International Journal of Innovative Research in Engineering & Management (IJIREM)
ISSN: 2350-0557, Volume-9, Issue-5, October 2022
https://doi.org/10.55524/ijirem.2022.9.5.6
Article ID IJIR-1255, Pages 48-52
www.ijirem.org

A Survey for Secure Routing Protocol Used in Internet of Things (IoT)

Pranjal Maurya[1], Sangeeta Devi[2], Munish Saran[3], Rajan Kumar Yadav[4], and Upendra Nath Tripathi[5]

[1,2,3,4,]Research Scholar Department of Computer Science, DDU Gorakhpur University, Gorakhpur, Uttar Pradesh, India
[5]Associate Professor, Department of Computer Science, DDU Gorakhpur University, Gorakhpur, Uttar Pradesh, India

Correspondence should be addressed to Pranjal Maurya; pranjalmaurya1996@gmail.com

ABSTRACT- IoT devices are the integral part of this century. It is estimated that more than 40 billion devices are connected and this number is increasing exponentially due to the heavy dependency of IoT with every field. These devices collect their concerned data through their sensors and allow the business to work smoothly. The routing protocols used by these IoT devices play a vital role in delivery of collected data packets. Routing protocols governs several factors among which security as well as fast delivery are the major ones. Several researchers have proposed various routing protocols that can handle the secure as well as efficient source to destination route for the packets. But still due to various shortcomings in the area of security and fast delivery of packets there is need for better as well as more optimized routing protocol. Our paper aims to review some of the latest research paper published in this area so that the researchers can get to know about the latest work in this field and carry on with their research.

KEYWORDS- IoT, Routing protocols, Challenges, Security.

I. INTRODUCTION

In last few years, technological advancements have influenced the human lives because of wide-ranging use of smart application like E-Vehicles, Smart homes, E-Agriculture, Smart traffic control system, E-health, Smart cities, Smart automation etc. These smart applications are collection of smart devices, deployed wirelessly in an open environment and works over the internet. The successive raise of several technologies and wireless communication among the smart devices builds the concept of Internet of Things [1]. It is basically a network of physical devices termed as “Things” which is embedded with software, sensor and technology aimed as build interaction among objects and to make communication among these devices through network and standard protocols over the internet. Transmission between nodes should be efficient and fast. Quality of Service (QoS) becomes an integral part in making an effective communication and also ensures that the transmission of data between nodes are secure, reliable, congestion free, high delivery rate and requires minimum power consumption. These attributes can be achieve using optimal routing protocol in data transmission.

So the consideration of these quality measures becomes very essential and crucial in order to make an effective communication and fast data transmission so that the data packets are delivered securely to its destination.

Routing Protocol are used in order to find the best optimum path between source and destination for data transmission between nodes.

Mainly two basic functions are performed by the routing protocols—firstly, selecting the best route between networks, and other is transmitting data packets securely through selected path toward its intended destination. While routing protocols are designed, it becomes very important to take into consideration few quality constraints such as simplicity, security, reliability, minimum overhead, transmission delay, flexibility and throughput.

A good practice is to maintain a record for all possible paths and their associated conditions so that the most efficient route feasible data transmission can be explored.

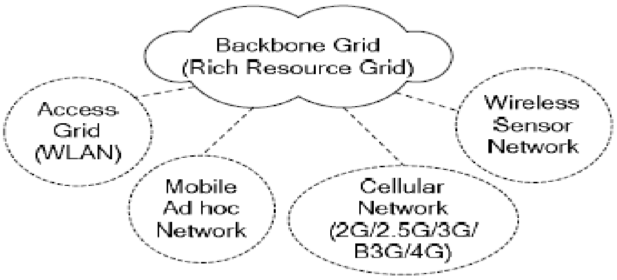

Figure 1: Pervasive wireless grid

Motivation for classifying Routing Protocol in IoTs (Challenges)

This section lists out various issues which ate to be considered while designing an efficient routing protocol for IoTs.

A. Security

In IoTs, Security is one of the biggest challenges for the communication of devices. Although it is believed, existing RPL protocol termed as Routing protocol for low power and lossy networks are secure and lightweight for IoT devices. Still there exits several networks attacks that affects the overall performance of the RPL protocol such as RANK, BLACKHOLE and SYBIL[8].

B. Scalability

Routing protocols vary with regard to their encouragement for scalability. Protocol which holds scalability configuration for this usually has computation more complex computations.. Hence, it becomes very important and critical to consider this aspect while making the selection of routing protocols [12].

C. Power

Extending the lifetime of network and energy preservation are the main issues in IoT. Therefore, the routing mechanism performs a vibrant job in data transmission, as an Internet of Things (IoT) device requisite to make the decision appropriately. In IoT, an inappropriate route selection is responsible for traffic overhead, energy depletion and data packets loss.

D. Transmission Time

End-to-end delay is a major issue for influencing the performance. The main liability of routing protocol is to transmit data to its destination in less time and using minimum energy. Network congestion gave raise to transmission delay and extensive energy consumption, but it can be controlled by using optimization [4].

II. RELATED WORK

Numerous routing protocols introduced for IoTs that main goal to grab different challenges as discussed in above section. Many article have appraised the routing protocol performance by using optimization techniques, though all these cannot be defined in same category as they differ in operational mechanism and also with the solution offered for the problem optimization.

A group of researcher Djedjig et.al introduced a RPL protocol which is based on Metric and Reliability Scheme, a cooperation-trust-based routing algorithm for RPL protocol used in IoT to provide security represents the MRTS performance is improved in case of nodes' rank changes, energy consumption, packet delivery ratio, and throughput. A study of a mathematical modelling demonstrations, MRTS fulfils the need of optimality, loop-freeness and consistency and that the designed trust-centered routing metric holds the required features for routing protocol as is tonicity and mono tonicity [4].

Author Kumar Rakesh and et.al proposed a Routing Infrastructure with high reliability for Green IoT Network in their research [7]. Author design routing protocol based on rendezvous- based routing protocol where rendezvous area is created with both a primary and alternative route is also designed and data transmission done via two method. First-data has been sent to nearest coordinating node until it reaches to the hub. In second method, the hub location is retrieved by source through connecting with the synchronizing devices and data packets are transmitted directly to the hub via the intermediary devices. Simulation result shows that the former technique overcomes the existing protocol is in constraints such as transmission delay as well as data delivery rate. The next approach consumes minimum energy as compared to that of existing protocol. Though, sensor devices are deployed randomly in remote areas, therefore IoT networks are susceptible to innumerable security threats which can undesirably change the overall performance of network. Hence it is necessary to have a secure and power-efficient, routing protocol which imposes minimum computing cost and less power consumption.

Another routing algorithm designed to provide more security against attacks in RPL routing protocols such as RANK, HOLES and SYBIL named as Fuzzy and Dynamic Routing Protocol based on trust for IoT by Hashemi et al in 2020 [8]. This scheme works on theory of trust as an umbrella, to address consequences of attacks covers countermeasures. Overall working of this protocol done in two steps. First, the trust's degree is computed individually in different dimensions using fuzzy methodology. The considered dimensions comprises contextual information, excellence of peer-to-peer communications and QoS.

Second, the total trust degree is computed by uniting faith in all aspects stand on the fuzzy method. The simulation results illustration, FDTM-RPL offers substantial enhancements with respect to mean of total parent changed, transmission delay and packet loss rate compared with existing standard protocols.

Author Enas Selem et.al designed a Temperature Heterogeneous Energy protocol for routing using concept of IoT applicable in E-Health field. This protocol is based on single-hop, multi-hopes and clustering, three selection criteria Coordinator node to fulfil the latency minimization requirement and parent node depend on residual energy ensures stability among all nodes' remaining power and extends network lifetime. THE protocol continues with maximum network throughput, improved network performance settings in field of long node lifetime [9].

In paper [10], an improved version of LOADng routing protocol, LOADng-IoT introduced, which is an efficient algorithm in terms of power consumption, QoS and reliability for mobile, sparse and dense networks. It don't need prior information of gateways so decreasing human interference offers self-adaption method for data transmission. It also poses a cache system that comprises internet routs, expediting the nodes to guide the route discovery to INs which are forwardly worked as gateways so that overall requisite control message overhead can be reduced in findings of Internet routes.

For IoT an energy efficient routing protocol based on composite metric introduced by Sennon Sankar et. al [13] named as LR-BDI (Load and Battery Discharge Index) in Iv6. Composite metric includes more the one metric node and satisfies the requirements of optimality, convergence and freeness from looping's. Building a route it take paths and nodes are traversed where Load and BDI are considered for every node of network. Results shows performance of RPL protocol is increased in terms of increment of network life time and decrement of packet loss rate.

In paper [14], a group of researcher introduces a routing algorithm for IoT device based on privacy and protection of source location. An impassable time-domain transmission is proposed to transfer actual data packets in order to increases adversary's backtracking time. Moreover, false data packets, spirit nodes, and an impassable ring are also applied to give a safeguard to the source location. Primarily, actual data packets are delivered expending impassable time-domain communication and after that it can be cached in the cluster heads on the basic ring. Next, false data packets are transmitted into impassable ring. Lastly, the initial node implements principal routing mechanism to transfer the actual data packet, those are stored on the sink node from basic ring [14]. This routing protocol rises the security without negotiating the life of network.

Another routing protocol proposed so as to decreasing the complexity of renewing the moveable sink's newest point named as Grid-Cycle Routing Protocol (GCRP).

Here, sensor area is subdivided into grid of cells and a grid cell head (GCH) is selected per cell and the sensor field is updated via mobile node nearly its newest location with less overhead, reduces the requirement of route re-modification and transfer the identified data with nominal delay[15].

A RPL routing protocol based on time and trust is designed with the aim of protecting IoT system against routing attacks. This Secure Trust scheme is imbedded in the RPL routing algorithm for securing adversary Sybiland Rank attacks. It is based on trust scheme for identifying and distinguish attacks though enhancing performance of network. On comparing Sec-Trust protocol to the existing RPL routing mechanism it is observed performance of *Sec Trust* protocol is superior than core RPL algorithm in the identification and distinguish of Sybil and Rank attacks [16].

Geographic-based multicast routing protocol requires more calculations to determine routes of transferring multicast data packets and designed multicast routes would be extensive if network has few void or holes and path may contains some loops. To avoid these problems Shiuan Pan et. al designed a Distributed Geographically distributed and light weighted Multicast Routing Protocol for IoT devices in their paper [17]. This protocol works in three steps - firstly, to reach its destination find the intermediate node then secondly, eliminates the loops and cuts the routes find in first step and finally checks selected multicast paths are future combined. Simulation result shows, new multicast routing path is shorter due to reduction in transmission nodes and decrease transmission delay.

Hua Yang and Zhiyong Liu in 2019 proposed an optimized routing protocol using neural network based on Dynamic Source Routing (DSR) for Flying Ad-hoc network named as Continuous Hopfield NN-DSR. This CHNN-DSR routing protocol increases FANET network and communication stability improving end-to-end transmission delay, packet delivery rate and throughput over the standard DSR routing protocol [18].

Baohua Shao introduced a wireless Particle Filter Routing – PaFiR with intelligent dimensions to encourage movable smart devices for the radio communication system because to fulfil the requirement to support services and application of IoTs, a lots of unexpected and imbalance data loads generated to the network.

With respect to traditional wireless networks, this protocol provides the divesting of traffic and empowers the IoT system to accept unmanned in-flight vehicles, therefore, also posing future revolution to flying network platforms. In simulation model with manageable rise in latency overhead, the delivery rate is improved by 40% [19].

A tabular summary of these papers used in literature reviews is given in Table: 1.

Table 1: Summarized Literature Review

Year	Author	Focused Area	Routing Mechanism	Result
2020	Djedjig et. al	Security	Metric-based RPL Trustworthiness Scheme	Proved a Secure and efficient routing mechanism with respect to throughput, data delivery rate, node's rank change and power consumption.
2019	Hashemi et. al	Security Attacks	Based on trust model using Dynamic, fuzzy and hierarchical model	During attack detection performance is high and expands overall network performance including transmission delay and data loss ratio.
2019	Enas Selem et. al	Network Performance	An energy aware routing mechanism based on Temperature Heterogeneity Energy (THE)	"THE" approved improvement in throughput 10% to 14% while power consumption decrease from 7% to 4%.
2019	José V. V. Sobral et. a l	Network performance	A Lightweight and On-request Ad hoc Distance-vector Routing algorithm	Proved an efficient routing algorithm as regards energy consumption, QoS and reliability for mobile, sparse and dense networks
2017	Sankar Sennan1 et. al	Energy Consumption	Battery discharge index (BDI) and load based combined Routing Protocol	Provide a better result such as lifetime of network, data delivery rate along with the routing metrics as total number of hop, RER, ETX (network load and BDI).

2018	Hao Wan et. al	Location Protection	A ring loop based routing method provide source location privacy and protection	The proposed protocol rises safety time without compromising network lifetime.
2018	Ayush Agrawala, et. al	Energy Consuption	A routing mechanism based on Grid-Cycle	The proposed scheme Overtakes existing work at several network sizes regarding to transmission time, data delivery rate, routing load, power consumption and network load.
2018	David Airehrour, et. al	Security	A trust-aware RPL routing algorithm based on time	This introduced method illustrates *Secure Trust-RPL protocol* sharing greater defence characteristics alongside Sybil and Rank attacks against the existing core RPL routing mechanism.
2016	Meng-Shiuan Pan et. al	Network Overhead	A geographically distributed and lightweight multicast routing mechanism	The proposed methodology can successfully shrink transmission network and reduce route distances in raised Multicast routes.
2019	Baohua Shao	Network Overhead	Intelligent abilities based on particle filter mechanism	More network scalability, acceptance and flexibility are offered by this particle filter routing mechanism. It provides up to 40% improved delivery rates with manageable increment in potential or overheads.

III. DISCUSSION AND CONCLUSION

Affluence of challenges with regard to information security, energy consumption, reliability, data transmission, throughput etc. within sensor nodes are recognized by many researchers in IoT. An efficient route discovery and packet addressing between sensor nodes in IoT are vital problem because of the necessity of designing integrated routing protocols for transferring data packets and communicating transversely various network topology from the source node to grasp the terminal node. There is possibility of executing their activities by Malicious node at the time of routing and data delivering, which is responsible for the occurrence of various types of attacks the in the transmitted information.

This paper highlighted the recent exploration of routing protocol used in IoTs, scenarios and research breaches in these routing mechanism aiming on security attacks, energy, transmission time, reliability and scalability. From the given study it can be concluded the research's either didn't offer perfect solutions for routing and forwarding or it has few deficiencies of security and performance requirements.

Hence, the main objective of this paper is to understand the challenges and the recent research for identifying the different domains of routing protocols such as security, energy, attacks, network overhead etc. with some deficiencies which need further more studies. Different routing algorithms facilitate valuable application of resources, E-devices, data routing and building flexible topologies.

REFERENCES

[1] Almusaylim, Z. A., Alhumam, A., &Jhanjhi, N. Z. (2020). Proposing a secure RPL based internet of things routing protocol: a review. Ad Hoc Networks, 101, 102096.

[2] Xin, H. M., & Yang, K. (2015, April). Routing protocols analysis for Internet of Things. In 2015 2nd International Conference on Information Science and Control Engineering (pp. 447-450). IEEE.

[3] Rathi, N., Saraswat, J., & Bhattacharya, P. P. (2012). A review on routing protocols for application in wireless sensor networks. arXiv preprint arXiv:1210.2940.

[4] Djedjig, N., Tandjaoui, D., Medjek, F., &Romdhani, I. (2020). Trust-aware and cooperative routing protocol for IoT security. Journal of Information Security and Applications, 52, 102467.

[5] Jaganathan, R., &Ramasamy, V. (2019). Performance modeling of bio-inspired routing protocols in Cognitive Radio Ad Hoc Network to reduce end-to-end delay. International Journal of Intelligent Engineering and Systems, 12(1), 221-231.

[6] Cheng, J., Cheng, J., Zhou, M., Liu, F., Gao, S., & Liu, C. (2015). Routing in internet of vehicles: A review. IEEE Transactions on Intelligent Transportation Systems, 16(5), 2339-2352.

[7] Lenka, R. K., Rath, A. K., & Sharma, S. (2019). Building reliable routing infrastructure for green IoT network. IEEE Access, 7, 129892-129909.

[8] Hashemi, S. Y., & Shams Aliee, F. (2020). Fuzzy, dynamic and trust based routing protocol for IoT. Journal of Network and Systems Management, 28(4), 1248-1278.

[9] Selem, E., Fatehy, M., Abd El-Kader, S. M., &Nassar, H. (2019). THE (temperature heterogeneity energy) aware routing protocol for IoT health application. IEEE Access, 7, 108957-108968.

[10] Sobral, J. V., Rodrigues, J. J., Rabêlo, R. A., Saleem, K., & Furtado, V. (2019). LOADng-IoT: An enhanced routing

protocol for internet of things applications over low power networks. Sensors, 19(1), 150.

[11] Conti, M., Kaliyar, P., Rabbani, M. M., &Ranise, S. (2020). Attestation-enabled secure and scalable routing protocol for IoT networks. Ad Hoc Networks, 98, 102054.

[12] Khalil, M., Khalid, A., Khan, F. U., &Shabbir, A. (2018, November). A review of routing protocol selection for wireless sensor networks in smart cities. In 2018 24th Asia-Pacific Conference on Communications (APCC) (pp. 610-615). IEEE.

[13] Sankar, S., & Srinivasan, P. (2017). Composite metric based energy efficient routing protocol for internet of things. International Journal of Intelligent Engineering and Systems, 10(5), 278-286.

[14] Wang, H., Han, G., Zhou, L., Ansere, J. A., & Zhang, W. (2019). A source location privacy protection scheme based on ring-loop routing for the IoT. Computer Networks, 148, 142-150.

[15] Agrawal, A., Singh, V., Jain, S., & Gupta, R. K. (2018). GCRP: Grid-cycle routing protocol for wireless sensor network with mobile sink. AEU-International Journal of Electronics and Communications, 94, 1-11.

[16] Airehrour, D., Gutierrez, J. A., & Ray, S. K. (2019). SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things. Future Generation Computer Systems, 93, 860-876.

[17] Pan, M. S., & Yang, S. W. (2017). A lightweight and distributed geographic multicast routing protocol for IoT applications. Computer Networks, 112, 95-107.

[18] Yang, H., & Liu, Z. (2019). An optimization routing protocol for FANETs. EURASIP Journal on Wireless Communications and Networking, 2019(1), 1-8.

[19] Shao, B., & Leeson, M. S. (2021). PaFiR: Particle Filter Routing–A predictive relaying scheme for UAV-assisted IoT communications in future innovated networks. Internet of Things, 14, 100077.

ABOUT THE AUTHORS

Pranjal Maurya received the Bachelor of Technology (B.Tech.) in Computer Science Engineering of Technology & Management and Master of Technology (M.Tech.) in Computer Science Engineering (CSE) from Madan Mohan Malaviya University of Technology. She is currently Ph.D. research Scholar in the Department of Computer Science, DDU Gorakhpur University. Her research interest includes WSN, Cloud Computing, IoT, Machine Learning and Deep Learning. She was previously working in Institute of Technology & Management as Assistant Professor for 1 years.

Sangeeta Devi received the Master of Computer Application (MCA) from IGNOU New Delhi and Master of Technology (M.Tech.) from AKTU Lucknow. She is currently Ph.D. research Scholar in the Department of Computer Science, DDU Gorakhpur University. Her research interest includes Data Science, WSN, IoT, Machine Learning and Deep Learning.

Munish Saran received the Bachelor of Technology (B.Tech.) in Computer Science Engineering (CSE) from Babu Banarasi Das National Institute of Technology & Management and Master of Technology (M.Tech. Gold Medal) in Computer Science Engineering (CSE) from Madan Mohan Malaviya University of Technology. He is currently Ph.D. research scholar in the Department of Computer Science, DDU Gorakhpur University. His research interest includes Cloud Computing, IoT, Machine Learning and Deep Learning. He was previously working in Infosys as senior system engineer for 4 years.

Rajan Kumar Yadav received the Bachelor of Science (B.Sc.) in computer Science from Deen Dayal Upadhyaya Gorakhpur University, Gorakhpur (Uttar Pradesh, India) and Master of Computer Application (MCA) from Madan Mohan Malaviya University of Technology. He is currently Ph.D. Research Scholar in the Department of Computer Science, DDU Gorakhpur University. His Research interest includes Cloud Computing, Machine Learning and IoT.

Dr. Upendra Nath Tripathi is currently Associate Professor in the Department of Computer Science, Deen Dayal Upadhyaya Gorakhpur University, Gorakhpur. He has 21 years of teaching and research experience. His areas of interests are Database, IoT, Machine Learning, Cloud Computing and Data Science.