automation is grown-up significantly (Robles and Kim, 2010). In addition to that, the peoples believe the IoT technology to address their security-related issues and also improve their living quality. For that, the IoT system with various sensors is exploited in many homes for enabling smart and automated security services to the users. Smart home technology allows household appliances to be remotely monitored and controlled using smart phones, tablets, or laptop computers to achieve a comfortable and safe home environment. The smart homes require regular interaction with their internal and external environments to provide accurate decisions. Due to its high popularity and consideration of sensitive information about users, smart home technology is faced with significant risks to security and privacy. With the growth in information technology, the development of smart homes with lower prices and intelligence environments to make complex decisions remains a challenge. Thus, there is a requirement of a large number of interconnections among sensors for collecting data in real-time.

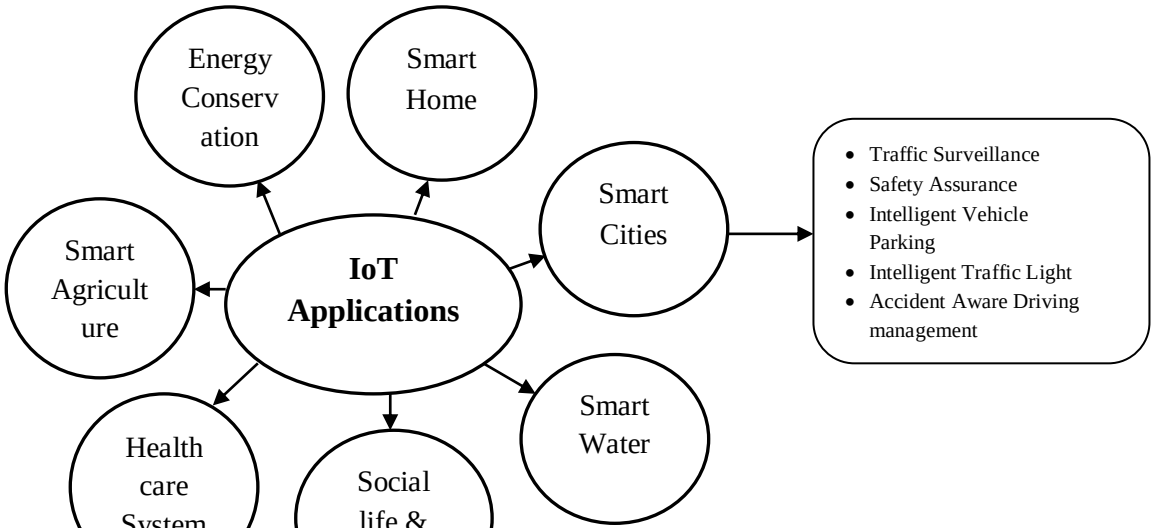

Figure 2.2: IoT Applications

Smart Cities: The smart city incorporates a huge type of applications such as traffic surveillance, safety assurance, intelligent vehicle parking management, intelligent traffic light, and accident aware driving management (Talari et al., 2017). Such smart city applications mostly exploit smart phone sensors like Global Positioning System (GPS), Google maps and accelerators for detecting vehicle moving patterns, accident detection, and the congested area of the city (Zanella et al., 2014) (Hancke et al., 2012) (Kyriazis et al., 2013).

Smart Water: Water scarcity is the major issue in today's world and it is crucial to handle the water resources efficiently. An intelligent solution for water management is to place smart meters over water pipelines and storm drains. Such smart meters assist in predicting the flooding previously and also preserves the humans from natural destruction.

Social Life and Entertainment: It plays a significant role in every human life day by day. Many smart phone applications are developed, and they are used to track human activities. It assists people in making better interactions with each other for a social purpose.

Healthcare Systems: Numerous wearable IoT devices are specially developed for healthcare monitoring purposes (Dziak et al., 2017) (Riazul et al., 2015) (Baker et al., 2017). Such a smart health care system is highly benefited for monitoring and improving the health condition of a human (Krishna and Sampath, 2017). **:** IoT plays a significant role in healthcare applications such as remote monitoring, elderly care, mobile personal assistants, and telemedicine in order to achieve a hassle-free health monitoring for both the users and medical professionals. However, these applications majorly affect the security and privacy of the user data due to the transmission of sensitive information through the wireless medium. In addition, the other benefits of IoT in the healthcare domain are tracking patients, staff, and objects, identification and authentication

of people, automatic data collection and sensing. Thus, IoT provides a considerable solution in providing a ubiquitous healthcare using wearable sensors that measure physiological parameters and uploads the data to servers and smart phones for communication. The advantage of the IoT paradigm in healthcare applications is that it specifies a way to monitor, store and utilize health providing ubiquitous and customized services for personal needs on a 24/7 basis.

Smart Agriculture: In agriculture, the parameters like temperature and humidity are severely affecting agriculture performance (Ayaz et al., 2019). In order to produce agriculture and improve the yields, the farmers utilize IoT enabled sensors to measure the environmental factors. Smart agriculture focuses on applying advanced features in agriculture sectors for achieving high yields and saving farmers from monetary losses. The role of smart agriculture includes soil moisture monitoring, humidity and temperature control, micro-climate condition control, and selective irrigation in dry zones, attacks of wild animals and thefts, field management, movement of the unwanted object. In precision agriculture sensor monitoring networks, agri-related information like temperature, humidity, soil PH, soil nutrition levels, and water level are measured and collected through sensors. Then, farmers are able to remotely monitor these measurements about their crops and equipment through phones and computers. Apart from this, the data collection through sensors provides updates about different environmental conditions that play a crucial role in crop productivity.

Energy Conservation: The intelligent communication IoT technology also improves power generation, conservation, and management system (Kyriazis et al., 2013). The intelligence of the smart grid system maximizes the power usage efficiency in smart homes by exploiting several types of sensors. Smart grid technology is employed in the power generation and distribution for houses and buildings with the aim of optimally and efficiently delivering the highest quality of energy at the lowest cost possible. In the smart grid, the smart meters are connected to sensors that continuously monitored, thereby sending data related to power consumption to the central server. The central server analyses the consumption pattern of the devices to improve productivity and achieve transient power targets. The major threat in smart grid is the security issues that include software vulnerabilities, network configuration vulnerabilities, network perimeter vulnerabilities, network communication vulnerabilities (Dalipi and Yayilgan, 2016). Therefore, there is a necessity of adopting and enhancing adaptive security mechanisms for complex systems that enables real-time security monitoring of grid operations for preventing

failures of security protections. The physical damages and disaster recovery plans, such as backup and contingency plans are to be included to make secure systems from natural calamities.

Intelligent Transportation Systems (ITS): The objective of ITS is to monitor and control the transport network by integrating computation and communication. The ITS achieves the better reliability, efficiency, availability, and safety of the transportation infrastructure. The role of IoT in ITS includes theft vehicle detecting system, prioritized vehicle scheduling, non-stop toll collecting system, traffic violation monitoring, traffic flow prediction, and congestion avoidance, and so on. The essential factor that needs to be focused on the ITS application is privacy protection in terms of managing transportation and highway security. In certain situations, these applications require systematic vehicle-vehicle communication or communication between vehicles and back-end servers. However, these applications require highly accurate and reliable real-time information as long delays and errors in the information provided by sensors lead to life-threatening situations for both assisted driving and self-driving vehicles. Due to the high possibility of malicious intrusions, the received messages have to be verified against any harmful or crashing entities and the malicious ones have to be removed from the network.

Retail and Logistics: IoT plays a significant role in supply chain management with applications such as error-free and quick stacking and loading operations, observing storage conditions throughout the supply chain, real-time product tracking, payment processing based on location or activity period in public transport, theme parks, gyms, and others. The IoT applications in the retail industry support both the front-end and back-end operations with assistance to control and identify the subsequent destination of goods/raw material. The Real-time tracking of logistics entities is performed by combining the capabilities of RFID, mobile devices, and the integrated browser interface. In large logistics enterprises, humans are replaced by robots for improving the efficacy in locating and moving assembly parts automatically.

2.2 IoT Routing

In order to enhance the life quality level of humans, IoT offers different kinds of application services in diverse environments. Due to the heterogeneity, the IoT devices produce an enormous amount of data, and hence, it is crucial to route the data among such devices according to the applications. In real-time, the IoT devices are resource-constrained in nature and it is very

tedious to route the information generated by heterogeneous devices (Tavakoli and Dawson-Haggerty 2009). The IoT routing issues also increases due to low energy and lossy links.

2.2.1 Designing Challenges of RPL Routing in IoT

IoT devices are generally resource-limited in terms of size, memory, processor, and battery power. It is a highly challenging task to ensure the desired level of quality of service according to the data type and application type. Additionally, the IoT devices are distributed on diverse geographical location and the IoT communication is mostly wireless communication. In IoT, routing the information among smart devices is essential, but it is very tedious in real-time, as the smart devices have unique characteristics. To provide appropriate routing services for low power lossy networks, the RPL routing has been proposed (Mercy and Pravin Renold, 2014). Further, the significant designing challenges of RPL routing in IoT are summarized as follows.

Mobility: The majority of the IoT devices are mobile in a realistic environment (Oliveira and Vazão, 2016). Thus, the devices continuously change their locations, and it is difficult to predict the locations of such devices for the route information. It also makes the IoT routing is challenging due to network dynamics.

Data Reliability: The IoT includes a lot of real-time applications in which some of the applications are time-sensitive. In IoT, the data may be lost due to unreliable wireless links. Hence, it is essential to deliver the information in a timely manner without reducing the quality of service.

Node Deployment: The sensor network is an essential component of IoT. On the contrary of traditional networks, the IoT needs to know the location of devices and also place the sensors in the exact location before implementing it. Therefore, node deployment plays a significant role in sensors based on IoT routing.

Device Heterogeneity: Based on the type of applications and network standards, the IoT devices differ in characteristics. Additionally, they are varied in terms of resources such as memory, size, processor, and battery power. The design of IoT routing should consider the device heterogeneity for attaining better routing efficiency.

Power constraints: Generally, the IoT devices are power limited, and the routing should consume a significant amount for power to successfully deliver the data among heterogeneous devices. Therefore, it is crucial to exploit the power resources of IoT devices efficiently.

Scalability: IoT technologies support both wired and wireless communication. Despite that, most of the communication is wireless, and the smart devices involved in the communication are either stable or mobile. Such devices are periodically entered and left in the network and thus, the scalability issues lead to routing performance degradation.

Diverse networking standards: IoT incorporates different technologies such that are wireless sensors, Zigbee, WiFi, and Bluetooth (Zeng et al., 2011). The diverse technologies utilize various protocol stacks based on their working principles. It is crucial to consider the network standards in routing protocol design.

Intermittent connectivity: The network connectivity is severely affected by two parameters that are device mobility and battery power. Due to constrained battery capacity, the communication links between two devices may break, and thus, it reduces the routing efficiency. Also, the devices move with high mobility cannot provide stable links for communication. Moreover, it is tedious to ensure connectivity in IoT.

Multi-hop communication: The communication range of smart devices is limited, and they require intermediate devices to relay the data to the desired destinations. Mostly, multi-hop communication is performed in IoT, and the routing protocol can support multi-hop communication.

Fault tolerance: The IoT devices are affected by environmental factors such as temperature and humidity. Thus, it reduces the routing performance considerably. Therefore, the routing protocols can manage such unpredictable events

Security: Many devices are participating in the routing process. Since some devices behave dishonestly in routing for improving their benefits. Therefore, it is essential to develop security-based routing solutions for IoT. Most of the current IoT routing techniques exploit lightweight cryptographic techniques for ensuring security. However, they lack to provide complete security in IoT due to the unique features.

2.3 Security in IoT Routing

RPL is an effective routing protocol utilized for IoT (Mercy and Pravin, 2014). The RPL routing protocol determines the routing paths between a source-destination pair as soon as possible. Currently exploited RPL for IoT is used key-based applications in pre-designed smart devices. However, the security level of RPL is weak, and it lacks to attain better performance under secure mission-critical applications. Moreover, the RPL protocol is susceptible to various types of routing attacks as the same as the sensor network, and also vulnerable to the attacks against the IoT. Most of the researchers define the security requirements of RPL over IoT, whereas there are no appropriate security solutions for such networks. Therefore, it is worth to analyze the routing attacks against RPL and it is essential to propose high RPL security against such attacks. Some of the RPL routing attacks such as route counterfeiting, message replay, version number falsification, Denial of Service (DoS), black hole, grey hole, Sybil, and selective forwarding (Wallgren et al., 2013). IoT requires the security measures of traditional networks, as the IoT in the real-world is envisioned by connecting the heterogeneous devices and various technologies with the internet. Thus, it significantly increases the security demands associated with an IoT. The malicious device not only modifies the contents of messages but also takes control of an entire IoT system. The advanced technologies of IoT devices also pose several new security threats. In general, the routing path is established when information is transmitted to a destination node. The route is established in a hop-by-hop manner until the data reaches the destination. Further, the roués are maintained or deleted according to the protocol process. In such routing, a misbehaving node may insert false information or dropping the messages for their benefits. For instance, a particular node transmits a vast amount of false amount to its neighboring node for creating the overflow in the routing table. Such malicious activities deny the real routed by occupying the routing table with spurious routing information. Such activity also drains the battery power of neighboring nodes quickly, resulting in reduced network performance. Therefore, a secure IoT routing algorithm is essential to detect and isolate such malicious activity from the network.

2.3.1 Security Requirements of IoT

In past years, the security requirements of IoT are divided into three categories that are confidentiality, integrity, and availability. The term confidentiality ensures that an authorized

party only accesses the network services. It is necessary to assure confidentiality in IoT, as the IoT offers sensitive applications like healthcare automation and smart finance system. Secondly, the term integrity assures that any attackers do not modify the received information in the network. It also differentiates the information errors that occurred due to network factors such as lossy links and mobility or attack behaviors. Finally, the term availability guarantees the availability of network resources to authorized users. Moreover, the IoT routing protocol ought to satisfy the fundamental security requirements for enhancing IoT performance. The IoT networks have mostly similar characteristics of the sensor and multi-hop wireless networks, and it faces attacks similar to conventional networking attacks. Some of the RPL attacks and their properties are explained in the following table.

Table 2.1: Comparison of Various Types of RPL attacks over IoT

Attacks	Description	Security Issues	Impact on Performance
Rank (Raza et al., 2013)	Aims to generate non-optimal paths and loops for routing	Confidentiality and Integrity	Reduces the packet delivery ratio and increases the delay
Sinkhole (Raza et al., 2013)	Compromises the nodes bypassing vast traffic via the attacker		High packet loss and delay in data delivery
Wormhole (Perazzo et al., 2018)	Disrupts the routing topology and the data traffic flow in the network		Inaccurate routing path discovery and high packet loss
Sybil and Clone ID (Wallgren, 2013)	Perform node compromise to disrupt routing paths and prevents		Reduced Routing Efficiency

	the traffic from reaching the destination		
Version number (Dvir et al., 2011)	Aims to change the version number and launching attacks		High control overhead, minimum packet delivery ratio, and a maximum end to end delay
Local repair Control overhead (Le et al., 2012)	Disrupts the control and data traffic flow		Routing performance degradation
Selective Forwarding (Wallgren, 2013)	Aims to disrupt routing functionalities		Diminishes routing efficiency
Hello flooding (Wallgren, 2013)	Aims to drain the battery power of devices quickly	Availability	High energy dissipation and poor network connectivity
Denial of Service (Kasinathan et al., 2013)	Denies the network services and makes the resources unavailable to nodes		Affecting data quality and unnecessary energy depletion at neighboring nodes
DODAG Information Solicitation (DIS) (Perrey et al., 2013)	An attacker aims to broadcast DIS messages continuously		Minimized packet delivery ratio, high packet delay, and High resource consumption
Neighbor attack (Perrey et al.,	Erroneous route discovery and route	Availability, Confidentiality	High resource consumption at

2013)	disruption activities	& Integrity	neighboring nodes
Blackhole (Jiang et al., 2018) (Ahmed, and Ko, 2016)	Aims to drop packets or increases the route traffic		Increases the control overhead and decreases the packet delivery ratio

2.3.2 Trust-based Secure IoT Routing

Trust is the affiliation of two devices that involve in the communication process (Djedjig et al., 2015) (Djedjig et al., 2017). A device that desires to estimate the trust value of other device named as trustee is known as trustor. The trust is categorized under three different categories fundamental, situational, and general. Essential trust is primarily from the past routing interactions of two communicating nodes. The situational trust is nothing but it is a trust value estimated based on the experience that is collected from various nodes. General trust is a trust value of a node in a particular situation. In networking, trust-based security is an important topic, as most of the routing protocols exploit trust models to detect the misbehaviors and improves the network performance. For accurate trust evaluation, the nodes have to collaboratively and cooperatively perform the network operations, but it is challenging in real-time. Selecting the routers based on trust motivates the nodes to behave honestly in the routing process and thus, it enhances the network performance significantly. Moreover, trust-based secure routing improves the reliability level of devices in a system. It mainly pinpoints the troubles that affect the trust efficiency level and also helps to detect the malicious areas that reduce the efficiency of network operations. The trust-based security solutions over sensor networks are highly suitable for IoT sensor nodes, as they have lightweight and resource-constrained nodes. For sensor network security, numerous security techniques have been introduced which are entropy-based, Bayesian theory-based, fuzzy logic-based, probability-based, particle swarm intelligence-based, Markov chain based, weight-based, and game theory-based (David et al., 2016).

Entropy-Based Trust: It evaluates trust based on the routing behaviors of nodes and also takes into account the probabilistic distribution. Further, it selects the nodes with the highest trust

probability for decision making and it selects a high-security path that includes high trustworthy nodes as routers for data delivery.

Bayesian theory-based Trust: In this type, the trust is estimated using Bayes theorem that predicts the probability values of an even. Further, it collects evidence from the various nodes for efficient decision making. It estimates the trust degree based on the evidence.

Fuzzy logic based Trust: This method calculates the trust in a multi-valued logic structure that determines the truth value by providing multiple levels of logic values. Finally, it exploits the binary logic model to compare the trust values like 0 or 1 and decides the trust level of nodes.

Probability-Based Trust: It utilizes the probability distribution of trust values for randomly analyzed to determine the node behavior. The indispensable entity of probability theory is random variation and routing behavior observation of nodes.

Particle Swarm Intelligence Based Trust: This model evaluates the trust values by collecting the neighboring nodes of a node and also calculates the final trust value locally. It exploits the concept of living things biological ecosystems in a specific environment.

Markov Chain Based Trust: It is a key management based trust model in which the trust values and trust certificates are evaluated using the key models. The Markov trust model calculates every one-hop neighbor's trust based on the routing history information. Finally, it chooses a highly trustworthy node as key management authority for trust evaluation.

Weighted Based Trust: It takes into account the product values of trust as reputation values. It observes the node behavior for a particular time interval and assigns weights to such values for final trust evaluation. The aggregated trust values are a final trust value of nodes in the weight-based trust model.

Game Theory Based Trust: This model considers the nodes as players and designing player strategies among such nodes (Duan et al., 2014). It takes a decision based on the strategies of best trust values. It is a fabulous trust evaluation method, as it evaluates accurate trust values of nodes by employing the best trust values of player strategies.

2.4 Literature Survey of Secure IoT Routing

The IoT routing requirements are varied due to the specifications of the application and device heterogeneity of IoT networks. Also, the IoT devices have limited resources such as the battery,

memory, size, and processing capabilities. Such IoT characteristics are vulnerable to several types of stacks in RPL over IoT. The work in (Wallgren et al., 2013) surveys the RPL attacks in IoT.

2.4.1 Survey of RPL Routing Protocols in IoT

The works in (Mercy and Pravin, 2014) and (Jeonggil et al., 2011) introduce a Routing Protocol for Low-power and Lossy networks named RPL. The RPL is a fundamental routing protocol for LLNs and IoT. The RPL protocol tries to reduce the control messages and total energy conservations in limited resource networks. Reliability is an essential requirement of IoT routing. The reliability is attained by reducing the packet loss and minimizing the delay in packet delivery. The work of (Dawans et al., 2012) achieves rich QoS in data delivery by enhancing the routing decision efficiency. A reactive routing method has been proposed in (Sobral et al., 2019). Instead of exploiting control messages for link quality selected, the reactive approach selects the high-quality links based on the number of data packet reception. Thus, it enhances network performance. The work in (Ancillotti et al., 2014) and (Ancillotti et al., 2014) evaluate the link quality based on cross-layer methods and they are highly suitable for RPL. Such a link quality model reduces the end-to-end delay and energy dissipation at nodes without reducing the routing efficiency. The work in (Chze and Leong, 2014) presents a secure multi-hop routing protocol (SMRP) for IoT communication. The SMRP provides the security of the IoT devices by authenticating the devices before join and leave from the network. For authentication purposes, the SMRP includes multi-layer parameters into account. Thus, it increases the overhead in the network. Moreover, the SMRP is not suitable for large scale IoT networks. Some of the RPL routing protocols are comparatively discussed in Table 2.2.

Table 2.2: Comparison of Various Types of RPL Routing protocols for IoT

Routing Protocol	Description	Advantages	Disadvantages	Application Type
RPL (Mercy and Pravin,	try to minimize the control messages	Low energy dissipation at	Changes need in fundamental	Resource limited IoT

2014)	traffic	resource limited network	protocol design Scalability issue	applications
Co-RPL (Gaddour et al., 2014) (Gaddour et al., 2015)	Routing solution by employing a corona mechanism	Alternative route discovery mechanism and improves routing efficiency	Requiring some changes in RPL default messages and requires a routing table extension	Smart mobile sensor network
Mod-RPL (Gara et al., 2015)	Aims to modify the RPL to control the mobile node operations	Minimizes the control message traffic	Not suitable for high mobility nodes	Medical automation applications
DualMOP-RPL (Ko et al., 2015)	Modifies the control messages of RPL for enhancing the operational efficiency	Rectify the interoperability issues exist among two mobile devices	High complexity	Heterogeneous device application
LOADng-CTP (Yi and Clausen, 2014)	Forms a bidirectional tree by inaugurating proactive routing features in LOADng	Significantly minimizes the overhead and delay in the network	Requiring high memory for implementation	Nil
CLRPL (Taghizadeh et al., 2018)	Creates novel methods that taking into account the link quality and energy level of nodes in parent node selection	Improves the packet delivery ratio and diminishes the energy consumption	High memory usage and high delay	Large scale applications with high traffic load
FQA + FSBRC (Sobral et al.,	Designs a novel protocol with tag reading that exploits	High-quality route selection with the help of RFID	High complexity for IoT devices	RFID and LLN enabled IoT devices based

2018)	a fuzzy model in route selection	enabled IoT devices		applications
LOADng-IoT (Sobral et al., 2019)	Aims to introduce a novel mechanism for route discovery among IoT devices	Reduces the overhead of route discovery process	Route catch requires high memory	Heterogeneous internet required IoT devices

2.4.2 Survey Related to Secure IoT Routing Protocols

The fundamental RPL protocol offers security against external attackers like topology-based attacks. Since there is a chance to compromise the internal nodes and obtains security keys of various devices for launching internal attacks. There is not a valid RPL protection mechanism against internal attacks (Vasseur et al., 2011) (Winter et al., 2012) (Chen et al., 2012). For a detailed study, the secure IoT routing protocols are classified into cryptography based and IDS based security solutions. A common technique named as digital signature provides secure authentication services in the sensors of IoT. In the digital signature model, every node necessitates a pair of public and private keys to inaugurate the signing process and other activities respectively. The public key cryptosystem is mainly classified into Identity-Based Cryptography (IBC) and Public Key Infrastructure (PKI) based on the key provisioning models. A public-key cryptosystem is a centralized approach that needs the centralized authority for providing and managing the keys. Additionally, nodes should have to interact with trusted authority before establishing secure communication. In (Nikravan et al., 2018), the RPL routing strategy has been proposed against two various topological attacks that are version number and rank spoofing. For detecting such attacks, the RPL strategy introduces a lightweight security solution that employs offline signatures for attack detection. In order to overcome the issues of cryptography security solutions, machine learning-based approaches are introduced. In (Pu and Hajjar, 2018), a monitor based mechanism named as CMD has been proposed for efficiently detecting the forwarding misbehaviors. Further, the CMD investigates the potential of forwarding misbehaving nodes and its impact on the RPL with low power and lossy networks.

A multi-level intrusion detection system has been proposed in (Alaparthy and Morgera, 2018). It exploits an immune theory referred to as danger theory for ensuring security over resource-limited wireless sensor networks. A COLlaborative Intrusion DEtection (COLIDE) framework has been proposed for IoT (Azad et al., 2018). The COLIDE collects the most useful information from the device and the network layer for detecting the misbehaviors. Based on the designing type, the COLIDE is classified into two layers that are edge routing and the device layer. In CoLIDE, the device monitors the node behaviors and sends a report to the edge routing layer for aggregately performing the attack detection process. Further, it permits multiple devices to generate a false event alarm and ensuring high security. By believing the events with multiple correlated alarms, the COLIDE improves false detection rate and also improves the routing efficiency. A proof of concept of study about IoT is described in (Furkan et al., 2018). Such work also proposed a deep learning-based detection strategy against three types of routing attacks that are rank, version number, and hello flood. A provenance based security method for detecting the malicious activities over RPL has been presented in (Sabah et al., 2018). The provenance method allows the node to maintain a provenance in its routing table by observing the forwarding behaviors. Further, it decides a threshold value for packet forwarding. It detects the malicious activities by comparing the packet delivery ratio of nodes with the decided threshold value. A rank attack detection model named Sink-based intrusion detection system (SBIDS) for RPL has been introduced in (Shafique et al., 2018). In SBIDS, the sink node is responsible for performing the attack detection process, and thus, it minimizes the energy use and power dissipation of nodes considerably. The work in (Stephen and Arockiam, 2018) proposes an energy-based intrusion detection system against rank inconsistency attacks over IoT. The work in (Mahmood et al., 2018) presents a hybrid monitoring model for anomaly detection against sinkhole attack over RPL. In RPL, the sinkhole attack is generally occurring by decreasing the rank of nodes. Such rank decrements lead to creating abnormal traffic over a specific network area. Using such rank decrement, the sinkhole attackers obtain the shortest routing path form the sink node. By using the falsified shortest path, the sinkhole node compromises the other nodes in the network and launching a selective forwarding attack on the network. To offer defense against such type of attacks, the hybrid monitoring model employs a node rank model. The work (Arıs et al., 2018) proposes a lightweight security model against the version number of attacks over RPL. A secure and scalable RPL routing protocol named SPLIT

has been presented in (Conti et al., 2018) for IoT networks. It assures integrity to the nodes in IoT by incorporating a lightweight remote attestation model. Thus, the SPLIT minimizes energy consumption and enhances the network scalability. A signature-based intrusion detection mechanism (Philokypros et al., 2018) detects the external and internal attacks of IoT. The signature-based model employs both centralized and distributed intrusion detection methods for successful attack detection. The work of (Aydogan et al., 2018) presents a centralized IDS system for the industrial IoT environment. The secure IoT routing protocols are compared in table 3.

Table 2.3: Comparison of Various types of Secure IoT Routing Protocols

Routing Mechanism	**Type of Security**	**Attack Type**	**Advantages**	**Limitations**
RPL (Mercy and Pravin, 2014)	Key-based	External	Highly suitable for resource-limited RPL	Reduced network performance in the presence of internal attackers
PKI	Key-based/ Centralized	Authentication	Medium security	High overhead and requires centralized authority for key generation
RPL routing strategy (Nikravan et al., 2018)	Signature-based/ Lightweight	Version number and rank spoofing	Minimizes the energy consumption and prolongs the network lifetime	High computational complexity and overhead
CMD (Pu and Hajjar, 2018)	Monitoring based	Forwarding misbehaviors	High packet delivery ratio and minimum energy consumption	High control overhead
Multi-level IDS	IDS based learning/	Novel and energy	High robustness and less memory and	Lacking to classify the attack behaviors

(Alaparthy and Morgera, 2018)	Distributed	depleting	energy requirements	efficiently
Deep learning-based detection strategy (Furkan et al., 2018)	Learning-based	Rank, version number, and hello flood	Fills the significant routing attack detection gaps	Minimum quality and needs novel datasets for implementation
Hybrid monitoring model (Mahmood et al., 2018)	Monitoring based	Sinkhole and selective forwarding	Minimum power consumption and high detection accuracy	Requires novel data set
Signature-based IDS (Philokypros et al., 2018)	Centralized/ Distributed	Denial of Service	Prevents attack reachability to IoT devices with less energy consumption	High false positives

2.5 Survey of Trust-based Secure IoT Routing Protocols

Numerous trust-based routing mechanisms have been introduced to the IoT environment. In (Din et al., 2018), a comprehensive set of security components for trust enhancement is presented. The first known intrusion detection system in the IoT is SVELTE (Shahid and Linus, 2013), which tracks the entire path between the source and gateway node. It prevents the IoT communication against the spoofing, sinkhole, and selective forwarding attack. The main advantage of the SVELTE is that it performs with less overhead, and it is adequate for the deployment of constrained IoT nodes (Jing et al., 2018). A trust-aware secure routing framework (TSRF) is mainly proposed for low power sensor networks (Duan et al., 2014). The TSRF model evaluates the trust of a sensor node by integrating both direct and indirect trust values evaluated using

routing behaviors. In (Chze and Leong, 2014), a Secure Multi-hop Routing Protocol (SMRP) is proposed that employs a multi-layer parameter into the routing algorithm, and such a parameter is shared with the IoT devices during network initialization, ensuring secure wireless communication. However, it induces high overhead in creating and sharing a multi-layer parameter and tends the protocol unsuitable for a large-scale environment. The Group-Based Trust Management Scheme (GTMS) (Shaikh et al., 2009) is a trust-based scheme involving direct routing observation and sharing direct trust as evidence to other nodes. The cluster head nodes are selected at the intra-group level, and the gateway node executes a distributed trust management scheme. Even though the GTMS identifies the black hole attacks, the group based secure communication requires high energy to communicate with the gateway, resulting in hotspot problem.

A Collaborative lightweight trust-based (CLT) routing protocol in (Anita at al, 2014) exploits the collaborative trust model with considerable resource utilization. The trust counselor monitors and warns when the nodes behave maliciously. The system, however, fails to prove the effectiveness among autonomous nodes as it assumes that all nodes have a unique identity, and thus, it remains unsuitable for some applications. The RPL routing is more vulnerable to the DDoS attack (Wallgre et al., 2013). An energy-aware trust derivation scheme (Duan et al., 2014) exploits the trust derivation of the Dilemma Game model against the attacks of bad-mouthing, DDoS, and Selfish nodes. A game-theoretic model (Feng et al., 2014) (Ding et al., 2013) identifies the best number of recommendations to satisfy the security requirements. The game theory-based trust model (Ding et al., 2013) depends on strategic decision making based on incentives. However, it excessively mounts the overhead due to trust request broadcasting, which degrades the performance of the network. The distributed attack detection technique exploits multi-hop acknowledgment and raises the alarm against attackers. In this scheme, each intermediate node in a routing path takes the responsibility to detect the malicious nodes. The selection of another path for packet retransmission increases the delay and communication overhead, especially when a node involves in more multi-hop response acknowledgment.

There are several security schemes against the active routing attacks in RPL to provide secure communication (Airehrour et al., 2016) (Yang et al., 2017). Mostly, the defense mechanism measures accurate trust value using a reputation scheme (Yan et al., 2014). The main issue in

IPv6 is to protect the border nodes that send packets from IPv6 to sensors. The defense system based on the intrusion detection model on the non-resource constraint is presented in (Chen et al., 2016). This work aims at defending the system against spoofing or altering malicious nodes. Moreover, it can be extended to detect the dropping attack variants on it. Instead of involving all the nodes in indirect trust measurement, selecting an optimal number of nodes is the best suitable way to strengthen the security system with reasonable resource consumption. Incorporating a general trust model in RPL (Krentz et al., 2013) is not combative with the dropping attack variants. It is essential to determine whether the trust evidence provided by the neighboring nodes is accurate. In (Airehrour et al., 2016) (Jøsang et al., 2006), the Dempster-Shafer theory and subjective logic models are applied to evaluate the trust value for a node. Dempster-Shaffer's theory solves the problem of ignorance. However, the opinion consensus rule is fundamentally flawed. The work in (Saled et al., 2013) proposes a secure trust mechanism named as time-based trust-aware RPL routing protocol (SecTrust-RPL) against IoT routing attacks such as Sybil and rank.

Table 2.4: Comparison of Various Trust approaches of RPL routing and IoT

Routing Protocol	**Types of Attacks**	**Trust Evaluation Type**	**Advantages**	**Limitations**
TSRF (Duan et al., 2014)	Conflicting behavior, selfish, bad-mouthing, and collusion.	Direct and indirect	The high attack detection rate	High trust computational complexity
GTMS (Shaikh et al., 2009)	Blackhole	Direct and indirect	Secure communication	Node batteries drained quickly due to frequent sink interactions
CLT (Anita ett al, 2014)	Blackhole, bad-mouthing, and good-mouthing	Collaborative trust model	Minimum resource consumption	Not suitable for diverse applications

Two-way acknowledgment-based trust (2-ACKT) (Anita et al., 2013)	Blackhole, spoofing and selfish behavior	Direct trust	High trust accuracy due to dual ACK scheme	Poor routing performance in the presence of a grey hole
SecTrust-RPL (Saled et al., 2013)	Rank and Sybil	Direct	Optimized Secure Routing Decisions	High energy consumption at the nodes
New trust metric for the RPL routing protocol (Djedjig et al., 2017)	Rank falsification	Objective function based trust	Enhances the RPL security	Increases the overhead and energy consumption
Trust-Based Neighbor Unreachability Detection for RPL (Guclu et al., 2016)	No attacks are addressed	Cross-layer assisted trust	Enhances the network reachability and Resource availability.	The considered trust parameters are not adaptable for network dynamism

SUMMARY

Chapter 2 explained the background and literature review of the proposed methodologies. The IoT fundamentals and its architecture are discussed in detail. The various technologies in IoT and its applications are presented. This chapter discussed the overview of security requirements and security challenges in IoT. The different security attacks are explained and secure routing schemes have been presented that highlight the relative advantages and limitations. The existing trust-based secure routing protocols designed are also explained in detail.