International Journal of Pure and Applied Mathematics
Volume 118 No. 20 2018, 653-667
ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

A Comprehensive Review on Security Attacks in Dynamic Wireless Sensor Networks based on RPL protocol

Basim Ahmad Alabsi[1,2,] Mohammed Anbar[1] & Selvakumar anickam[1]
National Advance IPv6 Centre (NAv6), Universiti Sains Malaysia, Penang, Malaysia
Faculty of Computer Science, Najran University, Najran, Saudi Arabia
Email: basimahmadalabsi@gmail.com

Corresponding Author: Basim Ahmad Alabsi

Abstract–Routing Protocolis designed for Low Power and Lossy Networks (RPL) to support communication among thousands of devices.Internet of Things (IoT) comprised of smart devices like sensors and actuators using RPL protocol. RPL is applied over different applications as industries, smart environments and urban areas. In this paper, a review on security attacks in wireless sensor networks is presented. Several research works have been undergone for resolving vulnerable security threats.Due to the increase in millions and billions of connected devices all over the world, security is a major issue. Hence the deployment of IoT sensor devices in Wireless Sensor Network (WSN) involves mechanisms and algorithms for providing confidentiality, privacy, authentication, attack identification and prevention.Hereby this paper work projects out the major requirements of security in WSN Since the participation of different attacks have been tremendously increased. RPL in IoT is enabled for many real-time applicationswhich also include sensitive data transmissions. The observation in previous research works under security are studied and suggested with future directions.

Index Terms –RPL, Security, attacks, Internet of Things, Low power and Lossy Networks (LLN)

1. Introduction

Developments in recent technologies have more importance to use internet in human's day-to-day life. Worldwide usage of IoT deals some challenges and limitations to be overwhelmed [1].The traditional fundamentals used in IoT are IPv4, IPv6, WSN, IEEE 802.15.4, RPL and Low Power Wireless Personal Area Network (6LoWPAN). IoT is comprised of different objects as vehicles, buildings, smart devices, etc, [2]. Smartdevices include mobiles phones and different types of sensors.Sensor devices in WSN is deployed for data acquisition, collection and analyzing. WSN with IoT covers several application of monitoring that are in industries, human health, electrical equipment, natural disaster, city pollution, water quality, smart grid, smart home, intelligent transportation, etc,.The growth of IoT is also applicable for Radio Frequency Identification (RFID) and mobile communications. IoT is comprised of four significant layers as sensing layer, network layer, service layer and interface layer [3], [4]. Fig 1 depicts the IoT environment with the major categories of application in which it is being used.In IoT the providence of privacy and security are considered to be the two major challenges while applied on any type of application. To ensure privacy from different harmful attacks a strong secure protocol is required. Since dynamic movement of IoT devices, the cause of attacks will be wider and complex to detect a specific unauthorized IoT device. Hence security in IoT should be ensured in each layer for achieving better performances [5], [6]. IoT in WSN is supported to aggregate all private information periodically and transmit directly to move the life with advanced technologies. Attacks in IoT are broadly categorized into direct attack and indirect attack. WSN-IoT also focused to improve Quality of Service (QoS) by which more numbers of users are attracted towards these recent technologies [7].Recent merging of WSN with IoT is designed for many novel possibilities and ideas for enhancing over different visions [8]. The application of sensors in IoT is ubiquitous for sharing information globally [9].Increased demand on internet has introduced smart devices via which people share all information. All intelligent applicationsare constructed by enabling advanced features and novelty.Innovative ideas in

IoT were initiated from the evolution of Internet of Things [10].Evolution of IoT shows growth in terms of technology, size, inter connection, data collection, system interaction and use of smart devices. The solution for privacy threats follows any one of the following; identification, profiling, localizing, tracking. Online Social Networks (OSN) is also a major category in IoT that deals with several harmful attacks and hence security protection in OSN is mandatory to safeguard data.

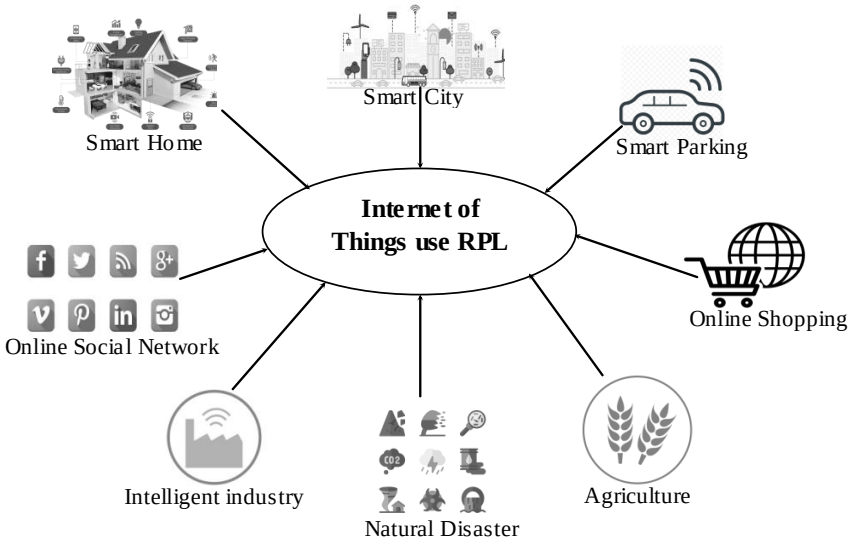

Figure. 1 IoT Environment

Security in IoT is supported by RPL, 6LoWPAN to minimize the impact of attacks [11].Attacks that occur based on RPL topology are selective forwarding attack, sinkhole attack, Sybil attack, hello flooding attack, wormhole attack, Denial of Service (DoS) attack, blackhole attack, clone ID attack, spoofing attack and more. For the purpose of security IoT designs an Intrusion Detection System (IDS) that detects attack with respect to event, host, specifications and signature based. RPL routing in IoT is applied on different standards; IEEE 802.15.4 is used in WSN and IEEE 805.15.1 is for Bluetooth [12]. IDS are helpful to extensively provide counter measures for internal attacks in WSN [13].In sensor network, each node is comprised with physical layer, datalink layer, network layer, transport layer and application layer. Each layer is subjected to different attacks; therefore security is needed to be provided in each layer. The major requirements of security are authentication, confidentiality, freshness, integrity, robustness and resiliency. Cryptography techniques were used for ensuring secure transmission of sensitive data.Firewall is involved for analyzing a packet in IDS to defend against dangerous attacks [14]. Use of IDS and firewall are considered to be light weight methods for resource constrained environment to filter out attackers. Expected Transmission (ETX) metric and rank are used in IDS for identifying malicious activities performed by nodes [15].ETX metric is computed from probabilities of received packets and acknowledgements. IDS system is proposed based on geographical hints, since rank is also taken in account. The determined ETX metric represents the distance between root node and the neighboring node.

2. Background Overview

2.1 RPL routing

RPL supports various applications in recent trends, RPL uses IPv6 (i.e.) based on distance-vector proactive routing protocol. Traditional process followed in RPL is the construction of Destination-Oriented Directed Acyclic Graph (DODAG) in the network [16], [17]. DODAG is created from the root node (i.e.) sink which is responsible to aggregate information from nodes participating in this network. To build DODAG four significant control messages are used such as DODAG Information Solicitation (DIS), DODAG Information Object (DIO), Destination Advertisement Object

(DAO) and DODAG Advertisement Object Acknowledgement (DAO-ACK). Each control message is necessary for the construction of DODAG to perform routing in RPL. Unicast and multicast data dissemination is performed using the exchange of these control messages [18], [19].

Table .1 DODAG control Messages

Control Message	Purpose
DIO message	This control message is initiated by the root node i.e. sink. This message is broadcasted to all the nodes present in the root node's coverage range. DIO message is required to adopt as a node in DODAG.
DIS message	This message is necessary while a node joining the DODAG. DIS control message is unicasted towards the neighboring nodes.
DAO message	It is a multicast message that is sent in terms of point-to-multipoint. Using this control message the nodes transfer information in upward direction which reaches the root.
DAO-ACK message	DAO-ACK is an acknowledgement message that is transmitted by a node which have received DAO message.

On the exchanges of control messages as shown in table 1, a complete DODAG is constructed to perform routing. This is also applicable for dynamic work nature of nodes.

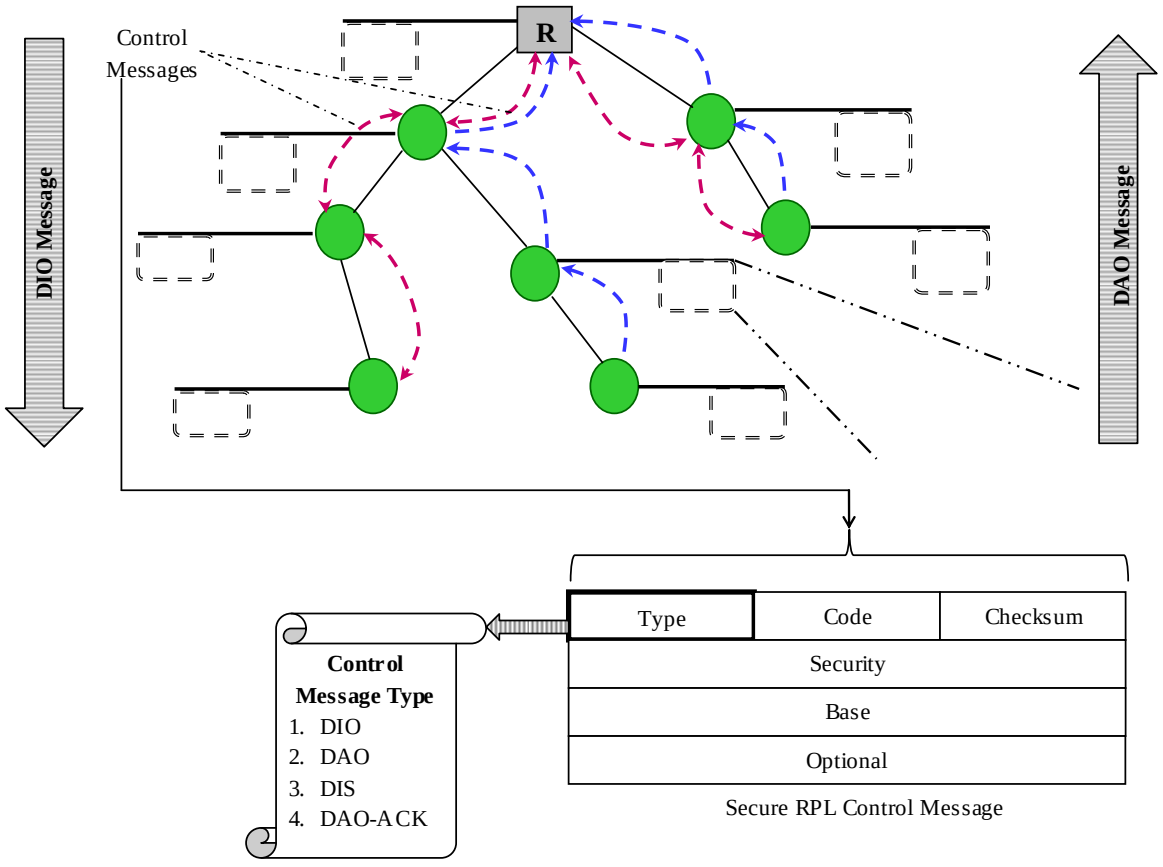

Figure.2. DODAG construction

Rank is provided for each node, on completion of DODAG construction. Ranking values are initiated from the root node and ends at the last node present in constructed DODAG. Node's rank value is provided based on the position of each node with respect to root node. Fig 2 shows the construction of DODAG from the root node and the corresponding rank values are given. For the purpose of security the control message format is included with a security field. The requirement of security is concentrated while constructing DODAG before routing is performed [20]. RPL follows two different topologies hierarchical and flat, this topology supports both static and dynamic nodes and achieves higher scalability [21].RPL involves with two modes of operation such as storing and non-storing. It is enabled to support three types of communication that is point-to-point, point-to-multipoint and multipoint-to-point. Here DODAG is constructed using control messages, hence RPL does not exchanges any hello packets with its neighboring nodes for routing. RPL performs routing after construction of DODAG.

2.2 Challenges of RPL

RPL routing is performed with certain Objective Function (OF) that is selected for routing a packet between nodes [22]. The majorly used Objective Functions are hop count, ETX, energy, stability, distance, Signal to Noise Ratio (SNR), connectivity and others. To achieve better results of RPL routing, a best objective function is selected, which is challenging in RPL routing.Other major challenges in RPL are discussed by authors in [23]. Due to the reason of battery-assisted node's participating in the network load balancing is required. Load balancing is needed while the level of traffic is too high, which is caused when thousands of nodes involve in data transmission. Load balancing issue is discussed under heavier traffic scenario.Multicast routing is significant in RPL which serves data dissemination and data broadcasting in the network. Traditionally Trickle Multicast (TM) algorithm, Stateless Multicast RPL Forwarding (SMRF)algorithm, Bi-directional Multicast RPL Forwarding (BMRF) algorithm is used [24], [25], [26].

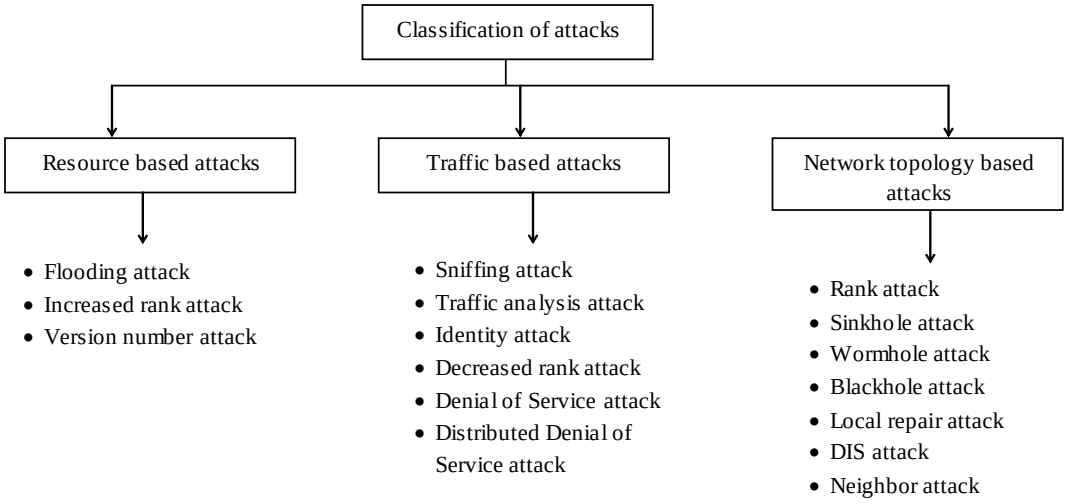

Figure.3. Attacks in RPL

Multicasting algorithms focused on suppression of re-broadcasted packets and also re-broadcasting causes overhead in the network. Data broadcasting using conventional algorithms also leads to a challenging process in RPL. One of the major challenge is security, even though security is optional. RPL used in different applications, each application involves with the participation of huge number of legitimate users and illegitimate users. Therefore security providence is required to ensure secure communication between users in the network. The challenging in ensuring security are trust management, bootstrapping, interoperability, mobility monitoring, legacy systems, resource provisioning, scalability, computation complexity and time maintenance [27]. As per the sensitivity of data sharing, the level of security has to be increased.

3. Common attacksagainst RPL

In RPL attacks are broadly classified into three categories as resource based, topology based and traffic based [28].Each category of attack is sub classified into two other partitions. Fig 3 depicts the major classification of attacks that occur in RPL routing. Resource based RPL attack is further classified into direct and indirect attacks. Traffic plays a major role in RPL due to the increased number of user's participation, therefore attackers penetrate the network via traffic. Traffic based attacks in RPL are classified into Eavesdropping and misappropriation [29]. The Eavesdropping attackers perform malicious activities as listening to other packet transmission and extracting the routing information from packets. The third category is network topology based attacks which is sub classified into sub-optimization attacks and isolation attacks [30].The goal of the attackers in sub-optimization attack is to minimize the performance of the entire network by involving into optimal path selection process.

Table 2Attacks against RPL

Attack	Working	Attack detection	Impacts network parameters	Counter Measure
Sink hole attack [31]	Sends false information (i.e.) false rank value	Yes	Packet loss	Analyzing packets
Rank attack [32]	Provides poor route quality	Yes	Downgrade QoS parameters	Correlation of location
Sybil Mobile attack [33]	Compromises legitimate nodes	Yes	Packet delivery ratio	Trust based IDS
Sybil attack [34]	Steal identities	No	Message overhead, Energy consumption	Evaluating the effects of attack
Wormhole attack [35]	Creates tunnel between communicating nodes	Yes	Detection rate, Packets overhead	Use location information and neighbor information
DoS attack [36], [37]	Sending unusual set of data to a target node, also occurs in distributed manner all over the network	No	Received Signal Strength, Packet sending rate, Packet receiving rate, Packet delivery ratio, Packet dropping rate, Packet forwarding rate	IDS, IDS probe
Version Number attack [38], [39]	Alters the version number which is associated to topology	Yes	Control overhead, True positive rate, False positive rate, Packet delivery ratio	Monitoring architecture, Distributed and cooperative verification mechanism
Blackhole attack [40]	Huge packet loss, limits resources	Yes	Packet loss, Throughput	Trust based mechanism
Selective Forwarding attack [41]	Drop sensitive information contained in a packet, Compromises legitimate nodes	Yes	Detection probability, overhead	Sequential Probability Ratio Test (SPRT), determine dropped packets with respect to ETX

Isolate attackers participate in the network to segregate a particular node from the network and make it no longer to perform communication with other nodes. Since RPL enables the support of dynamic network environment, the attackers keeps moving from one part to another. However a particular attacker is detected, it can participate in some other location by varying its position and identity. Table 2 illustrates different attacks that participate in network which is involved to degrade the network performance over significant metrics. The attacks are not limited to this list, it is extensively increased as per the advancement in technology.

4. Requirement of Security in RPL

In this section, the requirements of security in RPL are discussed. All these requirements are raised only due to the involvement of different types of attacks that is discussed in previous sections. To attain these requirements, several authors have concentrated over security in RPL. Hence the requirements of security in RPL are listed in the following section;

a) Confidentiality

Confidentiality is referred to data security maintained from other unauthorized entities in the network. This is achieved only when the end users is enabled to access their own data. Therefore those data is not allowed to have privilege access by other entities.

b) Integrity

Integrity is definedto guarantee the transmitted datawhich will never have a chance to be corrupted. Integrity in security mechanism occurs in two ways such as (i) Malicious altering and (ii) Accidental altering. In malicious altering, the data is purposely corrupted whereas in accidental altering the data is corrupted due to technical error.

c) Identity Management

Identity is unique for each node, since the individuality and legitimacy of the node can be predicted. The possibility is that a malicious node can falsely use identity of legitimate node; hence identity management is a significant requirement. Legitimate nodes are detected using this unique identity.

d) Anonymity

Anonymity is defined as maintenance of security at user side.An owner's data is kept secure and it is not to any other entities participating in the network. User data is protected to survive anonymity.

e) Authentication

Verifying a user entity by means of their original identity or address is called authentication. This process is performed by the network administration before allowing the user to perform data transmission.Authentication is major requirement which is needed to identify a user's true behavior and this is performed before a end-user starts their data transmission.

f) Non-repudiation

For identification and isolation of unauthorized node, this non-repudiation is required. Node behavior is detected either as normal / abnormal, then the particular node is isolated. So without a good security mechanism it is complex to achieve this requirement.

g) Availability

Availability is defined as maintenanceof available network services or network resources for the use of legitimate users. Availability ensures the survivability of entire network under the activities of attackers involved into the network.

h) Privacy

Privacy is required only when two end-users perform communication. Since an intruder may involve intermediately to capture the sensitive data that is shared between two entities. Privacy requirement in security is solved by providing a cryptography algorithm.

5. Previous research works

Many authors in their work have discussed with the solution of mitigating the attacks. In [42] wormhole attack detection method was proposed in IPv6 over LLN in WSN application. To detect wormhole attacks, a rank threshold is set by which the wormhole attackers are predicted from rank values. The DIO control message include rank threshold and rank difference value. Rank threshold is the different between ranking values of parent node and the child node. Here malicious node is detection if the rank different value obtained is grater than the rank threshold. Before computing the rank difference, blacklist of the node is verified. This work was able to achieve 100% accuracy in detection of wormhole attackers.Wormhole attacks are broadly classified into three types as closed wormhole, half-open wormhole and open wormhole [43]. Honeypot method also aims to minimize the forensics and other intrusions participating in the network.A Merkle tree based authentication protocol was proposed to ignore wormhole attackers [44]. This tree based approach provides authenticated communication which hashes the information. Merkle tree is constructed from the child nodes by using the Identity and key. Merkle tree is completely built only when it reaches root node. Authentication process is held by one way hashing pairs of identities and keys. In this work, the use of authentication process was enabled to prevent the wormhole attacker, but this was not focused to detect those attackers. In this case the prevented attackers participate in different location at next time period.

Vulnerabilities in routing are solved by providing node-to-node encryption based authentication [45]. This work was focused on two attacks as sinkhole attack and spoofing attack. Each node advertises for an encryption key before beginning data transmission. Requesting node's Identity / addressed is authenticated and then encryption key is provided.Further each new incoming node advertises for a secure encryption key.An Intrusion Detection and Response System (InDReS) was proposed to provide security [46]. Malicious node is detected based on the evidence followed by ranking algorithm. Evidence theory involves Dempster-Shaffer evidence theory which proceeds with basic probability assignment function, belief and Dempster combination Rules. Here a node is isolated, if the summed up ranking value is lesser than the parent node and also alert information is sent to other nodes in the network about the isolated node.

Specification based IDS were proposed for detecting RPL attacks especially rank and local repair attack [47].A monitoring architecture is designed in which object identity, rank, parent identity, parent rank and topological changes are monitored.Finite state machine is applied on each monitoring node to predict the state. Rank attack is detected by monitoring node which identifies the forging rank of a node, since it has the knowledge of root node's rank. Local repair attack is identified based on the threshold value.Common attacks in RPL were analyzed using trust management scheme in WSN [48]. In this trust based model, two different trust values are computed as direct trust and indirect trust, further the trusted nodes are constructed into tree with respect to the trust management scheme. Internal and external attackers are overcome by this scheme. Internal attack includes DoS, sniffing and replay attack whereas external attack is an illegitimate node that compromises a legitimate node that includes blackhole attack, greyhole attack, sinkhole attack and wormhole attack. This trust mechanism is enabled to monitor the behavior of nodes, so that the malicious activities of illegitimate node.A sliding window is used for the estimation of trust values of nodes. Direct trust is computed from the predicted number of misbehaviors of a node and indirect trust is computed by the recommendation trust. After computing trust values tree is constructed, followed by key establishment and authentication. Therefore this scheme was applied for resolving both internal and external attackers.

A lightweight Identity Based Offline-Online Signature (IOOS) based scheme was proposed in solution of version number attack and rank spoofing attack [49].A probabilistic key generation algorithm was used to generate private key and master secret key based on user's identity and system parameters. Usually in a version number attack the attacker increases DODAG version number and broadcast it towards the receiving nodes. If a global repair occurs, then DODAG generates new version number. Therefore this attack is performed repeatedly to downgrade the resource utilization.In this work signing of version number and rank value using the private key is enabled to overwhelm these two attacks and minimizes energy consumption and computation time in root node and also in other connect nodes.

Metric-based RPL Trustworthiness Scheme (MRTS) suggest in identifying the honest nodes according to the node's behavior [50]. In MRTS, Extended RPL Node Trustworthiness (ERNT) is computed to improve security in RPL. Direct trust is a weighted value of node's honesty, energy and unselfishness and indirect trust is the recommendation provided with respect to a node's trust. Security is sustained by using a trustworthiness scheme. Wormhole attack and flooding attack detection in RPL protocol was discussed by authors in [51]. Flooding attacks is also called as Denial of Service which sends continuous messages towards a targeted node. Wormhole attack is identified by the rank value of the node, if the rank value tends to be larger than the threshold value then that node is detected as wormhole attacker. Next flooding attack is identified by the node counting the number of router advertisement and neighbor advertisement messages. If the count of these two messages is greater than the threshold, then they are detected as flooding attacker. Initially the node checked whether it is present in the blacklist or not. If present in blacklist, then the presence of attacker node is alerted to neighboring node, else moves on for verification. Finally the detected attacker node is put into blacklist and also neighboring nodes are alerted

An malicious node detection and authentication by using standard 6LoWPAN Neighbor discovery and RPL protocol [52]. The additionally required control messages are minimized in this research work. A cryptography mechanism is used that is AES symmetric key algorithm, this mechanism guarantees node' authenticity and integrity. The solution of authentication is by data frame filtering function and distributed mechanism to identify the legitimate data frames. Data frame filtering process involves with a unique global key which is initially set in border router and it changes dynamically for new nodes participating in the network. A new node entering into the network is authorized by exchanging messages between new node and border router. The new node initiate with router solicitation to router and then router responses with router advertisement, further the new node sends neighbor solicitation with address registration option. In the next messages the node is authenticated by using one-way challenge authentication protocol. Challenge is based on generated random nonce, global key and AES encrypted pre-shared key. After validating this challenge, a MAC is generated with AES for message authentication.

Trusted Platform Module (TPM) was developed to provide secure communication in RPL network [53]. The problems like storage, key generation and message signing in a cryptography oriented security is resolved in TPM.Public and private key are generated using RSA algorithm. The design of trust establishment and key exchange in TPM was enabled to support integrity and authenticity of the messages transmitted from one node to another. In this work, security is provided but it was not tested under the participation of harmful attackers in the network.

Table 3Layer based attacks and their countermeasures

Layer	Attacks performed	Countermeasures
Physical layer	• Jamming attack • Tampering attack • Eavesdropping attack	• Monitoring architecture • Message Authentication Codes
Data link layer	• Sybil attack • Collisions attack • Exhaustion attack • Version Number attack	• Multiple Channel Access Methods • Error detection schemes • Signature schemes • Authentication methods • Trustworthiness methods
Network layer	• Spoofing attack • Misdirection attack • Smurf attack • Wormhole attack • Sinkhole attack • Blackhole attack • Selective forwarding attack • Replay attack	• Secure Routing • Cryptographic methods • Trust management schemes • Monitoring architecture • Localization verifying schemes • Radio Frequency Identification
Transport layer	• Flooding attack • De-synchronization attack	• Deep Packet Inspection • Intrusion Detection system
Application layer	• DoS attack • DDoS attack • Reprogramming attack	• Packet analysis • Intrusion Detection System

Attacks in RPL were participated according to processing of each layer. RPL oriented attacks involved in each layer are discussed [54], [55]. Attacks and their countermeasures are descripted in table 3, hereby it is clear that different attacks cannot be identified by using a single mechanism. Each attack varies in their characteristics and also in their goal to degrade a network performance.Data aggregation in WSN using a protocol also requires security [56]. Randomized multipath route was developed to solve the security constraints.In this work the authors have presented Purely Random Propagation (PRP), Directed Random Propagation (DRP), NonRepetitive Random Propagation (NRRP) and Multicast Tree assisted Ransom Propagation (MTRP). Shamir's algorithm is performed for secret sharing of data from sensor node to sink node.This secure data aggregation was tested under a limited number of blackhole attackers; hence it was not able to tolerate larger number of blackhole attackers.Lightweight authentication schemes as symmetric key cryptography or asymmetric key cryptography can be involved in RPL to provide security [57]. In RPL the nodes operate at in three different modes, first unsecured mode in which security field is absent in control message. Second is pre-installed mode in which key pairs are provided before deployment and third id authenticated mode in which the node is authenticated with the corresponding security process before joining the DODAG.Therefore, this section results with the vulnerabilities and attacks that participate in network while using RPL [58]. Due to dangerous attacks in IoT, mitigation of these attacks is mandatory. Attackers aim to gather sensitive data, abolish user's device, destroy network

performance and more. As per their goal, they participate in the network and communicate with legitimate nodes. A detailed survey on previous research works, on providence of security in RPL is discussed in this section.

5.Problems and Future Directions

The major security problems analyzed from previous research work is listed as follows;

- Privacy concerns
- Insecure integrated cloud / mobile interface
- Inadequate configurations for security
- Insecure web interface
- Lack of authentication
- Insufficient cryptographic techniques

The above mentioned problems of security are analyzedfrom the review gone over RPL used in WSN application. The problems in security are needed to be recognized and solved with novel solutions, so that in future IoT will be free of vulnerabilities and threats.IoT supports in many sensitive applications and for efficient use in particular application, IoT is integrated with mass storage services, social media, cloud, etc,.

In future IoT will be used in urban areas and which is required to be supported with secure connectivity. On taking into account of this security issue, IoT needs more analysis and novel security oriented algorithms. The use of recent development in the field of bio-metrics for security in IoT can be provided more concentration.Application based security can be provided, since it is sure that not all the data sharing is sensitive. The future requirements in IoTto solve different attacks are,

- Bio-metric based authentication
- Secret session establishment
- RFID based authentication
- Hybrid cryptography techniques
- Multi-factor authentication
- Face recognition / iris recognition
- QR code based authentication
- Cyber sensor to capture real time events

A best providence of security in IoT enables its use over private businesses, IT Companies, Organizations and Government authorities [59]. Whatever the application is used in IoT, the end-to-end security is suggested to be used. IoT is one of the developing trend among people all over the world, hence security providence will attract people in urban areas due to its widespread applications.

6. Conclusion

In this paper, we have reviewed all the aspects of security in RPL using over WSN. Security has become a major requirement in IoT-WSN due to participation of huge number of users under different applications worldwide. Recent research works that are published over 50 papers is discussed and the providence of security is descripted. The views of authors differ in solving different attacks and ensure higher level of security. The ubiquitous growth,in IoT supported billions of smart devices that inturndeveloped insecurity to participate in IoT. From this paper, we have analyzed the security risks that are associated to IoT and its supported applications.The requirements and common attacks that are held in RPL are detailed and also previous research works designed for security in RPL is also studied. The study of previous works insists the need of security to resolve different attacks that actively participate in the network. Hereby we conclude, this discussion is to promote security algorithms and techniques in all the sensitive

applications.Ubiquitous use of smart devices with advanced technology improved worldwide connectivity; however it has also increased the vulnerabilities and threats broadly. Harmful vulnerabilities should be mitigated to sustain the developments in IoT.

References

[1] Vipindev Adat, B.B. Gupta, "Security in Internet of Things: issues, challenges, taxonomy and architecture", Telecommunication systems, Springer, pp 1 – 19, 2017.

[2] Supriya C.Padwal, P.Balaramudu, Manoj Kumar, Chanakya Kumar Jha, "Analysis of environment changes using WSN for IoT applications", International Conference for Convergence in Technology, IEEE, 2017.

[3] Sarra Hammoudi, Zibouda Aliouat, Saad Harous, "Challenges and research directions for internet of things", Telecommunication systems, Springer, pp 1 – 19, 2017.

[4] Shancang Li, Li Da Xu, Shanshan Zhao, "The internet of things: a survey", Information systems Frontiers, Springer, vol. 17, no. 2, pp 243 – 259, 2015.

[5] Qi Jing, AthanasiosV. Vasilakos, jiafu Wan, Jingwei Lu, Dechao Qiu, "Security of the Internet of Things: perspectives and challenges", Wireless Networks, Springer, vol. 20, no. 8, pp 2481 – 2501, 2014.

[6] Arvind Kamble, Virendra S. Malemath, Deepika Patil, "Security attacks and secure routing protocols in RPL-based Internet of Things: Survey", International Conference on Emerging Trends and Innovation in ICT, pp 33 – 39, 2017.

[7] Syarifah Ezdiani, Indrajit S Acharyya, Sivaramakrishnan Sivakumar, Adnan Al-Anbuky, "An IoT Environment for WSN Adaptive QoS", IEEE International Conference on Data Science and Data Intensive Systems, pp 586 – 593, 2015.

[8] Andrew Whitmore, Anurag Agarwal, Li Da Xu, "The Internet of Things – A survey of topics and trends", Information systems Frontiers, Springer, vol. 17, no. 2, pp 261 – 274, 2014.

[9] Stefan Forsstrom, Theo Kanter, "Enabling ubiquitous sensor-assisted applications on internet-of-things", Personal and Ubiquitous Computing, Springer, vol. 18, no. 4, pp 977 – 986, 2014.

[10] Jan Henrik Ziegeldorf, Oscar Garcia Morchon, Klaus Wehrlr, "Privacy in the Internet of Things: threats and challenges", Security and Communication Networks, Wiley Online Library, vol. 7, no. 12, pp 2728 – 2742, 2013.

[11] Pavan Pongle, Gurunath Chavan, "A survey: Attacks on RPL and 6LoWPAN in IoT", International Conference on Pervasive Computing, IEEE, 2015.

[12] S.Umamaheswari, Atul Negi, "Internet of things and RPL routing protocol: A study and evaluation", International Conference on Computer Communication and Informatics, IEEE, 2017.

[13] Anhtuan Le, Jonathan Loo, Aboubaker Lasebae, Mahdi Aiash, Yuan Luo, "6LoWPAN: a study on QoS security threats and countermeasures using intrusion detection system approach", vol. 25, no. 9, pp 1189 – 1212, 2012.

[14] Himanshu B.Patel, Devesh C. Jinwala, Dhiren R. Patel, "Baseline Intrusion Detection Framework for 6LoWPAN Devices", International Conference on Mobile and Ubiquitous Systems: Computing Networking and Services, ACM, pp 72 – 76, 2016.

[15] Dharmini Shreenivas, Shahid Raza, Thiemo Voigt, "Intrusion Detection in the RPL-connected 6LoWPAN Networks", ACM International Workshop on IoT Privacy, Trust and Security, pp 31 – 38, 2017.

[16] Ming Zhao, Arun Kumar, Peter Han Joo Chong, Rongxing Lu, "A comprehensive study of RPL and P2P-RPL routing protocols: Implementation, challenges and opportunities", Peer-to-Peer Networking and Applications, Springer, vol. 10, no. 5, pp 1232 – 1256, 2017.

[17] Belghachi Mohamed, Feham Mohamed, "QoS Routing RPL for Low Power and Lossy Networks", International Journal of Distributed Sensor Networks, 2015.

[18] Hanane Lamaazi, Nabil Benamar, Antonio J. Jara, "RPL-Based Networks in static and mobile environment: a performance assessment analysis", Journal of King Saud University - Computer and Information Sciences, 2017.

[19] Tao Zhang, Xianfeng Li, "Evaluating and analyzing the performance of RPL in contiki", Proceedings of the first international workshop on Mobile sensing, computing and communication, ACM, pp 19 – 24, 2014.

[20] Jorge Granjal, Edmundo Monteiro, Jorge Sá Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues", IEEE Communications Surveys & Tutorials, vol. 17, no. 3, pp 1294 – 1312, 2015.

[21] Deepak Sharma, Ajay Narayan Shukla, "A Comparative Study of the Routing Protocols LOAD and RPL in Low and Lossy Networks (LLN)", Journal of Engineering and Technology, vol. 2, no. 1, pp 85 – 87, 2014.

[22] Xiyuan Liu, Zhengguo Sheng, Changchuan Yin, Falah Ali, Daniel Roggen, "Performance Analysis of Routing for Low Power and Lossy Networks (RPL) in Large Scale Networks", IEEE Internet of Thing Journal, vol. 4, no. 6, pp 2172 – 2185, 2017.

[23] Hyung-Sin Kim, Jeonggil Ko, David E. Culler, Jeongyeup Paek, "Challenging the IPv6 Routing Protocol for Low Power and Lossy Networks (RPL): A Survey", IEEE Communications Suveys and Tutorials, vol. 19, no. 4, pp 2502 – 2525, 2017.

[24] George Oikonomou, Iain Phillips, "Stateless multicast forwarding with RPL in 6LowPAN sensor networks", IEEE International Conference on Pervasive Computing and Communications Workshops, pp 272 – 277, 2012.

[25] George Oikonomou, Iain Phillips, Theo Tryfonas, "IPv6 Multicast Forwarding in RPL-Based Wireless Sensor Networks", Wireless Personal Communication, Springer, 2013.

[26] Guillermo Gastón Lorente, Bart Lemmens, Matthias Carlier, An Braeken, Kris Steenhaut, "BMRF: Bidirectional Multicast RPL Forwarding", Ad Hoc Networks, Elsevier, 2016.

[27] Chakib Bekara, "Security Issues and Challenges for the IoT-based Smart Grid", International Workshop on Communicating Objects and Machine to Machine for Mission Critical Application, Elsevier, pp 532 – 537, 2014.

[28] Anth´ea Mayzaud, R´emi Badonnel , Isabelle Chrismen, "A Taxonomy of Attacks in RPL-based Internet of Things", International Journal of Network Security, vol.18, no. 3, pp 459 – 473, 2016.

[29] Divya Sharma, Ishani Mishra, Sanjay Jain, "A Detailed Classification of Routing Attacks against RPL in Internet of Things", International Journal of Advanced Research, Ideas and Innovations in Technology, vol. 3, no. 1, pp 692 – 703, 2017.

[30]Heiner Perrey, Martin Landsmann, Osman Ugus, Matthias Wahlisch, Thomas C. Schmidt, "TRAIL: Topology Authentication in RPL", International Conference on Embedded Wireless systems and Networks, ACM, pp 59 – 64, 2016.

[31] R. Stephen, L. Arockiam, "Intrusion Detection System to Detect Sinkhole Attack on RPL protocol in Internet of Things", International Journal of Electrical Electronics and Computer Science, vol. 4, no. 4, pp 16 -20, 2017.

[32] Anhtuan Le, Jonathan Loo, Aboubaker Lasebae, Alexey Vinel, Yue Chen, Michael Chai, "The Impact of Rank Attack on Network Topology of Routing Protocol for Low-Power and Lossy Networks", IEEE Sensors Journal, vol. 13, no. 10, pp 3685 – 3692, 2013.

[33] Faiza Medjek, Djamel Tandjaoui, Imed Romdhani, Nabil Djedjig, "A Trust-based Intrusion Detection System for Mobile RPL Based Networks", EEE International Conference on Internet of Things, 2017.

[34] Faiza Medjek , Djamel Tandjaoui, Mohammed Riyadh Abdmeziem, Nabil Djedjig,"Analytical evaluation of the impacts of Sybil attacks against RPL under mobility", International Symposium on Programming and Systems, 2015

[35] Pavan Pongle, Gurunath Chavan, "Real Time Intrusion and Wormhole Attack Detection in Internet of Things", International Journal of Computer Applications, vol. 121, no. 9, 2015.

[36] Anass Rghioui, Anass Khannous, Mohammed Bouhorma, "Denial-of-Service attacks on 6LoWPAN-RPL networks: Threats and an intrusion detection system proposition", Journal of Advanced Computer Science and Technology, vol. 3, no. 2, pp 143 – 153, 2014.

[37] Tejas M. Mehare, Snehal Bhosale, "Design and Development of Intrusion Detection System for Internet of Things", International Journal of innovative Research in Computer and Communication Engineering, vol. 5, no. 7, pp 13469 -13475, 2017.

[38] Anthea Mayzaud, Remi Badonnel, Isabelle Chrisment, "Detecting version number attacks in RPL-based networks using a distributed monitoring architecture", IEEE International Conference on Network and Service Management, 20116.

[39] FirozAhmed, Young-Bae Ko, "A Distributed and Cooperative Verification Mechanism to Defend against DODAG Version Number Attack in RPL", International joint conference on Pervasive and Embedded Computing and Communication systems, vol. 1, pp 55 – 62, 2016.

[40] David Airehrour, Jairo Gutierrez, Sayan Kumar Ray, "Securing RPL routing protocol from blackhole attacks using a trust-based mechanism", International Telecommunication Networks and Applications Conference, 2016.

[41]Fatma Gara, Leila Ben Saad, Rahma Ben Ayed, "An intrusion detection system for selective forwarding attack in IPv6-based mobile WSNs", International Wireless Communications and Mobile Computing Conference, pp 276 - 281,2017.

[42] Du Hsin Lai, "Detection of wormhole attacks on IPv6 mobility-based wireless sensor network", Journal on Wireless Communications and Networking, Springer, 2016.

[43] Roshini Patel, Rutvik Mehta, "A Survey: Locating the Attacker of Wormhole Attack on RPL in IoT", International Journal of Advanced Research in Engineering, Science and Technology, vol. 3, no. 6, pp 333 – 343, 2016.

[44] Faraz Idris Khan, Taeshik Shon, Taekkyeun Lee, Kihyung Kim, "Wormhole attack prevention mechanism for RPL based LLN network", International Conference on Ubiquitous and Future Networks, 2013.

[45] Clark Taylor, Thienne Johnson, "Strong authentication countermeasures using dynamic keying for sinkhole and distance spoofing attacks in smart grid networks", IEEE Wireless Communications and Networking Conference, 2015.

[46] M.Surender, A. Umamakeswari, “InDReS: An Intrusion Detection and Response system for Internet of Things with 6LoWPAN”, International Conference on Wireless Communications, Signal Processing and Networking, 2016.

[47] Anhtuan Le, Jonathan Loo, Yuan Luo, Aboubaker Lasebae, “Specification-based IDS for securing RPL from topology attacks”, IEEE IFIP Wireless Days, 2011.

[48] Zhi Hu, Yuxia Bie, Hong Zhao, “Trusted Tree-Based Trust Management Scheme for Secure Routing in Wireless Sensor Networks”, International Journal of Distributed Sensor Networks, 2015.

[49] Mohammad Nikravan, Ali Moaghar, Mehdi Hosseinzadeh, “A Lightweight Defense Approach to Mitigate Version Number and Rank Attacks in Low-Power and Lossy Networks”, Wireless Personal Communications, Springer, pp 1 – 25, 2018.

[50] Nabil Djedjig, Djamel Tandjaoui, Faiza Medjek, Imed Romdhani, “New trust metric for the RPL routing protocol”, International Conference on Information and Communication Systems, IEEE, 2017.

[51] Chia-Mei Chen, Sung-Chien Hsu, Gu-Hsin Lai, “Defense Denial-of-Service Attacks on IPv6 Wireless Sensor Networks”, Genetic and Evolutionary Computing, Springer, Volume 387, pp 319 – 326, 2016.

[52] Luís M.L. Oliveira, Joel J. P. C. Rodrigues, Amaro F. de Sousa, and Victor M. Denisov, “Network Admission Control Solution for 6LoWPAN Networks Based on Symmetric Key Mechanisms”, IEEE Transactions on Industrial Informatics, pp 1 – 10, 2016.

[54] Azamuddin, “Survey on IoT Security”, https://www.cse.wustl.edu/~jain/cse570-15/ftp/iot_sec2.pdf

[55] Krešimir Grgić, Višnja Križanović Čik, Vanja Mandrić Radivojević, “Security Aspects of IPv6-based Wireless Sensor Networks”, Conference on Science in Practice, vol. 7, no. 1, 2016.

[56] Tao Shu, Marwan Krunz, Sisi Liu, “Secure Data Collection in Wireless Sensor Networks Using Randomized Dispersive Routes”, IEEE Transactions on Mobile Computing, vol. 9, no. 7, pp 941 – 954, 2010.

[57] Mohamad Faiz Razali, Mohd Ezanee Rusli, Norziana Jamil, Roslan Ismail, Salman Yussof, “The authentication Techniques for enhancing the RPL Security Model: A Survey”, International Conference on Computing and Informatics , pp 735 – 743, 2017.

[58] Stuart Millar, “Network Security Issues in Internet of Things (IoT)”, Queen's University Belfast, 2016.

[59] Yogita Pundir, Nancy Sharma, Yaduvir Singh, “Internet of Things (IoT): Challenges and Future Directions”, International Journal of Advanced Research in Computer and Communication Engineering, vol. 5, no. 3, pp 960 – 964, 2016.