




Review

Security Aspects for Rpl-Based Protocols: A Systematic Review in IoT

Karen Avila ^{1,*}, Daladier Jabba ¹ and Javier Gomez ²

¹ Departamento de Ingenieria de Sistemas, Universidad del Norte, Barranquilla 081007, Colombia; djabba@uninorte.edu.co

² Departamento de Ingenieria en Telecomunicaciones, Universidad Nacional Autonoma de Mexico, Ciudad de Mexico 04510, Mexico; javiergo@comunidad.unam.mx

* Correspondence: karena@uninorte.edu.co; Tel.: +57-5-3509509

Received: 9 July 2020; Accepted: 7 September 2020; Published: 17 September 2020



Abstract: The Internet of things (IoT) is a concept that has gained traction over the last decade. IoT networks have evolved around the wireless sensor network (WSN), and the following research looks at relevant IoT concepts and the different security issues that occur specifically at the network layer. This analysis is performed using a structured literature review (SLR). This form of bibliographic review has been a trend in recent years. Its strength is the performance of a bibliometric analysis that allows studying both trends in the line of research that you want to address and the relevant authors. This SLR reviews 53 proposals between 2011 and 2020, whose contribution is to mitigate attacks in the RPL (Routing Protocol for Low-Power and Lossy Networks) protocol. The revised proposals emerged after selecting keywords and databases in which to apply the search. Initially, approximately 380 research works appeared, for which it was necessary to continue using filters to refine the proposals to be included. After reading titles and abstracts, 53 papers were finally selected. In addition to analyzing the attacks mitigated in the RPL protocol, it is intended to identify the trend by which these attacks are reduced, as a result of the review, nine attacks have been found: rank, blackhole, selective forwarding, wormhole, DODAG (Destination-Oriented Directed Acyclic Graph) version number, DAO (Destination Advertisement Object) inconsistency, DIO (DODAG Information Object) suppression, Sybil, and sinkhole. Each of the 53 proposals analyzed in this review has an associated mitigation strategy, these strategies have been categorized into four groups, based on authentication or cryptography, based on network monitoring, based on secure parent node selection and other. According to the results, the authors' primary mitigation strategy is based on network monitoring, with 30%. This review also identifies the principal authors and countries that need the development of this line of research.

Keywords: security in RPL; attacks in RPL; wireless sensor networks; internet of things

1. Introduction

Wireless sensor networks (WSN) are useful in today's world, and their main benefit is the ability to monitor different scenarios remotely. There are several purposes to do it, such as making decisions based on the behavior of specific variables to avoid an event with a tragic consequence. Another purpose is to control objects remotely for different actions. WSN allows us, for example, to monitor hostile environments without the need to have a person present on site.

A common use of WSN can be found in the area of agriculture for irrigation systems. In healthcare, WSN has had a high impact because it provides immediate access to reading different critical variables in a patient. Early detection of some indicators in the patient's health can mean the difference between life and death [1].

Another area in which WSNs have been applied is geology, and it is often necessary to monitor areas of difficult access such as volcanoes, rivers, and forests. However, despite the significant benefits WSN offer, various risks and obstacles remain. The biggest obstacle can be found in the low power of data processing, leading us to another, and it is the battery level. If a sensor raises its processing, it consumes more energy. This situation happens because sensors are designed to capture data and send them to a receiver responsible for performing the necessary processing, storing it, forwarding it, discarding it, and launching and alerting.

The low-cost sensor hardware and basic design with low processing lead to the lack of a security implementation that strengthens the system. Any network must be protected because it handles crucial data for its owners. Captured data are sent without incidents to a secure receiver. It is required for this information not to be altered by unauthorized people.

It is essential to mention that a system is never 100% safe, as there is always a type of vulnerability. Researchers work every day in order to mitigate these vulnerabilities and make the systems safer. Traditional computer networks have a strong advantage when compared with sensor networks [2], especially concerning a higher processing power. Resources in WSN are scarce, limiting the implementation of any security mechanisms to only those that can operate with limited resources.

WSN allows us to implement monitoring systems in real time. Therefore the security of sensed data that will be transmitted must be guaranteed. However, due to their low processing level, they cannot support many processor-intensive security protocols, becoming the target of various security attacks [3]. Data protection in WSN links four aspects: authenticity, integrity, confidentiality, and availability of messages or data [4].

- Confidentiality: Refers to the mechanisms that ensure that only authorized persons can access the available data.
- Integrity: States the fact that the data transmitted is the same throughout its transmission.
- Authenticity: Denotes the verification that must be done before sending data, the issuer must be known and belong to the network.
- Availability: Refers to data being available at any time.

Each layer of the OSI (Open Systems Interconnection) model has its security considerations. In a network composed of sensors, there are mainly two layers involved, physical and link layers. Advanced sensors with higher processing capacity present a third layer, routing. Attacks against security are divided into two groups, passive and active. Passive attacks only access the system to gather data, and this group of attacks compromises the confidentiality of the system. On the other hand, active attacks cause damage to the system, alter data, or disable node members, allowing access to unauthorized members, among other things [5].

In recent times, a new concept has been emerging, the Internet of things (IoT), which refers to all things or objects connected to the Internet that can be accessed them remotely [6]. The basis of this paradigm is the wireless sensor network because, to control a "thing" remotely, it is necessary to do it through a sensor. Therefore, all the advantages and disadvantages of sensor networks are inherited by the Internet of things.

Architectures based on IoT are usually divided into three layers: perception, network, and application layer, as shown in Figure 1 and mentioned in [1,7–9].

- Perception layer: dispositive like sensors, gateways, RFID (Radio Frequency Identification) tags, and barcode belong to this category. Its main task is to gather information.
- Network layer: this layer is composed of various networks such as wired, wireless, private, and public. Its main task is to propagate and process information collected in the perception layer.
- Application layer: the related user interfaces and services are always based on the characteristics of the applications such as an intelligent transport system, monitoring system environment, and remote medical system.

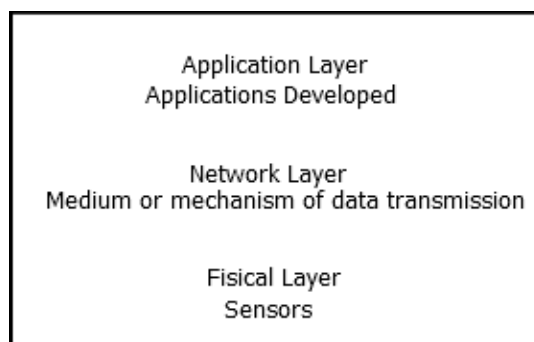


Figure 1. Internet of things (IoT) architecture [7,8,10].

One of the fundamental bases of the Internet of things is sensor networks, which is one of the reasons IoT systems inherit the security risks present in WSN. The security of the system must consider each network component. It is always better to include security mechanisms parallel with the design of the architecture, which should be the correct approach. The wrong approach is to design an architecture and, in the end, try to add security to a system already developed. Through these lessons, to achieve a system with the minimum security requirements, it is fundamental that security must be integrated into all components of the network [11]. Unfortunately, as is the case with many internet protocols, security is only added in a later-final stage, with the result that the added security becomes a patch to the original protocol that is not the best nor the adequate solution. Sadly, the RPL (Routing Protocol for Low-Power and Lossy Networks) protocol follows this path, although there is still time security taken into consideration before RPL becomes more widely used by both academia and industry.

RPL [12] is a distance vector routing protocol based on the construction of a directed acyclic graph (DAG). A design based on distance vector is considered suitable for low power and loss networks (LLN) such as RPL. In [12,13], RPL is designed for restricted and IP-based environments because it is recognized as the Internet of Things (IoT) routing protocol. The construction of the RPL topology is developed through the creation of a tree. For this cause, the root starts the process, and this tree is built through the sending of control messages. Within the tree construction process, each node is assigned a rank, the rank tells the node how many jumps it is from the root, and the root node will have rank 0. In other words, the node's rank corresponds to the level in the one inside the DAG. Within the terminology of this protocol, the term DODAG (destination-oriented DAG) is also known; it is a DAG rooted in a single destination, that is, in a single-root DAG (the root DODAG) which has no outgoing links. A DODAG is built using an objective function (FO) configured by the programmer, and this FO is used by the nodes to select its parent. Regarding control messages, RPL handles three types, and these are DIS (DODAG information solicitation), DIO (DODAG information object), and DAO (destination advertisement object). DIS is a control message used to request information from a DODAG, DIO is a down control message that allows a node to discover an instance of RPL, learn its configuration parameters, select a parent set, and maintain the DODAG. DAO is a control message that is used to propagate destination information up through the DODAG.

In [14], a work related to the classification of attacks in the RPL protocol is presented. However, the work has 23 references in total, and the most updated reference corresponds to the year 2016.

The literature shows us different types of attacks that can appear while using the RPL protocol, and these attacks and their consequences or impact are summarized in Table 1.

Table 1. Attack coding.

Attack	Occurs When?	Consequences	Coding
Rank attack	This attack happens when malicious nodes send information a lower range, simulating closer than others to the root. This situation allows, as a consequence, malicious nodes to capture as much traffic as possible [15,16].	In this attack, an attacker can decrease the network performance in terms of delay and packet delivery rate and this leads to suboptimal routes, especially when the attacking node location is in a high forward load area [17].	RA
Blackhole attack	It is carried out by a malicious node so that all the traffic that passes through it disappears discretely, thus isolating part of the network [15].	This attack isolates part of the network, eliminating all the messages that reach it. Its impact is highly negative since data from a subnet is wholly lost. The closer the malicious node is to the tree's root, the larger the subnet from which data is lost.	BA
Selective forwarding attack	This is a particular case of the BA, in which some packets (data or control messages) are deleted, while others are successfully forwarded, interrupting the routing process and affecting the efficiency of the network [15].	This attack isolates part of the network like the BA, but to a lesser extent since it does not delete all the messages it receives, but only a part of them. Its impact lies in the loss of data that depends on the percentage of packets that the malicious node has decided to discard.	SFA
Wormhole attack	This attack usually involves two or more attackers in the network, and attackers use a high-bandwidth tunnel in the network. These tunnels are advertised as high-quality routes by the attackers [18].	This attack attracts network traffic to a tunnel that is attractive for its bandwidth, generating consequences of traffic diversion and possible theft of sensitive data.	WA
DODAG version number attack	The DODAG version number is the same during the DODAG creation. When this number changes, the RPL protocol triggers a global repair mechanism of the DODAG. This type of attack consumes network resources, decreasing node lifetime as nodes use precious resources to repair the DODAG [19].	Its most significant impact is focused on reducing the lifetime of the network since the nodes spend energy rebuilding the network topology unnecessarily as a consequence of the attack executed.	DA
DAO inconsistency attack	In this attack, a malicious node intentionally drops the received packets and sets the forwarding-error flag in the packet option header to create the forwarding error packet, and then replies with the forwarding error packet to cause the parent node to discard valid downward routes in the routing table [20].	This attack modifies the control message through which a node selects a parent node. Consequently, valid routes are eliminated or discarded that can, for example, reduce the number of hops that take the sending of a packet from an origin to its destiny.	DAA
DIO suppression attack	This attack induces victim nodes to suppress the transmission of DIO messages needed to build the routing topology [21].	This attack eliminates the control message through which the topology's construction and maintenance are carried out when eliminating these messages. The construction of an incomplete tree, or even the no-construction of the tree, will result, making it impossible to put network running.	DIA
Sybil attack	In this attack, nodes pretend to be more than one node simultaneously in this attack [22]	As a consequence of this attack, there is a possible theft of data, since an illegitimate node tries to take the identity a legitimate node with the possible intention of forwarding the traffic to another place. If the data is sensitive, this could have inclusive legal consequences.	SYA
Sinkhole attack	The adversary node tries to attract most of the traffic, thus controlling most of the data moving through the network. For this purpose, the attacker must appear before others as "very attractive" when presenting optimal routes [15]	This attack has the same consequences as the RA attack, since its objective is the same, appearing attractive to other nodes, being part of the possible routes, and receiving most of the captured data.	SIA

This paper presents an investigation about the attacks present in RPL and the mitigation mechanisms used in the literature. This research is exposed through a structured literature review (SLR) according to Massaro protocol presented in [23], and following these reviews [24–26]. The contribution of this research is to establish a starting point for new investigations regarding the attacks mitigated in the RPL protocol and the strategies used, that is: What attacks have been presented? How many contributions exist? If it exists or not, is there persistence in the authors’ research line, and what is the future trend? To date, there is no review of state of the art using the SLR methodology that can guide researchers regarding the development and contributions of existing publications. This situation becomes the contribution of this manuscript, to contribute to the literature an SLR review covering the proposals that mitigate attacks in RPL and their mitigation strategies. The main object of this paper is to show the progress of security aspects in RPL-protocol, and answer the following research questions. RQ1: What are the development issues in IoT in RPL-security? RQ2: What are the trends to solve the security problems of the RPL-protocol? RQ3: What is the trend of future research?

2. Research Selection Method

The selection process was divided into three steps: the first step was identifying the different search terms related to security in RPL. In the second step, for each database, we identified the advanced search system and entered the combination of the selected keywords. Then, once the papers were selected in the second step, a new filter was applied after reading their titles and abstracts.

In this SLR, the following search terms were used: RPL Secure, RPL Based Secure, Authentication Protocol and Security Routing Based RPL. Terms were selected after a brief study of the keywords used in the papers related to the line of research addressed in this SLR. As a first step, the most relevant keywords that could yield the desired search results were identified, that is, proposals for secure protocols based on RPL that would mitigate the attacks that are detailed in Table 1. Subsequently, the keywords that threw up a large number of papers and made it impossible to analyze each of them. Finally, the keywords removed in the previous step were combined to refine the search results. The terms finally selected were those that yielded quantitatively valid results for the analysis of this review.

The databases explored were IEEE, Science Direct, and Springer. These databases were selected because they host proposals for conferences and journals related to the area of computer science and electrical and electronic engineering. Results about the number of papers selected to the second and third steps are presented in Table 2.

Table 2. Results by databases.

Query/Database	IEEE		Science Direct		Springer	
	Step 2	Step 3	Step 2	Step 3	Step 2	Step 3
((("All Metadata": security) AND "All Metadata": routing) AND "All Metadata": rpl) NOT "All Metadata": review)	131	43	–	–	–	–
Title, abstract, keywords: RPL based secure and RPL secure and authentication protocol and Security Routing Based RPL	–	–	147	4	–	–
'rpl AND based AND secure AND and AND rpl AND secure AND and AND authentication AND protocol AND and AND Security AND Routing AND Based AND RPL'.	–	–	–	–	181	6

The proposals selected for the analysis totaled 53. Review papers, or proposals implemented using a routing protocol other than RPL, were discarded (only proposals that concretely ensured the protocol’s security were taken into account). Among the proposals reviewed in this section, we found different mechanisms that improve the security of the RPL protocol, and these proposals will be discussed below.

Table 3 presents the coding for journals and conferences where papers were published, and Table 4 shows the type of paper coding. These codes are established in order to make reference to conferences, journals, and types of paper during the development of the manuscript in a simpler way.

Table 3. Conferences, journals and books coding.

Type	Title	Code	
Conferences	2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems	EIAD	
	2016 IEEE Global Communications Conference (GLOBECOM)	GLOBECOM	
	2017 25th International Conference on Software, Telecommunications and Computer Networks (SoftCOM)	SoftCOM	
	2016 International Conference on Wireless Communications, Signal Processing and Networking (WISPNET)	WISPNET	
	2011 IFIP Wireless Days (WD)	WD	
	2014 11th International Symposium on Wireless Communications Systems (ISWCS)	ISWCS	
	2015 21st Asia-Pacific Conference on Communications (APCC)	APCC	
	2017 8th International Conference on Information and Communication Systems (ICICS)	ICICS	
	2017 International Conference on Advances in Computing, Communications, and Informatics (ICACCI)	ICACCI	
	2017 Global Internet of Things Summit (GloTS)	GloTS	
	2015 IEEE Symposium on Computers and Communication (ISCC)	ISCC	
	Proceedings of the 9th International Conference on Network and Service Management (CNSM 2013)	CNSM	
	Interoperability, Safety, and Security in IoT	ISSIOT	
	Computing and Network Sustainability	CNS	
	2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)	IWCMC	
	2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC)	CCNC8	
	2017 International Conference on Networking and Network Applications (NaNA)	NaNA	
	2013 Fifth International Conference on Ubiquitous and Future Networks (ICUFN)	ICUFN	
	2016 26th International Telecommunication Networks and Applications Conference (ITNAC)	ITNAC6	
	2017 27th International Telecommunication Networks and Applications Conference (ITNAC)	ITNAC7	
	2018 3rd International Conference for Convergence in Technology (I2CT)	I2CT	
	2017 International Conference on Information and Communication Technologies (ICICT)	ICICT	
	2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)	CCWC	
	2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)	ICIOT	
	MILCOM 2019–2019 IEEE Military Communications Conference (MILCOM)	MILCOM	
	2020 7th International Conference on Signal Processing and Integrated Networks (SPIN)	SPIN	
	International Conference on Intelligent Computing and Communication Technologies	ICICCT	
	2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)	ERFA	
	2017 IEEE 16th International Symposium on Network Computing and Applications (NCA)	NCA	
	2018 14th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)	WIMOB	
	2018 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC)	APSIPA	
	2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN)	ViTECON	
	2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA)	AICCSA	
	2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC)	CCNC9	
	2019 Chinese Control Conference (CCC)	CCC	
	2019 Twelfth International Conference on Contemporary Computing (IC3)	IC3	
	2019 4th International conference on Internet of Things: Smart innovation and usages (IoT-SIU)	SIU	
	2019 15th IEEE International Workshop on Factory Communication Systems (WFCS)	WFCS	
	2019 5th International Conference on Web Research (ICWR)	ICWR	
	2019 International Conference on Computing, Networking and Communications (ICNC)	ICNC	
	2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS)	MACS	
	2019 9th International Conference on Computer and Knowledge Engineering (ICCKE)	ICCKE	
	TENCON 2019–2019 IEEE Region 10 Conference (TENCON)	TENCON	
	Journals	Wireless Personal Communications	WPC
		Ad Hoc Networks	AND
		IEEE Transactions on Network and Service Management	TNSM
		IEEE Communications Letters	ICL
		Future Generation Computer Systems	FGCS
		Ad Hoc Networks	ADH
		Journal Of Network And Systems Management	JNSM
Journal of Information Security and Applications		JISA	
IEEE Internet of Things Journal		ITJ	

Table 4. Type of paper coding.

Type of Paper	Code
Conference paper (proceedings)	CP
Journal paper	JP

The theme and approach coding is described in Table 5. Due to their operation, some attacks shown in Table 1 are related to each other. Therefore it has been decided to unite these attacks and analyze them as a group within this manuscript. Both the RA (rank attack) and the SIA (sinkhole attack) aim to attract network traffic to a specific node, so these two attacks make up an analysis group. SFA (selective forwarding) and BA (blackhole attack) work in the same way with the difference that all received packets are discarded in the BA attack, and in the SFA attack, the malicious node decides which packets to forward and which not. Finally, the DAA and DIA attacks have been united into a single group since they are related to modifying protocol control messages. These groups formed are detailed in Table 5 and are selected as the analysis topics following the SLR review structure.

Table 5. Theme coding.

Theme	Code
Rank attack/Sinkhole attack	RSA
Selective forwarding/Blackhole attack	SBA
Wormhole attack	WA
DOGAG number version attack	DNA
DAO/DIS message inconsistency attack	D2A
Sybil attack	SA

3 mitigation strategies used by the authors have been identified, these are specified in Table 6, including the “others” category, in order to assign a category to those proposals that do not adapt to the 3 identified strategies.

Table 6. Approach coding: presents the mechanisms or strategies used by the authors to mitigate the attacks.

Type of Approach	Code
Based on authentication or cryptography	AC
Based on network monitoring	NM
Based on secure parent node selection	SP
Other	OT

Table 7 summarizes relevant data from 53 papers selected for this SLR according to Tables 3–6. The first column gives the author name and year of publications of the proposal. Column 2 refers to the number of citations the proposal has at the time of submission of this review. Column 3 shows type code according to Table 4. Column 4 refers to the journal or conference code, according to Table 3. Columns 5–10 specifies the theme code according to Table 5. Columns 11–14 detail the approach code according to the table. Finally, the last column shows the proposal’s reference.

Table 7. Paper classification.

Authors	Cited	Type Code	J/C/Code	Theme Code						Approach Coding			Reference		
				RSA	SBA	WA	DNA	D2A	SA	AC	NM	SP		OT	
Dvir, A et al. (2011)	128	CP	EIAD	X			X				X				[27]
Le, A et al. (2011)	73	CP	WD	X								X			[28]
Raza, S et al. (2013)	512	JP	AND	X			X					X			[29]
Khan, Faraz et al. (2013)	30	CP	ICUFN			X					X				[18]
Seeber, Sebastian et al. (2013)	27	CP	CNSM	X	X	X					X				[30]
Matsunaga, T et al. (2014)	11	CP	ISWCS	X								X			[31]
Iuchi, K et al. (2015)	18	CP	APCC	X									X		[32]
Djedjig, N et al. (2015)	29	CP	ISCC	X									X		[33]
El Hajjar, Ayman et al. (2016)	2	CP	ISSIOT	X	X	X					X				[34]
Nan, Jiang et al. (2016)	3	CP	WISFNET	X	X						X				[19]
Airehrour, D et al. (2016)	31	CP	ITNAC6			X							X		[35]
Glissa, G et al. (2016)	39	CP	GLOBECOM	X	X	X					X				[15]
Djedjig, N et al. (2017)	27	CP	ICICS	X									X		[36]
Elleuchi, M et al. (2017)	5	CP	SoftCOM	X		X		X	X	X					[37]
Kallapur, P et al. (2017)	2	CP	ICACCI	X									X		[38]
El Hajjar, Ayman et al. (2017)	2	CP	GLoTS	X	X								X		[39]
Kaur, Gagandeep et al. (2017)	1	CP	CNS	X	X						X				[40]
Airehrour, D et al. (2017)	5	CP	ITNAC7			X							X		[41]
Ahsan, M et al. (2017)	6	CP	ICICT			X								X	[42]
Mayzaud, A et al. (2017)	25	JP	TNSM				X					X			[43]
Gara, F et al. (2017)	9	CP	IWCMC	X	X							X			[44]
Ma, G et al. (2017)	7	CP	NaNA		X									X	[45]
Medjek, F et al. (2017)	8	CP	ICIOT						X		X				[46]
Althubaity, A et al. (2017)	3	CP	ERFA	X						X		X			[47]
Lahbib, A et al. (2017)	6	CP	NCA		X								X		[48]
Pu, C et al. (2018)	23	CP	CCNC8	X	X							X			[49]
Mehta, R et al. (2018)	3	CP	I2CT			X							X		[50]
Nikravan, M et al. (2018)	6	JP	WPC	X			X				X				[51]
Pu, C (2018)	13	CP	CCWC					X					X		[20]
Nikam, A et al. (2018)	3	CP	I2CT						X			X			[22]
Ghaleb et al. (2018)	13	JP	ICL					X						X	[52]
Jiang, J et al. (2018)	2	CP	APSIPA		X							X			[53]
Conti, M et al. (2018)	15	CP	WIMOB					X						X	[54]
Airehrour et al. (2019)	44	JP	FGCS		X								X		[55]
A Arı̇s et al. (2019)	6	JP	ADH				X				X				[56]
Groves et al. (2019)	2	CP	MILCOM						X		X				[57]
N Bhalaji et al. (2019)	2	CP	ICICCT		X					X			X		[58]
S. Choudhary et al. (2019)	0	CP	AICCSA	X	X						X				[59]
Thulasiraman, P et al. (2019)	9	CP	CCNC9						X				X		[60]
Yugha, R et al. (2019)	1	CP	VITECON			X				X					[61]
Zhang, T et al. (2019)	2	CP	CCC		X					X					[62]
Tandon, A et al. (2019)	2	CP	IC3	X						X			X		[63]
Verma, A et al. (2019)	8	CP	SIU	X	X					X				X	[64]
Farzaneh, B et al. (2019)	8	CP	ICWR					X				X			[65]
Aydogan, E et al. (2019)	8	CP	WPCS				X							X	[66]
Jhanjhi, NZ et al. (2019)	2	CP	MACS	X		X						X			[67]
Taghanaki, S et al. (2019)	0	CP	ICCKE	X									X		[68]
Patel, H et al. (2019)	2	CP	TENCON		X							X			[69]
G Soni et al. (2020)	0	CP	SPIN		X							X			[70]
Zaminkar Mina et al. (2020)	0	JP	WPC	X									X		[71]
Hashemi et al. (2020)	0	JP	JNSM	X	X				X				X		[72]
Djedjig et al. (2020)	1	JP	JISA	X	X								X		[73]
S. Murali et al. (2020)	6	JP	ITJ						X				X		[74]

3. General Conclusions

For bibliographic analysis and citations, the bibliometrix package in RStudio [75] was used. It was possible to determine the most cited authors or the most productive countries. The analyzed papers were papers displayed in Table 7. Table 8 shows the primary information about data.

Table 8. Main information about data.

Description	Value
Number of Documents	53
Keywords Plus	106
Authors Keywords	144
Period	2011–2020
Average citations per documents	22.45
Authors	142
Authors appearances	169
Authors single-authored documents	1
Documents per author	0.373
Authors per document	2.68
Co-authors per documents	3.19
Collaboration index	2.71
Conferences proceedings	43
Journal paper	10

Percentages of paper approaches presented in Table 9 and Figure 2 are based on the papers analyzed, and the selected categories. According to the results, there are more significant proposals at the SP (Based on secure parent node selection) and NM (based on network monitoring) approach, followed by AC (based on authentication or cryptography) and OT (Other).

Table 9. Paper approach.

Approach Code	Value	Percent
AC	12	23
NM	16	30
SP	19	36
OT	6	11

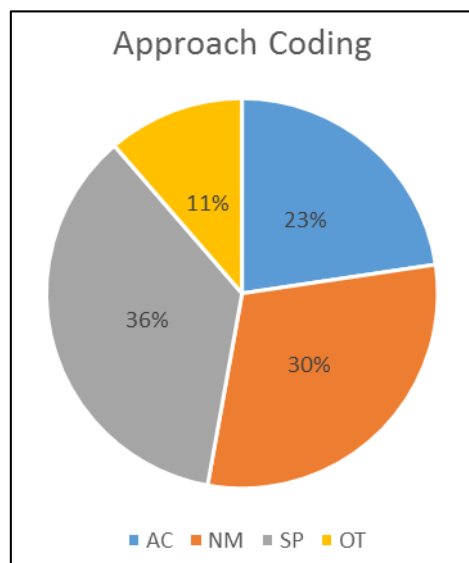
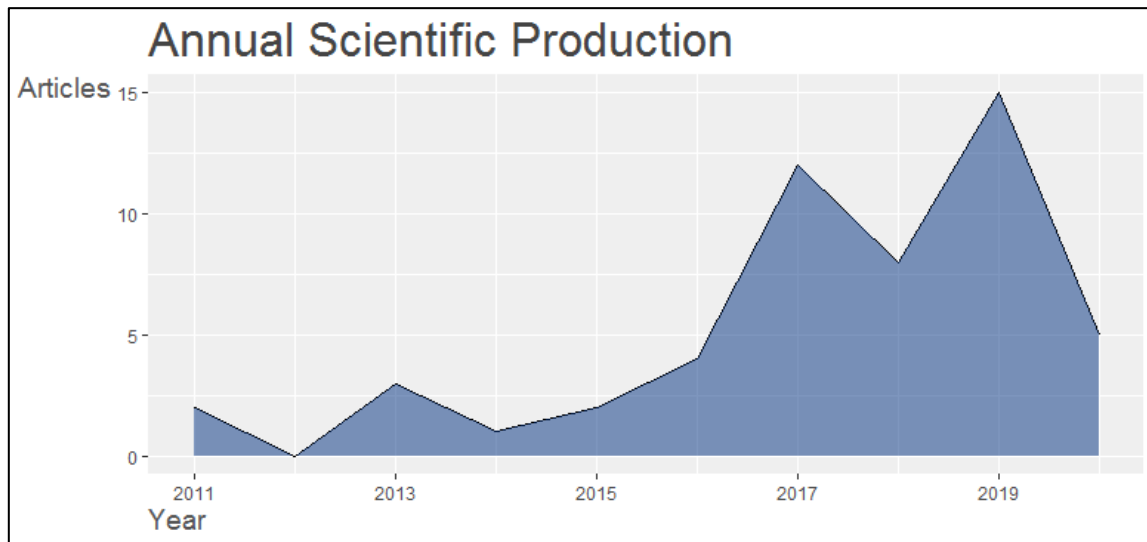
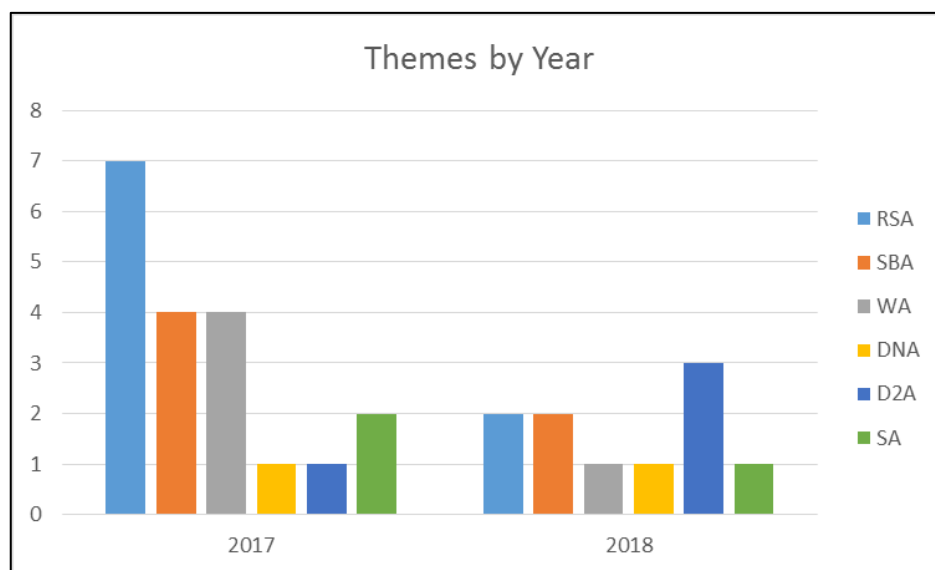


Figure 2. Approach coding.

Annual scientific productions are shown in Figure 3a. Publications correspond to the years between 2011 and 2020. From this figure, it is concluded that the number of papers has increased over the years. However, throughout this period of time, the trend did not always increase, and there are some years in which production in the area decreased. Between the years 2011–2012, 2013–2014, and 2017–2019 there was a decrease of two, two, and six proposals, respectively.



(a) Annual scientific production.



(b) Themes by Year

Figure 3. (a) Annual scientific production. (b) Themes by year.

The most relevant decrease occurs between the years 2017 and 2018. Details of the subjects studied in this period are shown in Figure 3b, it is observed that this decrease is mainly associated with the line of research associated with the subject RSA (Rank attack/Sinkhole attack) but there was an increase in research related to the D2A (DAO/DIS message inconsistency attack) issue. D2A is a group of two attacks that arise from the nature of RPL, affecting the DIO and DAO control messages. Therefore it can be concluded that, in 2018, researchers worked more to strengthen the security of the nature of the protocol compared to the previous year. For the rest of the subjects, the study remains almost constant.

The most productive authors are shown in Figure 4. There are two authors with two papers, four authors with three papers, and four authors with four papers. The above shows that these authors show continuity in the research topic.

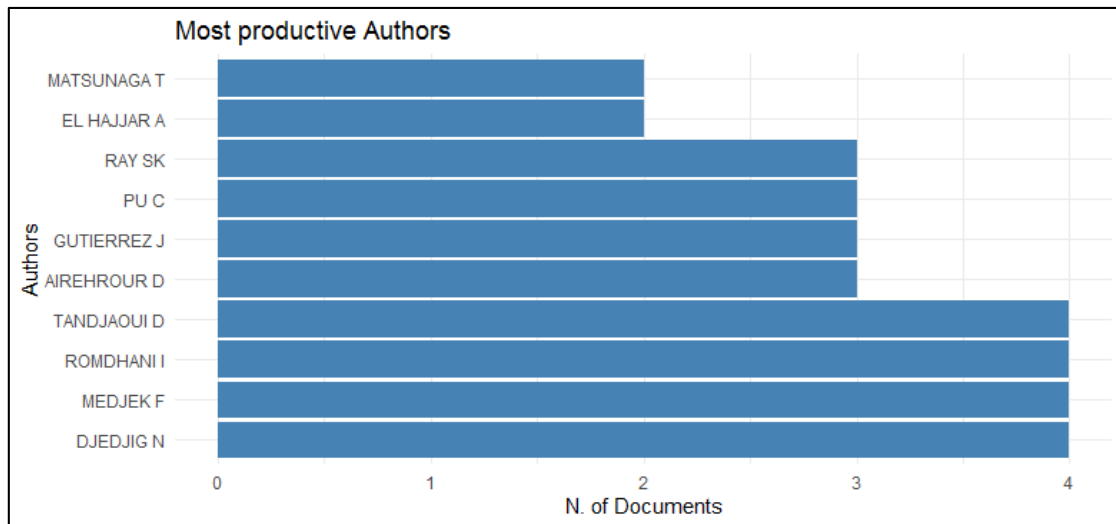


Figure 4. Most productive authors.

Table 10 lists the contributions of the authors mentioned in Figure 4. From this table, we can obtain information that Figure 4 by itself does not provide. The authors S.K. Ray and J. Gutierrez are listed in Figure 4 with three contributions each, although these contributions are the same for both authors. The same happens with the authors D. Tandjaoui, F. Medjek, and N. Djedjig, for whom Figure 4 shows four contributions. Other information that can be inferred from Table 10 is the period of publication, and it is considered that these authors maintain their current research line, with 2019 or 2020 being the last year of publication, except for the authors T. Matsunaga and A. El Hajjar.

Table 10. Main Authors and Publication Years.

Author	Period	Reference
Matsunaga T	2014–2015	[31,32]
El Hajjar A	2017	[34,39]
Pu C	2018–2019	[20,49,57]
Ray SK	2016–2019	[35,41,55]
Gutierrez J	2016–2019	[35,41,55]
Airehrour D	2016–2019	[35,41,55]
Romdhani I	2017–2020	[36,46,52,73]
Tandjaoui D	2015–2020	[34,36,46,73]
Medjek F	2015–2020	[34,36,46,73]
Djedjig N	2015–2020	[34,36,46,73]

Figure 5 shows the most productive countries; a high concentration of publications are in Algeria, India, Iran, and New Zealand with three productions each.

Figure 6 locates on the world map of the four most productive countries in the line of research associated with this SLR. It can be seen that the productions come from the continents of Asia, Africa, and Oceania, with Africa being the continent that groups the largest countries. It can also be observed that Europe and America do not have publications on the subject.

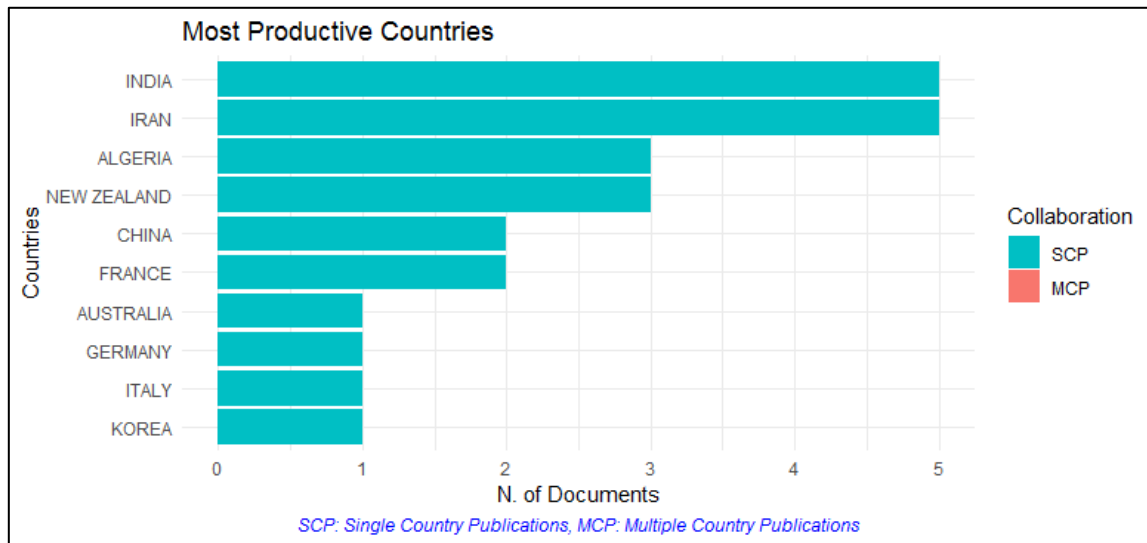


Figure 5. Most productive countries.

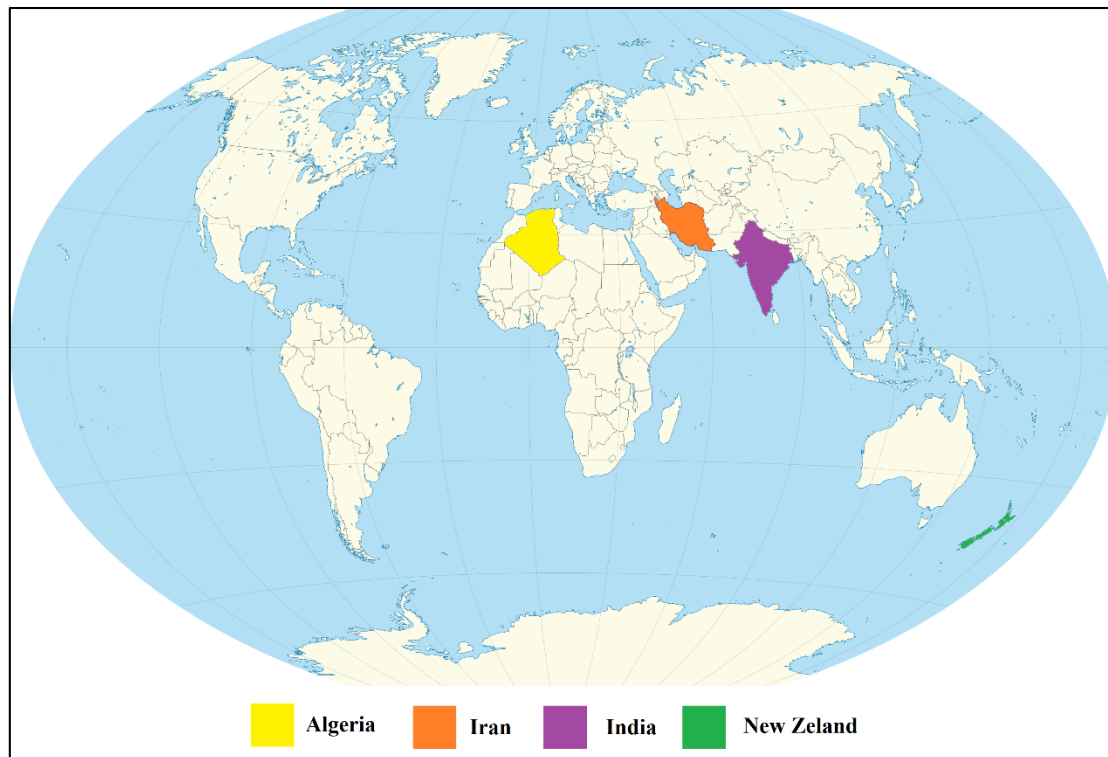


Figure 6. Most Productive Countries in the Map.

Figure 7 shows the keyword co-occurrences. The network resulting from the analysis of keywords co-occurrences shows three significant groups. The green group shows the relationship of words such as wireless communications, energy consumption, hardware, authentication between others. Red group evidences the association between protocols, monitoring, topology, maintenance, and security. The blue group shows the relationship between words such as the internet of things, 6lowpan, IoT, trust, sinkhole attack, version number attack, sensors, and intrusion detection. The image shows us the closeness of these three groups, indicating their close relationship. The spheres' size representing each of the keywords indicates their level of importance within the group. The larger the sphere, the more significant its relevance. Links indicate the relationship between keywords in the same group.

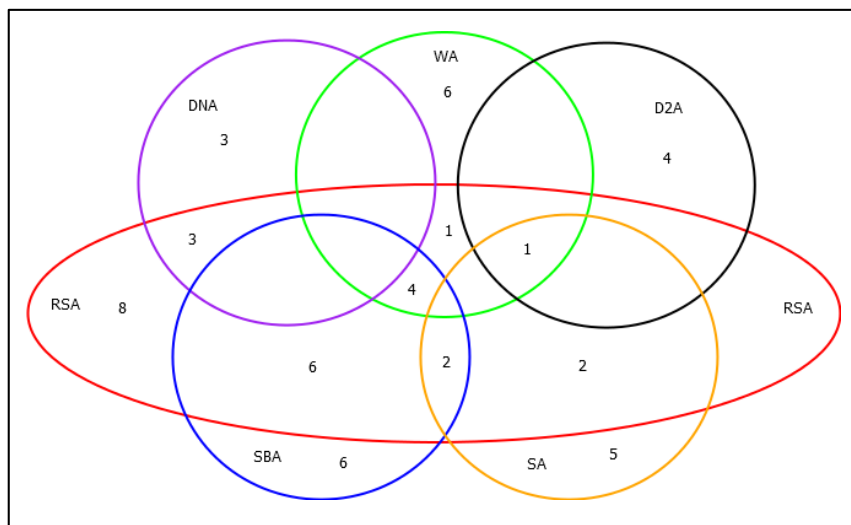


Figure 9. Correlation between mitigated attacks.

It can also be seen in Figure 9 that no attack is mitigated independently. There is at least one proposal in each category, mitigating a set of attacks, and that is why there is no isolated set in the view diagram. In the case of the D2A theme, this attack is mitigated in five proposals, four of them mitigate only this attack, but, in one proposal, it is mitigated together with the WA, SA, and RSA themes. Finally, it can be noted that no proposal mitigates all the attacks detailed here, as seen in Figure 8.

Tables and figures allow us to detail the following implications:

Implication 1: RPL security is a topic highly associated with the industry since the highest percentage of publications are in proceedings of international conferences (see Table 8).

Implication 2: The investigation takes strength in the field of security in RPL. Since its inception, its authors stated that this protocol did not manage security at the network layer. Therefore this has been a starting point for the investigation and implementation of mechanisms to mitigate attacks in this protocol (see Figure 3).

Implication 3: 10 authors have more than one publication in this SLR. This shows a trend of the persistence of researchers in the area. On the other hand, according to Table 8, the collaboration index is 2.65, which shows temporary work among the authors.

Implication 4: New Zealand is evidenced as a strong country at the level of technological research, according to Figure 5.

Implication 5: Of the five proposals for 2020, only one of them belongs to a conference, and the rest are part of journals. This is deduced given the global crisis experienced due to the Covid-19 pandemic, for which mass gatherings of people have been restricted, including academic or research conferences.

The statistics and taxonomy generated allow us to answer the research questions detailed in the introduction.

RQ1: What are the development issues in IoT in RPL attacks. Development issues in the RPL attacks are presented in Table 5, where themes are detailed. Each one of these attacks is described in section II. Table 5 shows attacks on the RPL protocols in layer 3. Some attacks are inherited from the WSN, like SA or WA. Attacks like DNA or D2A are attacks that arise from the logic of the protocol.

RQ2: What are the trends to solve the security problems of the RPL-protocol. Table 6 summarizes three principal groups into which this SLR divides the mechanisms to mitigate attacks on the RPL protocol. To mitigate attacks, the authors have designed strategies related to selecting a reliable parent in the design of the protocol topology, cryptography or authentication to change messages, and monitor the network for unusual behavior.

RQ3: What is the trend of future research. There is a tendency to improve the metrics of the RPL protocol. One of these metrics is energy consumption, given the nature of WSN, and it is necessary to

maximize the lifetime to the sensors. In the protocol proposal [12], the authors affirm that they do not have security mechanisms implemented for the routing layer, leaving the line of investigation open to those who wish to improve the said protocol. In the first instance in the investigations, it was evidenced not to take into account the energy consumption, although, as a future trend, it is a metric that is intended to improve even so by implementing the security mechanisms.

4. Conclusions

This research presents an SLR for mitigating frequent attacks at the network layer in wireless sensor networks using the RPL protocol. It is essential to mention that the IoT security analysis must also be seen from the WSN perspective because the problems that are present in WSN are also inherited to IoT. As a general trend, this work emphasized how the provision of security related to IoT is gaining more attention in recent years, even though there is a decrease in literary production between 2017 and 2019, as shown in Figure 3a. In 2020 the publications of the year 2019 were already matched, and it is expected that, by the end of 2020, this production will increase in number.

According to the bibliographic review, nine attacks have been found: rank, blackhole, selective forwarding, wormhole, DODAG version number, DAO inconsistency, DIO suppression, Sybil, and sinkhole. Each of the 53 proposals analyzed in this review has an associated mitigation strategy, these strategies have been categorized into four groups: based on authentication or cryptography, based on network monitoring, based on secure parent node selection and other. According to the results, the primary mitigation strategy used by the authors is based on parent selection or trust model, with 36% (See Figure 2). Figure 4 shows that some authors have been constant in the investigation of the subject, and this is concluded because these authors have more than one proposal included in this review. An important conclusion is that there is a tendency to mitigate a single attack within a unique paper. This is evidenced in Figure 8, which shows that 35 proposals were classified with a thematic code. Only one research was classified with four thematic codes. This figure shows that the number of publications is inversely proportional to the number of mitigated attacks.

The implications made in this review were as follows: (1) RPL security is a topic highly associated with the industry since the highest percentage of publications are in proceedings of international conferences (see Table 8). (2) The investigation takes strength in the field of security in RPL. Since its inception, its authors stated that this protocol did not manage security at the network layer. Therefore this has been a starting point for the investigation and implementation of mechanisms to mitigate attacks in this protocol (see Figure 3). (3) 10 authors have more than one publication in this SLR. This situation shows a trend of the persistence of researchers in the area. On the other hand, according to Table 8, the collaboration index is 2.71, which shows temporary work among the authors. (4) New Zealand, India, Iran and Algeria are evidenced as strong countries at the level of technological research, according to Figure 5.

There is a tendency to improve the metrics of the RPL protocol. One of these metrics is energy consumption, given the nature of WSN, and it is necessary to maximize the lifetime to the sensors. In the protocol proposal [12], the authors affirm that they do not have security mechanisms implemented for the routing layer, leaving the line of investigation open to those who wish to improve the said protocol. In the first instance in the research, it was evidenced not to take into account the energy consumption. However, as a future trend, it is a metric that is intended to improve even by implementing the security mechanisms.

The biggest obstacle to developing security mechanisms for IoT is the nature of the network. The reason is that things or sensors are small devices with little processing capacity, which makes it challenging to execute robust algorithms that strengthen the security of the system. RPL does not have a defined implementation for its security operations, as the standard only advises on how to improve the security of the protocol. It is vital to continue working on strengthening the security aspects of RPL since even a small security flaw can be exploited and misused by third parties.

Author Contributions: K.A. proposed the structured literary review (SLR) structure for the preparation of the manuscript, and carried out the search for the documents to be reviewed. D.J. and J.G. divided the papers into groups according to the types of attacks and their solutions. K.A. wrote the paper. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Universidad del Norte and the call 785 of Colciencias (Administrative Department of Science, Technology and Innovation).

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

References

1. Avila, K.; Sanmartin, P.; Jabba, D.; Jimeno, M. Applications Based on Service-Oriented Architecture (SOA) in the Field of Home Healthcare. *Sensors* **2017**, *17*, 1703. [CrossRef]
2. Walters, J.P.; Liang, Z.; Shi, W.; Chaudhary, V. Wireless sensor network security: A survey. In *Security in Distributed, Grid, and Pervasive Computing*; Xiao, Y., Ed.; CRC Press, Publications: Boca Raton, FL, USA, 2007.
3. Xiangyu, J.; Chao, W. The security routing research for WSN in the application of intelligent transport system. In Proceedings of the 2006 IEEE International Conference on Mechatronics and Automation, Luoyang, China, 25–28 June 2006; pp. 2318–2323.
4. Azzabi, T.; Farhat, H.; Sahli, N. A survey on wireless sensor networks security issues and military specificities. In Proceedings of the 2017 International Conference on Advanced Systems and Electric Technologies (IC_ASET), Hammamet, Tunisia, 14–17 January 2017; pp. 66–72.
5. Blilat, A.; Bouayad, A.; Chaoui, N.E.H.; El Ghazi, M. Wireless sensor network: Security challenges. In Proceedings of the 2012 National Days of Network Security and Systems (JNS2), Marrakech, Morocco, 20–21 April 2012; pp. 68–72.
6. Airehrou, D.; Gutierrez, J.; Ray, S.K. Secure routing for internet of things: A survey. *J. Netw. Comput. Appl.* **2016**, *66*, 198–213. [CrossRef]
7. Peng, S.Q.; Shen, H.B. *Security Technology Analysis of IOT*; Springer: Berlin/Heidelberg, Germany, 2015; pp. 401–408. [CrossRef]
8. Ju, Z.; Li, Y. Analysis on internet of things (IOT) based on the “subway supermarket” e-commerce mode of TESCO. In Proceedings of the 2011 International Conference on Information Management, Innovation Management and Industrial Engineering (ICIII), Shenzhen, China, 26–27 November 2011; pp. 430–433.
9. Vilorio Núñez, C.A.; Sanmartín Mendoza, P.; Avila Hernández, K.; Jabba Molinares, D. Internet de las cosas y la salud centrada en el hogar. *Revista científica salud uninorte. Rev. Salud Uninorte* **2016**, *32*, 337–359.
10. Kassab, W.A.; Darabkh, K.A. A–Z survey of Internet of Things: Architectures, protocols, applications, recent advances, future directions and recommendations. *J. Netw. Comput. Appl.* **2020**, *163*, 102663. [CrossRef]
11. Oreku, G.S. Reliability in WSN for security: Mathematical approach. In Proceedings of the 2013 International Conference on Computer Applications Technology (ICCAT), Sousse, Tunisia, 20–22 January 2013; pp. 1–6.
12. Thubert, P.; Winter, T.; Brandt, A.; Hui, J.; Kelsey, R.; Levis, P.; Pister, K.; Struik, R.; Vasseur, J.; Alexander, R. RPL: IPv6 Routing Protocol for Low power and Lossy Networks. Available online: <https://tools.ietf.org/html/rfc6550> (accessed on 8 September 2020).
13. Sanmartin, P.; Rojas, A.; Fernandez, L.; Avila, K.; Jabba, D.; Valle, S. Sigma Routing Metric for RPL Protocol. *Sensors* **2018**, *18*, 1277. [CrossRef]
14. Sharma, D.; Mishra, I.; Jain, S. A Detailed Classification of Routing Attacks against RPL in Internet of Things. *Int. J. Adv. Res. Ideas Innov. Technol.* **2017**, *3*, 692–703.
15. Glissa, G.; Rachedi, A.; Meddeb, A. A secure routing protocol based on RPL for internet of things. In Proceedings of the 2016 IEEE Global Communications Conference (GLOBECOM), Washington, DC, USA, 4–8 December 2016; pp. 1–7.
16. Sahay, R.; Geethakumari, G.; Modugu, K. Attack graph—Based vulnerability assessment of rank property in RPL-6LOWPAN in IoT. In Proceedings of the 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore, 5–8 February 2018; pp. 308–313.
17. Rai, K.K.; Asawa, K. Impact analysis of rank attack with spoofed IP on routing in 6LoWPAN network. In Proceedings of the 2017 Tenth International Conference on Contemporary Computing (IC3), Noida, India, 10–12 August 2017; pp. 1–5.

18. Khan, F.I.; Taeshik, S.; Taekkyeun, L.; Kihyung, K. Wormhole attack prevention mechanism for RPL based LLN network. In Proceedings of the 2013 Fifth International Conference on Ubiquitous and Future Networks (ICUFN), Da Nang, Vietnam, 2–5 July 2013; pp. 149–154.
19. Nan, J.; Jianfei, L.; Wei, X.; Hongzhou, S. Routing attacks prevention mechanism for RPL based on micropayment scheme. In Proceedings of the 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, India, 23–25 March 2016; pp. 835–841.
20. Pu, C. Mitigating DAO inconsistency attack in RPL-based low power and lossy networks. In Proceedings of the 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 8–10 January 2018; pp. 570–574.
21. Perazzo, P.; Vallati, C.; Anastasi, G.; Dini, G. DIO Suppression Attack against Routing in the Internet of Things. *IEEE Commun. Lett.* **2017**, *21*, 2524–2527. [[CrossRef](#)]
22. Nikam, A.; Ambawade, D. Opinion metric based intrusion detection mechanism for RPL protocol in IoT. In Proceedings of the 2018 3rd International Conference for Convergence in Technology (I2CT), Pune, India, 6–8 April 2018; pp. 1–6.
23. Massaro, M.; Dumay, J.; Guthrie, J. On the shoulders of giants: Undertaking a structured literature review in accounting. *Account. Audit. Account. J.* **2016**, *29*, 767–801. [[CrossRef](#)]
24. Ng, C.K.; Wu, C.H.; Yung, K.L.; Ip, W.H.; Cheung, T. A semantic similarity analysis of Internet of Things. *Enterp. Inf. Syst.* **2018**, *12*, 820–855. [[CrossRef](#)]
25. Xu, L.D.; Duan, L. Big data for cyber physical systems in industry 4.0: A survey. *Enterp. Inf. Syst.* **2019**, *13*, 148–169. [[CrossRef](#)]
26. Burton-Jones, A.; Akhlaghpour, S.; Ayre, S.; Barde, P.; Staib, A.; Sullivan, C. Changing the conversation on evaluating digital transformation in healthcare: Insights from an institutional analysis. *Inf. Organ.* **2020**, *30*, 100255. [[CrossRef](#)]
27. Dvir, A.; Holczer, T.; Buttyan, L. VeRA—Version number and rank authentication in RPL. In Proceedings of the 2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems, Valencia, Spain, 17–22 October 2011; pp. 709–714.
28. Le, A.; Loo, J.; Luo, Y.; Lasebae, A. Specification-based IDS for securing RPL from topology attacks. In Proceedings of the 2011 IFIP Wireless Days (WD), Niagara Falls, ON, Canada, 10–12 October 2011; pp. 1–3.
29. Raza, S.; Wallgren, L.; Voigt, T. SVELTE: Real-time intrusion detection in the Internet of Things. *Ad Hoc Netw.* **2013**, *11*, 2661–2674. [[CrossRef](#)]
30. Seeber, S.; Sehgal, A.; Stelte, B.; Rodosek, G.D.; Schonwalder, J. Towards a trust computing architecture for RPL in cyber physical systems. In Proceedings of the 2013 9th International Conference on Network and Service Management, IEEE, Zurich, Switzerland, 14–18 October 2013; pp. 134–137.
31. Matsunaga, T.; Toyoda, K.; Sasase, I. Low false alarm rate RPL network monitoring system by considering timing inconstancy between the rank measurements. In Proceedings of the 2014 11th International Symposium on Wireless Communications Systems (ISWCS), Barcelona, Spain, 26–29 August 2014; pp. 427–431.
32. Iuchi, K.; Matsunaga, T.; Toyoda, K.; Sasase, I. Secure parent node selection scheme in route construction to exclude attacking nodes from RPL network. In Proceedings of the 2015 21st Asia-Pacific Conference on Communications (APCC), Kyoto, Japan, 14–16 October 2015; pp. 299–303.
33. Djedjig, N.; Tandjaoui, D.; Medjek, F. Trust-based RPL for the Internet of Things. In Proceedings of the 2015 IEEE Symposium on Computers and Communication (ISCC), Larnaca, Cyprus, 6–9 July 2015; pp. 962–967.
34. El Hajjar, A.; Roussos, G.; Paterson, M. On the performance of key pre-distribution for RPL-based IoT networks. In *Interoperability, Safety and Security in IOT*; Mitton, N., Chaouchi, H., Noel, T., Watteyne, T., Gabillon, A., Capolsini, P., Eds.; Springer: Berlin/Heidelberg, Germany, 2017; Volume 190, pp. 67–78.
35. Airehrour, D.; Gutierrez, J.; Ray, S.K. Securing RPL routing protocol from blackhole attacks using a trust-based mechanism. In Proceedings of the 2016 26th International Telecommunication Networks and Applications Conference (ITNAC), Dunedin, New Zealand, 7–9 December 2016; pp. 115–120.
36. Djedjig, N.; Tandjaoui, D.; Medjek, F.; Romdhani, I. New trust metric for the RPL routing protocol. In Proceedings of the 2017 8th International Conference on Information and Communication Systems (ICICS), Irbid, Jordan, 4–6 April 2017; pp. 328–335.
37. Elleuchi, M.; Boujeleben, M.; Abid, M.; BenSaleh, M.S. Securing RPL-based Internet of Things applied for water pipeline monitoring. In Proceedings of the 2017 25th International Conference on Software, Telecommunications and Computer Networks (SoftCOM), Split, Croatia, 21–23 September 2017; pp. 1–7.

38. Kallapur, P.V.; Ranjan, N.; Vidyarthi, R.; Anshuman; Singh, V. Enhanced variant of RPL for improved security. In Proceedings of the 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Udupi, India, 13–16 September 2017; pp. 2302–2306.
39. El Hajjar, A.; Roussos, G.; Paterson, M. Secure routing in IoT networks with SISLOF. In Proceedings of the 2017 Global Internet of Things Summit (GloTS), Geneva, Switzerland, 6–9 June 2017; pp. 403–408.
40. Kaur, G.; Saini, E.K.S. Securing network communication between motes using hierarchical group key management scheme using threshold cryptography in smart home using internet of things. In *Computing and Network Sustainability*; Vishwakarma, H.R., Akashe, S., Eds.; Springer: Berlin/Heidelberg, Germany, 2017; Volume 12, pp. 201–212.
41. Airehrour, D.; Gutierrez, J.; Ray, S.K. A testbed implementation of a trust-aware RPL routing protocol. In Proceedings of the 2017 27th International Telecommunication Networks and Applications Conference (ITNAC), Melbourne, Australia, 22–24 November 2017; pp. 1–6.
42. Ahsan, M.S.; Bhutta, M.N.M.; Maqsood, M. Wormhole attack detection in routing protocol for low power lossy networks. In Proceedings of the 2017 International Conference on Information and Communication Technologies (ICICT), Karachi, Pakistan, 30–31 December 2017; pp. 58–67.
43. Mayzaud, A.; Badonnel, R.; Chrisment, I. A Distributed Monitoring Strategy for Detecting Version Number Attacks in RPL-Based Networks. *IEEE Trans. Netw. Serv. Manag.* **2017**, *14*, 472–486. [[CrossRef](#)]
44. Gara, F.; Saad, L.B.; Ayed, R.B. An intrusion detection system for selective forwarding attack in IPv6-based mobile WSNs. In Proceedings of the 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), Valencia, Spain, 26–30 June 2017; pp. 276–281.
45. Ma, G.; Li, X.; Pei, Q.; Li, Z. A security routing protocol for Internet of Things based on RPL. In Proceedings of the 2017 International Conference on Networking and Network Applications (NaNA), Kathmandu, Nepal, 16–19 October 2017; pp. 209–213.
46. Medjek, F.; Tandjaoui, D.; Romdhani, I.; Djedjig, N. A trust-based intrusion detection system for mobile RPL based networks. In Proceedings of the 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Exeter, UK, 21–23 June 2017; pp. 735–742.
47. Althubaity, A.; Ji, H.; Gong, T.; Nixon, M.; Ammar, R.; Han, S. ARM: A hybrid specification-based intrusion detection system for rank attacks in 6TiSCH networks. In Proceedings of the 2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Limassol, Cyprus, 12–15 September 2017; pp. 1–8.
48. Lahbib, A.; Toumi, K.; Elleuch, S.; Laouiti, A.; Martin, S. Link reliable and trust aware RPL routing protocol for Internet of Things. In Proceedings of the 2017 IEEE 16th International Symposium on Network Computing and Applications (NCA), Cambridge, MA, USA, 30 October–1 November 2017; pp. 1–5.
49. Pu, C.; Hajjar, S. Mitigating Forwarding misbehaviors in RPL-based low power and lossy networks. In Proceedings of the 15th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 12–15 January 2018; pp. 1–6.
50. Mehta, R.; Parmar, M.M. Trust based mechanism for securing IoT routing protocol RPL against wormhole & grayhole attacks. In Proceedings of the 3rd International Conference for Convergence in Technology (I2CT), Pune, India, 6–8 April 2018; pp. 1–6.
51. Nikravan, M.; Movaghar, A.; Hosseinzadeh, M. A Lightweight Defense Approach to Mitigate Version Number and Rank Attacks in Low-Power and Lossy Networks. *Wirel. Pers. Commun.* **2018**, *99*, 1035–1059. [[CrossRef](#)]
52. Ghaleb, B.; Al-Dubai, A.; Ekonomou, E.; Qasem, M.; Romdhani, I.; Mackenzie, L. Addressing the DAO Insider Attack in RPL's Internet of Things Networks. *IEEE Commun. Lett.* **2019**, *23*, 68–71. [[CrossRef](#)]
53. Jiang, J.; Liu, Y.; Dezfouli, B. A root-based defense mechanism against RPL blackhole attacks in internet of things networks. In Proceedings of the 2018 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC), Honolulu, HI, USA, 12–15 November 2018; pp. 1194–1199.
54. Conti, M.; Kaliyar, P.; Rabbani, M.M.; Ranise, S. SPLIT: A secure and scalable RPL routing protocol for internet of things. In Proceedings of the 2018 14th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Limassol, Cyprus, 15–17 October 2018; pp. 1–8.
55. Airehrour, D.; Gutierrez, J.A.; Ray, S.K. SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things. *Future Gener. Comput. Syst.* **2019**, *93*, 860–876. [[CrossRef](#)]

56. Arış, A.; Örs Yalçın, S.B.; Oktuğ, S.F. New lightweight mitigation techniques for RPL version number attacks. *Ad Hoc Netw.* **2019**, *85*, 81–91. [[CrossRef](#)]
57. Groves, B.; Pu, C. A Gini index-based countermeasure against sybil attack in the internet of things. In Proceedings of the MILCOM 2019—2019 IEEE Military Communications Conference (MILCOM), Norfolk, VA, USA, 12–14 November 2019; pp. 1–6.
58. Bhalaji, N.; Hariharasudan, K.S.; Aashika, K. A trust based mechanism to combat blackhole attack in RPL protocol. In Proceedings of the ICICCT 2019—System Reliability, Quality Control, Safety, Maintenance and Management, Singapore, 29–30 April 2019; pp. 457–464.
59. Choudhary, S.; Kesswani, N. Cluster-based intrusion detection method for internet of things. In Proceedings of the IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA), Abu Dhabi, UAE, 3–7 November 2019; pp. 1–8.
60. Thulasiraman, P.; Wang, Y. A lightweight trust-based security architecture for RPL in mobile IoT networks. In Proceedings of the 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 11–14 January 2019; pp. 1–6.
61. Yugha, R.; Chithra, S. Attribute based trust evaluation for secure RPL protocol in IoT environment. In Proceedings of the 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN), Vellore, India, 30–31 March 2019; pp. 1–7.
62. Zhang, T.; Ji, X.; Xu, W. Cuckoo-RPL: Cuckoo filter based RPL for defending AMI network from blackhole attacks. In Proceedings of the 2019 Chinese Control Conference (CCC), Guangzhou, China, 27–30 July 2019; pp. 8920–8925.
63. Tandon, A.; Srivastava, P. Trust-based enhanced secure routing against rank and sybil attacks in IoT. In Proceedings of the Twelfth International Conference on Contemporary Computing (IC3), Noida, India, 8–10 August 2019; pp. 1–7.
64. Verma, A.; Ranga, V. ELNIDS: Ensemble learning based network intrusion detection system for RPL based internet of things. In Proceedings of the 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Ghaziabad, India, 18–19 April 2019; pp. 1–6.
65. Farzaneh, B.; Montazeri, M.A.; Jamali, S. An anomaly-based ids for detecting attacks in RPL-based internet of things. In Proceedings of the 5th International Conference on Web Research (ICWR), Tehran, Iran, 24–25 April 2019; pp. 61–66.
66. Aydogan, E.; Yilmaz, S.; Sen, S.; Butun, I.; Forsström, S.; Gidlund, M. A central intrusion detection system for RPL-based industrial internet of things. In Proceedings of the 15th IEEE International Workshop on Factory Communication Systems (WFCS), Sundsvall, Sweden, 27–29 May 2019; pp. 1–5.
67. Fatima tuz, Z.; Jhanjhi, N.; Brohi, S.N.; Malik, N.A. Proposing a rank and wormhole attack detection framework using machine learning. In Proceedings of the 2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS), Karachi, Pakistan, 14–15 December 2019; pp. 1–9.
68. Taghanaki, S.R.; Jamshidi, K.; Bohlooli, A. DEEM: A Decentralized and energy efficient method for detecting sinkhole attacks on the internet of things. In Proceedings of the 2019 9th International Conference on Computer and Knowledge Engineering (ICCKE), Mashhad, Iran, 24–25 October 2019; pp. 325–330.
69. Patel, H.B.; Jinwala, D.C. Blackhole detection in 6LoWPAN based internet of things: An anomaly based approach. In Proceedings of the TENCON 2019—2019 IEEE Region 10 Conference (TENCON), Kochi, India, 17–20 October 2019; pp. 947–954.
70. Soni, G.; Sudhakar, R. A L-IDS against dropping attack to secure and improve RPL performance in WSN aided IoT. In Proceedings of the 2020 7th International Conference on Signal Processing and Integrated Networks (SPIN), Noida, India, 27–28 February 2020; pp. 377–383.
71. Zaminkar, M.; Fotohi, R. SoS-RPL: Securing Internet of Things against Sinkhole Attack Using RPL Protocol-Based Node Rating and Ranking Mechanism. *Wirel. Pers. Commun.* **2020**. [[CrossRef](#)]
72. Hashemi, S.Y.; Aliee, F.S. Fuzzy, Dynamic and Trust Based Routing Protocol for IoT. *J. Netw. Syst. Manag.* **2020**. [[CrossRef](#)]
73. Djedjig, N.; Tandjaoui, D.; Medjek, F.; Romdhani, I. Trust-aware and cooperative routing protocol for IoT security. *J. Inf. Secur. Appl.* **2020**, *52*, 102467. [[CrossRef](#)]

74. Murali, S.; Jamalipour, A. A Lightweight Intrusion Detection for Sybil Attack under Mobile RPL in the Internet of Things. *IEEE Internet Things J.* **2020**, *7*, 379–388. [[CrossRef](#)]
75. Team, R. *RStudio: Integrated Development for R*; RStudio, Inc.: Boston, MA, USA, 2015; Volume 42, p. 14. Available online: <http://www.rstudio.com> (accessed on 8 September 2020).



© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).