A Survey on Routing Protocols Exclusively for IoT

Ena Jain[1], Dr. D.V. Gupta[2], Dr. R.K. Naik[3]
[1]*Ph.D Research Scholar, Uttarakhand Technical University, Dehradun*
Assistant Professor, Department of CSE, DIT University, Dehradun, Uttarakhand
[2]*Professor and HOD, College of Engineering, Roorkee, Uttarakhand*
[3]*Professor, Department of CSE, MIT College, Maharashtra*

Abstract- Routing Protocol for low power and lossy network (RPL) isaIPV6 routing protocol standardised by IETF in 2012. With the development of IoT, RPL is entitled to new chancefor the development of wireless sensor networks in a large scale. It is able to meet the specific routing requirements of application areas including urban networks, building automation, industrial automation, and home automation. Among those mechanisms standardized in RPL, routing and message control are two important mechanisms in establishing and maintaining an effective and reliable network. In this survey paper, we investigate the most related studies obtained about RPL routing protocol that concern to its implementation, performance, applications evaluation, and improvement. Finally, this survey can support researchers to further understand the RPL and participate to further improve it in the future research works.

I. INTRODUCTION

The Internet of Things (IoT) is a technology that'spresently dynamical and reinventing business and society. Thischange leads to increase in focus on integrating, the new and massive flow of data from sensors and will be available as thefundamental service. The IoT has become a new focus forboth industry and academia involving information and communication technologies (ICTs), and it is predicted that there would be almost 50 billion devices connected with each other through IoT by 2020 [1]. The concept of IoT can be traced back to the pioneering work done by Kevin Ashton in 1999 and it is initially linked to the new idea of using radio frequency identification in supply chains. Soon after, this term became popular and is well known as a new ICT where the Internet is connected to the physical world via ubiquitous wireless sensor networks (WSNs) [2]. With the development of WSN technologies, a wide range of intelligent and tiny wireless sensing devices will be deployed in a variety of application environments. Generally, these sensing devices are constrained by limited energy resources (battery power), processing and storage capability, radio communication range and reliability, etc., and yet their deployment must cover a wide range of areas. In order to cope with those challenges, a number of breakthrough solutions have been developed, for example, efficient channel hopping in IEEE 802.15.4e TSCH [3], emerging IPv6 protocol stack for connected devices [4] and improved bandwidth of mobile
transmission. Routing, particular in large scale networks, is always challenging for resource constrained sensor devices. The IETF Routing Over Low-power and Lossy networks (ROLL) working group has been focusing on routing protocol design and is committed to standardize the IPv6 routing protocol for Low-power and Lossy Networks (LLN). RFC6550 [5], first proposed by ROLL group of IETF in the form of draft to define Routing Protocol over Low Power and Lossy Networks (RPL), serves as a milestone in solving routing problems in LLNs.

Due to the limitation of short-range radio in personal area network (PAN) and local area network (LAN), multi-hop transmission is necessary in large scale networks. RPL is designated to provide such a viable solution to maintain connectivity and efficiency in a cost effective way. However, there is a lack of existing literature in evaluating the RPL performance in large scale networks. RPL does not come with any major security features to secure routing completely and hence, it is vulnerable to various attacks on the network [5]. Security in RPL is a major issue that needs to be put in the limelight as routing carries data that should not be leaked or accessed by an intruder or any third party who is not an authorized member of the network. RPL gets affected majorly due to attacks by an outsider or evensometimes by insider nodes. Measures have been implied toprotect RPL from outside attacks, but there still poses threat from insider nodes. In this survey, we explore about Routing Protocol for Low Power and Lossy network, its working and also study its functionality for constrained networks.In this paper, we focus on the comprehensive review of RPL protocol and its performance.

II. LITERATURE SURVEY

This section gives an overview of some existing protocols based on RPL standard like in [1- 28]. The authors in [1] proposed Mobility enhanced RPL (MERPL) to improve the RPL and balance the traffic over the routes. MERPL outperforms standard RPL in terms of the stability of the path. However, authors do not utilize some major parameters such as the delay of handover, the cost of signalling, and the energy dissipation.

The authors in [2] investigated the RPL performance with some modifications. In the first step, the timer of the DIO trickle is disabled due to the unsuitability of using it in the periodic changing of topology. Then, the reactivity is enhanced through evaluating the quality of link directly with updating the graph of routing. After that, the problem of the loop is discovered and prevented through putting the ID of the parent in the DIO packet.

In [3], the GI-RPL scheme is proposed as an enhancement to the RPL in Vehicular Ad-hoc Networks (VANET). In order to deal with periodic changing in the topology, GI-RPL depends

on the localization of the node. The position of the node is determined by using the direction of the car and the distance to the sink. In addition, the duration of adaptive DIO is included in the solution instead of the timer of the trickle to increase the performance. An enhancement is introduced by these solutions to the packet submission rate and the message delay. Nevertheless, the constraint of power is not considered due to the characteristics of VANETs.

The work in [4], the authors proposed a modification to the cluster-directed acyclic into a cluster-directed acyclic graph(DAG) to improve the redundancy of topology at the MAC layer because that structure was followed by IEEE 802.14.2 which lead to network partitions even after single link or node failure.

In [5], a way for transmitting the sensed data from through a single path from sensors to root is proposed. Nevertheless, depending on the unreliability of wireless links and the constraints of sensor nodes, a single path is not an effective strategy to cope with the demands of the performance of different applications. Therefore, the authors suggest three kinds of multipath methods depending on RPL (Energy Load Balancing (ELB), Fast Local Repair (FLR), and their integration ELB-FLR.

In [6], the communication path is very important for RPL because it passes to the centre of the router that might give near optimal paths making no uniqueness for the application-driven extension to the proposed RPL. This enables the increase in the WSN lifetime limiting the functions of the net-work routing and forwarding, especially, the node that uses the similar applications.

In [8], a novel method named Co-RPL is proposed. The Corona scheme is used by this solution positioning the nodes according to the position of the DAG root to dis-cover the movement of these nodes. Nevertheless, the problem of mobility (e.g., MN disconnection) does not be solved in this solution.

The work in [16] introduced a new objective function to balance the number of overloaded children nodes to ensure the maximization of the node lifetime. The implementation of the mode (OF), they modified the form of DIO layout using new technology.

In [18], the authors extend the RPL from the mobility point of view. The presented schemes are analysed to observe the impact on the LLNS requirements.

The authors in [19] check the RPL performance in the density of the medium using the two objective functions in various to-apologies.

The research in [21] focused on the requirement for an intermediate layer between network and mac layers to get rid of the negative impact on the redundant paths numbers and their quality and overall performance of the routing protocol.

In [22], authors suggested a hybrid RPL routing approach based on power-saving cluster-parent named HECRPL. The main goal of this protocol is to perform simultaneously reliability and energy-saving.

The work in [23], they presented an enhanced version of RPL called enhanced-RBL to mitigate the problem of strong limitation of the preferred parent nodes. The node is allowed to distribute prefixes belonging to its sub-network among multiple parents.

In [26], authors proposed MRBL protocol to deal with mobility based on a proactive approach. In spite of this scheme presented a good contribution and succeeded to improve some needed performances, the enhancement is still needed.

The research in [27] displays a study of RPL with the latest updated version. For example, point to point RPL (P2P-RBL), assessment, performance, challenges, re-search defiance, and the RPL visualized opportunities.

The authors in [28] proposed Objective Function Based on Fuzzy logic (OF-FL). This is a new function that gets rid of the standard objective functions restriction which is developed for RPL through taking into account important nodes and links metrics like hop-counts, end- end delay, Link Quality Level (LQL), and Expected Transmission Count (ETX).

In [29], they proposed a new solution which aims to achieve distributed monitoring with minimal computational complexity. The main objective is to increase robustness in IoT via monitoring the links in the destination-oriented directed acyclic graph (DODAG) constructed by RPL.

In [31], Mayzaudet. al. suggests the use of risk management process as it is a theoretical concept, it can be used to solve multiple attacks but the problem with it can be the storage for codes for different techniques.

Airehrour et al. suggests various trust based model such as Bayesian Trust Model, Game Theoretic Trust Model, etc. can be used to solve the problem of security in RPL based on that we have, the trust-based solution proposed by Djedjig et al. in [32].

In [33], Pongle et al. suggested that lot more research required in IDS, so that IDS can be extended to solve multiple attacks. While, in [1] D. RPL comes with built-in security modes, which are not enough to mitigate all types of attacks. Tsaoet. al. [34], in RFC7416, proposed a security framework which analysed RPL's security. From this analysis, they came up with a set of security recommendations.

Security poses a serious challenge to RPL implementation.There are issues related to energy and link quality specified by LLNs [35]. LLNs require stable links maintenance and lower energy consumption beyond the common network circumstances and their limitation tends to have high impact on the effective design of security solutions. Especially in large scale networks, security should be well considered in order to avoid large scale contamination or information leakage.

Threats and attacks over RPL can lead to failures in authentication, maintenance of routing information and attacks on integrity or availability of the network operations [36]. Once an attacker captures a node, it is able to obtain the encrypted information and inject evil code to disturb the routing, which is quite difficult to be detected particularly when innocent nodes fail to know the attacks.

The attacks can lead to a non-optimal routing or even result in a worse situation such as routing loops or unreachable

neighbours. For example, when node 3 chooses node 6 as its preferred parent, which has a larger rank, a rank attack happens with a formed loop of 3-6-5. Routing choice attack happens when node 7 detaches node 5 and chooses node 2 as its parent node. As for neighbour attack, node 4 can replicate messages from node 2 and deceives node 8 to choose node 2 as its parent, which is totally out range for node 8. To solve the above issues, an Intrusion Detection System (IDS) that is capable of analysing activities or processesin a network or in a node is proposed. The IDS normallydeploys monitor nodes in finite state machine mode, every node in a network should be monitored under at least one of them. Such a method works well to efficiently detect rank attacks and local attacks [37].

Other IDS based methods, such as the one mainly focusing on the inner intrusion [38], can successfully solve routing choice attack by avoiding the optimal routing path failure caused by tampering options of DIOs. [39] Made a comprehensive analysis of rank attack, local repair attack, neighbour attack and DIS attack, and suggested that the handling models of the attacks can be developed through training of data. Besides the intrusion detection based methods, the encryption of information in RPL is another option.

Clark et al.[40] proposed a node-to-node encrypted authentication method by exchanging encryption key. Seeber et al. [41] deployed a Trust Platform Model (TPM), which is able to provide cryptographic operations and node authentication, to avoid evil routing information through related trust construction and key exchange mechanism.

Anti-attacks can be a challenging task for LLNs. ROLL WG analysed the security threats and attacks including authentication, access control, confidentiality, integrity and availability. Considering the different categories of threats and attacks, possible solutions have been offered, which mainly focus on establishing session keys, encapsulation during encryption and access control. It also points out that the sensor network limitations including energy, physical locations, directional traffic and etc., combining with use case requirements including urban networks, building automation, industrial automation and home automation, can be the new motivation to design more effective RPL in real scenarios.

III. CONCLUSION

The Internet of Things (IoT) will change the world and makes our environment completely monitored using smartly connected nodes. RPL Routing in IoTs networks has been extensively studied in the last years. This network is highly unreliable, prone to multi-hop interference, and to the quality of a time-varying link quality. Furthermore, the nodes are composed of limited memory, processing, power, and battery.. We have discussed the routing protocols for Low-Power and Lossy Networks. Several single paths and multipath routing protocols are reviewed. We have addressed the main challenges of RPL routing protocols in LLNs. In this survey, the focus is to study all possible issues in RPL, classify them and suggest countermeasures. This survey may help the researchers for the better understanding of RPL protocols, issues and possible solutions.

IV. REFERENCES

[1]. El Korbi, I., Ben Brahim, M., Adjihy, C. and Azouzm L., "Mobility Enhanced RPL for Wireless Sensor Networks", IEEE Third International Conference on the Network of the Future (NOF), Gammarth, Tunisie, 21-23 Nov., (2012).

[2]. Lee K.C., Sudhaakar R., Dai, L., Addepalli, S., and Gerla M., "RPL under mobility", In proc. of 2012 IEEE Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, USA, January, (2012).

[3]. Tian B., Hou K.M., Shi H., Liu X., Diao X., "Application of modied RPL under VANET-WSN communication architecture", Fifth (ICCIS), 2013 pp. 1467-1470. doi:10.1109/ICCIS, (2013).

[4]. Pavkovic, B., and et al. "Efficient topology construction for RPL over IEEE 802.15. 4 in wireless sensor networks." Ad Hoc Networks 15: 25-38, (2014).

[5]. Le, Q., Thu Ngo-Quynh, and Thomaz M.. "RPL-based multipath routing protocols for In-ternet of Things on wireless sensor networks." Advanced Technologies for Communica-tions (ATC), 2014 International Conference on. IEEE, (2014).

[6]. Marques, Bruno F., and Manuel P., "Improving the energy efficiency of WSN by using application-layer topologies to constrain RPL-defined routing trees." Ad Hoc networking workshop (MED-HOC-NET), 2014 13th annual Mediterranean. IEEE, (2014).

[7]. Jeong G. K. and Marcus C., "MoMoRo: Providing Mobility Support for Low-Power Wireless Applications", IEEE Systems Journal, Volume: PP , Issue: 99, ISSN : 1932-8184, pp 1-10, mars (2014).

[8]. Gaddour O., Koubaa A., and et al, "Co-RPL:RPL routing for mobile low power wireless sensor networks using corona mechanism", 9th IEEE International Symposium on Indus-trial Embedded Systems (SIES), pp.200-209, (2014).

[9]. Banh, M., et al., "Performance evaluation of multiple RPL routing tree instances for Inter-net of Things applications." Advanced Technologies for Communications (ATC), 2015 In-ternational Conference on. IEEE, (2015).

[10]. Djedjig, N., Djamel T., and Faiza M., "Trust-based RPL for the Internet of Things." Com-puters and Communication (ISCC), 2015 IEEE Symposium on. IEEE, (2015).

[11]. Iova, O., Fabrice T., and Thomas N. "Exploiting multiple parents in RPL to improve both the network lifetime and its stability." Communications (ICC), 2015 IEEE International Conference on. IEEE, (2015).

[12]. Zhao, M., Ivan Wang-HeiHo, and Peter H.. "An energy-efficient region-based RPL rout-ing protocol for low-power and lossy networks." IEEE Internet of Things Journal 3.6, pp. 1319-1333, (2016).

[13]. Emran A., Muneer B. Yassein, and Shadi A., "Routing protocol of low-power and lossy network: Survey and open issues." Engineering & MIS (ICEMIS), International Confer-ence on. IEEE, (2016).

[14]. Lassouaoui, Lilia, and et al. "Evaluation of energy aware routing metrics for RPL." Wire-less and Mobile Computing, Networking and Communications (WiMob), 2016 IEEE 12th International Conference on. IEEE, (2016).

[15]. Banh, Mai, et al. "Energy balancing RPL-based routing for Internet of Things." Commu-nications and Electronics (ICCE), 2016 IEEE Sixth International Conference on. IEEE, (2016).

[16]. Qasem, M., et al. "A new efficient objective function for routing in Internet of Things par-adigm." Standards for Communications and Networking (CSCN), 2016 IEEE Conference on. IEEE, (2016).

[17]. Jin, Y., et al. "Content centric routing in IoT networks and its integration in RPL." Com-puter Communications 89, pp.: 87-104, (2016).
[18]. Oliveira, A., and Teresa V., "Low-power and lossy networks under mobility: A survey." Computer Networks 107, pp.: 339-352, (2016).
[19]. Banh, M., et al. "Performance evaluation of multiple RPL routing tree instances for Inter-net of Things applications." Advanced Technologies for Communications (ATC), 2015 In-ternational Conference on. IEEE, (2015).
[20]. Iova, O., et al. "RPL: "The Routing Standard for the Internet of Things ... Or Is It?." IEEE Communications Magazine 54.12, pp.: 16-22, (2016).
[21]. Iova, O., et al. "The Love-Hate Relationship between IEEE 802.15. 4 and RPL." IEEE Communications Magazine 55.1, pp.:188-194, (2017).
[22]. Zhao, M., Peter H., and Henry C., "An energy-efficient and cluster-parent based RPL with power-level refinement for low-power and lossy networks." Computer Communications 104, pp.: 17-33, (2017).
[23]. Ghaleb, B., et al. "A new enhanced RPL based routing for Internet of Things." Communi-cations Workshops (ICC Workshops), 2017 IEEE International Conference on. IEEE, (2017).
[24]. Hyung-Sin K., et al. "Load balancing under heavy traffic in RPL routing protocol for low power and lossy networks." IEEE Transactions on Mobile Computing 16.4, pp.: 964-979, (2017).
[25]. Bouaziz, M., Abderrezak R., and Abdelfettah B., "EC-MRPL: An energy-efficient and mobility support routing protocol for Internet of Mobile Things." Consumer Communica-tions& Networking Conference (CCNC), 2017 14th IEEE Annual. IEEE, (2017).
[26]. H. Fotouhi, D. Moreira, M. Alves, "mRPL: Boosting mobility in the Internet of Things", ELSEVIER Journal of Ad Hoc Networks 26 pp 17-35, (2015).
[27]. Zhao, M., et al. "A comprehensive study of RPL and P2P-RPL routing protocols: Imple-mentation, challenges and opportunities." Peer-to-Peer Networking and Applications 10.5, pp.: 1232-1256, (2017).
[28]. Gaddour, O., Anis K., and Mohamed A., "Quality-of-service aware routing for static and mobile ipv6-based low-power and lossy sensor networks using RPL." Ad Hoc Networks 33, pp.: 233-256, (2015).
[29]. Mostafa, B., et al. "Distributed monitoring in 6LoWPAN based Internet of Things." Se-lected Topics in Mobile & Wireless Networking (MoWNeT), 2016 International Confer-ence on. IEEE, (2016).
[30]. Winter, T. "RPL: IPv6 routing protocol for low-power and lossy networks." (2012).
[31]. Mayzaud, Anthéa, RémiBadonnel, and Isabelle Chrisment. "A Taxonomy of Attacks in RPL-based Internet of Things." International Journal of Network Security 18.3 : 459-473, 2016.
[32]. Perrey, Heiner, et al. "TRAIL: topology authentication in RPL." arXiv preprint arXiv:1312.0984, 2013.
[33]. Pongle, Pavan, and GurunathChavan. "A survey: Attacks on RPL and 6LoWPAN in IoT." Pervasive Computing (ICPC), 2015 International Conference on. IEEE, 2015.
[34]. Tsao, T., et al. "A Security Threat Analysis for the Routing Protocol for Low-Power and Lossy Networks (RPLs)". No. RFC 7416, 2015.
[35]. A. Aijaz, H. Su, and A. H. Aghvami, "Corpl: A routing protocol for cognitive radio enabled ami networks," IEEE Trans. on Smart Grid, vol. 6, no. 1, pp. 477–485, 2014.
[36]. T. Tsao, R. Alexander, M. Dohler, V. Daza, A. Lozano, and M. Richardson, "A Security Threat Analysis for the Routing Protocol for Low-Power and Lossy Networks (RPLs)," RFC 7416, Accessed on Sep. 2017. [Online]. Available: https://rfc-editor.org/rfc/rfc7416.txt
[37]. A. Le, J. Loo, Y. Luo, and A. Lasebae, "Specification-based ids for securing rpl from topology attacks," in Proc. IFIP Wireless Days (WD), Niagara Falls, ON, Oct 2011, pp. 1–3.
[38]. L. Zhang, G. Feng, and S. Qin, "Intrusion detection system for rpl from routing choice intrusion," in Proc. IEEE Intl. Conf. on Communication Workshop (ICCW), London, June 2015, pp. 2652–2658.
[39]. A. Le, J. Loo, Y. Luo, and A. Lasebae, "The impacts of internal threats towards routing protocol for low power and lossy network performance," in Proc. IEEE Symposium on Computers and Communications (ISCC), Split, July 2013, pp. 000 789–000 794.
[40]. C. Taylor and T. Johnson, "Strong authentication countermeasures using dynamic keying for sinkhole and distance spoofing attacks in smart grid networks," in Proc. IEEE Wireless Communications and Networking Conference (WCNC), New Orleans, LA, March 2015, pp. 1835–1840.
[41]. S. Seeber, A. Sehgal, B. Stelte, G. D. Rodosek, and J. SchÃ¨unwÃd'lder, "Towards a trust computing architecture for rpl in cyber physical systems," in Proc. Intl. Conf. on Network and Service Management (CNSM 2013), Zurich, Oct 2013, pp. 134–137.
[42]. Lee K. C., Sudhaakar, J. Ning, Dai L., Addepalli S., Gerla M. "A Comprehensive Evalua-tion of RPL under Mobility", International Journal of Vehicular Technology, pp.300-304, (2012).
[43]. Tian, B., et al., "Application of modified RPL under VANET-WSN communication archi-tecture." Computational and Information Sciences (ICCIS), 2013 Fifth International Con-ference on. IEEE, (2013).
[44]. Idrees, A. K., Deschinkel, K., Salomon, M., & Couturier, R. Multiround Distributed Life-time Coverage Optimization protocol in wireless sensor networks. The Journal of Super-computing, 1-24, (2017).
[45]. Idrees, A. K., Deschinkel, K., Salomon, M., & Couturier, R. Perimeter-based coverage op-timization to improve lifetime in wireless sensor networks. Engineering Optimization, 48(11), 1951-1972 (2016).
[46]. Harb, H., Idrees, A. K., Jaber, A., Makhoul, A., Zahwe, O., &Taam, M. A. Wireless Sen-sor Networks: A Big Data Source in Internet of Things. International Journal of Sensors Wireless Communications and Control, 7(2), 93-109 (2017).
[47]. 55. Idrees, A. K., Deschinkel, K., Salomon, M., & Couturier, R. Distributed lifetime coverage optimization protocol in wireless sensor networks. The Journal of Supercomputing, 71(12), 4578-4593 (2015).
[48]. Idrees, A. K., Harb, H., Jaber, A., Zahwe, O., &Taam, M. A. Adaptive distributed ener-gy-saving data gathering technique for wireless sensor networks. In Wireless and Mobile Computing, Networking and Communications (WiMob), IEEE, pp. 55-62 (2017, October).
[49]. Idrees, A. K., & Al-Qurabat, A. K. M. Distributed Adaptive Data Collection Protocol for Improving Lifetime in Periodic Sensor Networks. IAENG International Journal of Com-puter Science, 44(3), (2017).
[50]. Adat, V., & Gupta, B. B.: Security in Internet of Things: issues, challenges, taxonomy, and architecture. Telecommunication Systems, 67(3), 423-441 (2018).