Journal of Information Technology and Digital World (2021)
Vol. 03/ No. 02
Pages: 67-76
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2021.2.001

Metric Routing Protocol for Detecting Untrustworthy Nodes for Packet Transmission

Dr. S. Smys,
Professor, Department of Computer Science and Engineering,
RVS Technical Campus,
Coimbatore, India.
smys375@gmail.com

Mr. C. Vijesh Joe,
Assistant Professor, Department of Computer Science and Engineering,
VV College of Engineering,
Tirunelveli, India.
vijesh.joe@gmail.com

Abstract: IoT objects that have a resource constrained nature resulting in a number of attacks in the routing protocol for lossy networks and low-power networks. RPL is very vulnerable to selfish behaviours and internal attacks though they are built with encryption protection to secure messages. To address this vulnerability, in this paper, we propose a novel trustworthiness methodology based on metric for incorporating trust evaluation, enhancing the robustness of security mechanism. Simulation results indicate that the proposed work is efficient in terms of throughput, nodes' rank changes, energy consumption and packet delivery ratio. Moreover, using mathematical modelling, it has been observed that this methodology meets the demands of loop-freeness, optimality and consistency. This shows that this metic has both monotonicity and isotonicity requirements to enable the routing protocol. Incorporating the concepts of game theory, we can use this technique as a strategy to iterate Prisoner's Dilemma. Both evolutionary simulation and mathematical analysis indicate that the proposed metric-based routing protocol is an efficient technique in promoting evolution and stability of the IoT network.

Keywords: Cooperation enforcement; Game Theory; Trust Management; Internet of Things; Secure Routing; RPL

ISSN: 2582-418X
Submitted: 21.03.2021
Revised: 15.04.2021
Accepted: 4.05.2021
Published: 25.05.2021

Journal of Information Technology and Digital World (2021)
Vol. 03/ No. 02
Pages: 67-76
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2021.2.001

1. Introduction

The introduction of Internet of Things (IoT) is a novel communication technique that has an impact on the everyday lifestyle of the people in terms of industrial, urban application, automobiles, building and home automation and healthcare. The IoT based networks are built using Lossy and Low Power networks that are built with a number of wireless devices like actuators, sensors, RFID tags etc. Both communication and computing systems are embedded in this system in a seamless manner [1]. The IoT objects are categorized based on their lossy communication links and strong resource constraints. However, these objects have constraints such as short communication ranges, limited frame size, low throughput, high loss rate, energy supply, memory and processing power. However, these restrictions lead to a number of challenges in academic research and industry community such as security, routing and scalability [2]. In the past few years, a number of routing solutions have been suggested for LLNs. A standardised routing protocol has been recommended by the Internet Engineering Task Force, for Lossy and low power networks. However, the security of the routing protocol is considered to be a crucial part and will serve to be a critical domain for understanding. RPL [3] is vulnerable to many internal threats from known as well as new sources. However, it ensures the confidentiality and integrity of messages that are defined with mechanisms based on cryptography [4], against outsider attacks.

In this paper, we have focused on addressing the issues of RPL with respect to routing security, using a Metric-based trustworthiness methodology that is used to secure the transmission of data between the nodes. This methodology is used to calculate and pick the path that can be trusted the most from the source to the destination, on avoiding the malicious nodes, in a secure manner [5]. In this paper, mathematical analysis and simulation validation is carried out taking into consideration the collaboration and cooperation of trust relationships between the nodes to enhance the network's security. In [6], the authors used cooperation since it can be possible to determine the behaviour of another party making this means of trust a more reliable one. In this algorithm, the nodes are demanded to cooperate with the routing algorithm in order to improve the ability to detect untrusted nodes. To establish this concept, punishment mechanism (by isolating untrusted nodes) is used as a means to encourage cooperation among the nodes [7]. Hence using cooperation enforcement, we

ISSN: 2582-418X
Submitted: 21.03.2021
Revised: 15.04.2021
Accepted: 4.05.2021
Published: 25.05.2021

Journal of Information Technology and Digital World (2021)
Vol. 03/ No. 02
Pages: 67-76
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2021.2.001

emphasis that the proposed work is comparatively as efficient as other strategies such as spiteful and tit-for-tat strategy.

2. Related Work

A number of methodologies presented over the years have proposed the used of Intrusion Detection System to isolate and detect RPL attacks. In [8], a novel IDS methodology was introduced with the goal of Selective-Forwarding, sinkhole and targets rank attacks. However, this methodology shows a number of disadvantages like lack of synchronisation and high false detection rate. To overcome these methodologies, authors in [9] have introduced a wormhole attack detector using IDS anomaly. In this method, they have used a neighbour verification/ discovery based. Here, information about the neighbours are gathered from the node and are further sent to the base reception unit. They make use of the data obtained to determine the intruders and arrive at a conclusive decision. To secure RPL against neighbouring attacks, sinkholes and ranks, a hybrid methodology is used by [10]. Here the information is monitored using the nodes to identify the attacks. Information on states and transitions were used in Extended Finite State Machine. Similarly, to detect wormhole attacks, sinkhole and hello-flood, a compression header analyser based IDS is proposed by authors in [11]. Here correlation-based features, greedy stepwise and Best first search algorithm are used for features selection and detection. However, this methodology was too long to be compatible for usage. Deep learning and machine learning methodologies that are used by the IoT system demand for a lot in terms of storage and computation. In the recent years, a number of research works are used to tackle the issue of trust management for various IoT networks. Authors in [12] and [13] are known as the inventors of distributed IoT Trust Management. In this proposed work calculation of trust level is done by the nodes using metrics like reliability, community-interest, cooperativeness and honesty, on indirect and direct recommendations [14].

ISSN: 2582-418X
Submitted: 21.03.2021
Revised: 15.04.2021
Accepted: 4.05.2021
Published: 25.05.2021

Journal of Information Technology and Digital World (2021)
Vol. 03/ No. 02
Pages: 67-76
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2021.2.001

3. Proposed Methodology

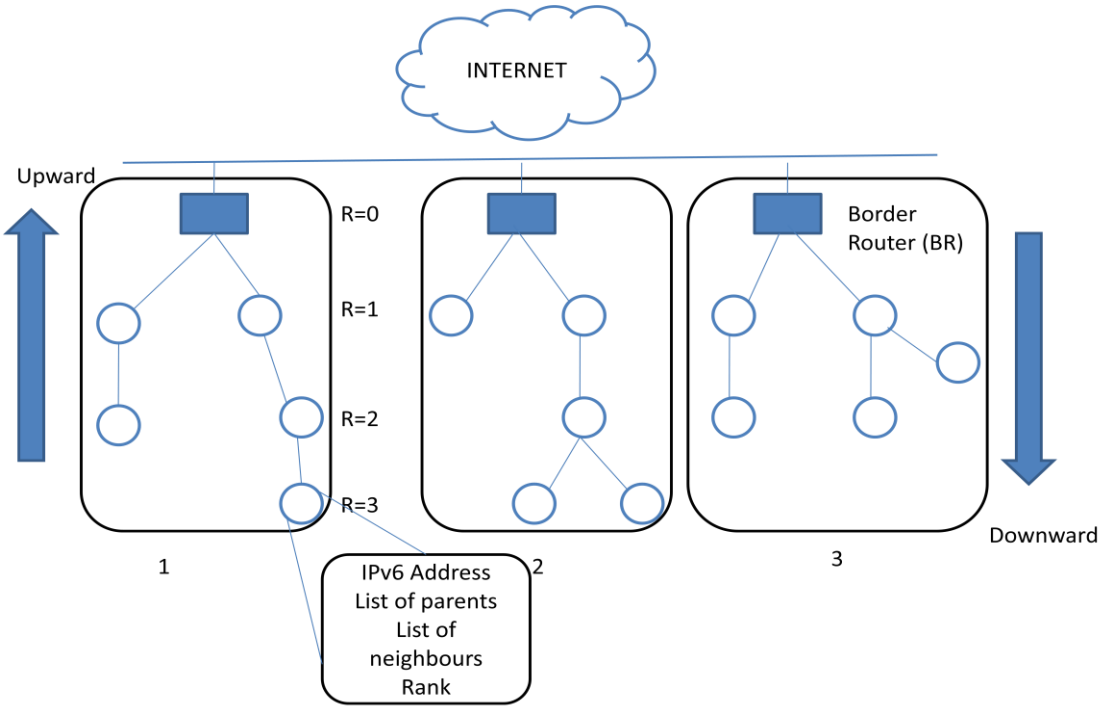

Fig.1. RPL Technology Implemented

The RPL mechanism using trust mechanism is proposed in this paper (Fig.1.) where the trust worthiness of the neighbouring nodes are calculated and analyzed based on the indirect recommendations of the neighbours as well as through direct observation. The issue with this method is that it is dependent on node metrics like selfishness, honesty and energy in order to determine the optimal path to travel. If these nodes are not selfish, but honest, the parent node can be identified using energy metric. Hence, more amount of energy will be consumed by the trusted paths selected which will lead to an imbalance in the consumed energy. Moreover, link metrics have a crucial role to play to assess the reliability of a particular path which in turn will affect the high delivery ratio. Figure 2 shows the integration of ERNT with the proposed work resulting in DIO messages. There are four major parameters that are used to evaluate the trustworthiness of a node namely energy, ETX, honesty and selfishness. This work is adjustable and flexible by removing or adding components that are related to particular IOT applications.

ISSN: 2582-418X
Submitted: 21.03.2021
Revised: 15.04.2021
Accepted: 4.05.2021
Published: 25.05.2021

Journal of Information Technology and Digital World (2021)
Vol. 03/ No. 02
Pages: 67-76
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2021.2.001

3.1. Energy

Energy is a part of QoS trust component. It indicates the measure of of energy expected by the node 'a' from the node 'b' in order to achieve specific goals. Similarly the remaining energy percentage is indicative of the energy trust between the nodes. In general energy is consumed in IoT during the process of sending and receiving data. This energy can be calculated using various energy models. In this paper, the energy used by a particular node 'a' to send information of length 'l' to another node 'b' can be determined using the following expression:

$$E_a^t = l \times (E_{disp} \times d^2 + E_{elec})$$

Where d represents the communication range, E_{elec} is the electronics energy and E_{disp} represents the amount of energy dissipated. On the other hand, the energy consumed by the node 'b' which is receiving the information can be calculated using the following equation:

$$E_a^{tr} = l \times E_{elec}$$

When t=0, the maximum energy is equal to the receive energy. This can also be represented as:

$$ER_a(0) = E_{max}$$

Hence the total amount of energy that is used by a particular node is the summation of energy consumed while receiving the message and when sending the message. Accordingly, the energy remaining can be calculated such that:

$$ER_a^t = ER_a(t - \Delta t) - E_a^{tr}(t) - E_a^{rx}(t)$$

ISSN: 2582-418X
Submitted: 21.03.2021
Revised: 15.04.2021
Accepted: 4.05.2021
Published: 25.05.2021

Journal of Information Technology and Digital World (2021)
Vol. 03/ No. 02
Pages: 67-76
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2021.2.001

3.2. Selfishness

A node that tends to use the resources of other nodes while using only a limited amount of its own resources is known as a selfish node. A selfish node 'b' can be identified by another node 'a' on evaluation over a specific period of time 'P' by means of methodologies such as snooping and overhearing. Consider an application that will need energy of E_{min}. A node is said to be selfish if it satisfies the condition $ER_a^t < E_{min}$. When calculating trust, the metrics approach allows a specific level of selfishness in order to ensure safety of the resources of that node. Hence a trade-off is established between the selfishness and energy of the nodes.

$$T_{ab}^{selfish} = \begin{cases} 0 & if\ N(t) \geq T_{selfish} \\ 1 - \dfrac{N(t)}{T_{selfish}} & otherwise \end{cases}$$

3.3. Honesty

Identification of a malicious node is possible using the honesty parameter. The node 'b' is evaluated by node 'a' to determine if it has been affected. To determine this intrusion, a number of detection systems are used to identify the node. In this work, every node 'a' implements an intrusion detection system to detect and monitor malicious behavior.

$$T_{ab}^{Honesty,new}(t) = \begin{cases} 0, & if\ node\ b\ misbehaves \\ 1, & else \end{cases}$$

4. Results and Discussion

Simulation of the proposed work is done using 2.7/Cooja simulator which is an open source. We have used a BR that uses 30 nodes via simulation and 29 sender nodes are also located in a random manner. Every sender node is built with 48kBytes of flash memory and 10kBytes of RAM. Of the 29 nodes, 3 are built to be attackers that lead to Black hole or Rank attacks.

ISSN: 2582-418X
Submitted: 21.03.2021
Revised: 15.04.2021
Accepted: 4.05.2021
Published: 25.05.2021

Journal of Information Technology and Digital World (2021)
Vol. 03/ No. 02
Pages: 67-76
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2021.2.001

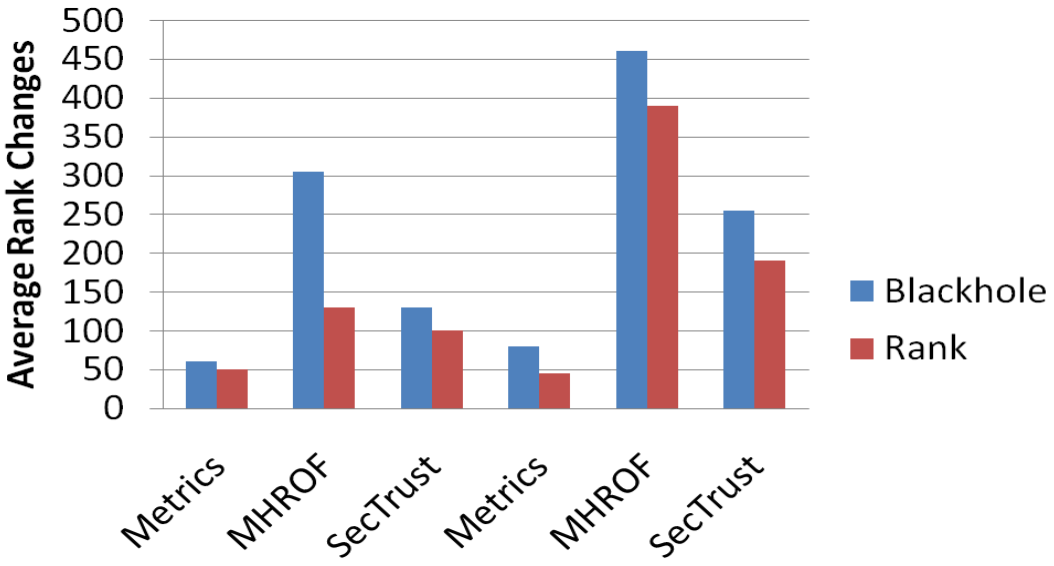

Fig.2. Comparison of nodes with respect to average rank changes in Black Hole and Rank

Fig.2. shows the changes in average rank for SecTrust, MRHOF-RPL and Metrics based on the attack by blackhole and rank.

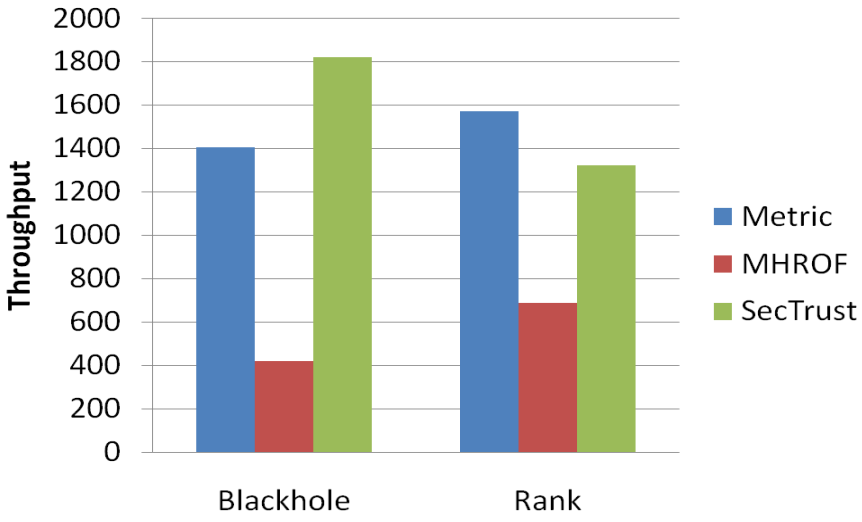

Fig.3. Comparison of nodes with respect to Thoughput in Black Hole and Rank

ISSN: 2582-418X
Submitted: 21.03.2021
Revised: 15.04.2021
Accepted: 4.05.2021
Published: 25.05.2021

Journal of Information Technology and Digital World (2021)
Vol. 03/ No. 02
Pages: 67-76
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2021.2.001

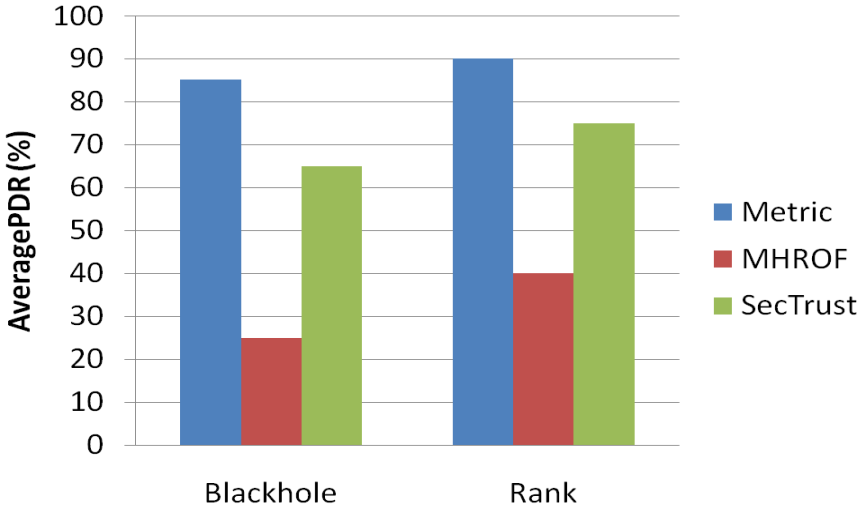

Fig.4. Comparison of nodes with respect to Average PDR in Black Hole and Rank

Fig.3 and Fig.4 shows a comparative study on three methodologies- Metric, MHROF and SecTrust with respect to Throughput and Average PDR.

5. Conclusion

In this proposed work, we have used a Metrics routing protocol where the node with higher trust value is chosen with every hop by the child node. Using simulation, we demonstrate that the proposed Metrics Methodology not only improves packet delivery ratio but also contributes significantly to decrease the amount of energy consumed by the system. Moreover, the use of metrics can be converted into strategy in game theory techniques. The nodes that are found to be uncooperative are punished or isolated and will also enhance the security of the network. Future work of metrics involves evaluation of the performance that can be incorporated in large scale networks

References

[1] Machado, K., Rosário, D., Cerqueira, E., Loureiro, A. A., Neto, A., & De Souza, J. N. (2013). A routing protocol based on energy and link quality for internet of things applications. *sensors*, *13*(2), 1942-1964.

ISSN: 2582-418X
Submitted: 21.03.2021
Revised: 15.04.2021
Accepted: 4.05.2021
Published: 25.05.2021

[2] Behera, T. M., Mohapatra, S. K., Samal, U. C., Khan, M. S., Daneshmand, M., & Gandomi, A. H. (2019). I-SEP: An improved routing protocol for heterogeneous WSN for IoT-based environmental monitoring. *IEEE Internet of Things Journal*, *7*(1), 710-717.

[3] Chze, P. L. R., & Leong, K. S. (2014, March). A secure multi-hop routing for IoT communication. In *2014 IEEE World forum on internet of things (WF-iot)* (pp. 428-432). IEEE.

[4] Vaiyapuri, T., Parvathy, V. S., Manikandan, V., Krishnaraj, N., Gupta, D., & Shankar, K. (2021). A Novel Hybrid Optimization for Cluster-Based Routing Protocol in Information-Centric Wireless Sensor Networks for IoT Based Mobile Edge Computing. *Wireless Personal Communications*, 1-24.

[5] Zhu, M., Chang, L., Wang, N., & You, I. (2020). A smart collaborative routing protocol for delay sensitive applications in industrial IoT. *IEEE Access*, *8*, 20413-20427.

[6] Kavitha, V. (2021). Privacy preserving using multi-hop dynamic clustering routing protocol and elliptic curve cryptosystem for WSN in IoT environment. *Peer-to-Peer Networking and Applications*, *14*(2), 821-836.

[7] Senthilkumar, M., Kavitha, V. R., Kumar, M. S., Raj, P. A. C., & Shirley, D. R. A. (2021, March). Routing in a Wireless Sensor Network using a Hybrid Algorithm to Improve the Lifetime of the Nodes. In *IOP Conference Series: Materials Science and Engineering* (Vol. 1084, No. 1, p. 012051). IOP Publishing.

[8] Serhani, A., Naja, N., & Jamali, A. (2020). AQ-Routing: mobility-, stability-aware adaptive routing protocol for data routing in MANET–IoT systems. *Cluster Computing*, *23*(1), 13-27.

[9] Sankar, S., Srinivasan, P., Luhach, A. K., Somula, R., & Chilamkurti, N. (2020). Energy-aware grid-based data aggregation scheme in routing protocol for agricultural internet of things. *Sustainable Computing: Informatics and Systems*, *28*, 100422.

[10] Hameed, A. R., ul Islam, S., Raza, M., & Khattak, H. A. (2020). Towards energy and performance aware geographic routing for IoT enabled sensor networks. *Computers & Electrical Engineering*, *85*, 106643.

[11] Sugave, S., & Jagdale, B. (2020). Monarch-EWA: Monarch-Earthworm-Based Secure Routing Protocol in IoT. *The Computer Journal*, *63*(6), 817-831.

ISSN: 2582-418X
Submitted: 21.03.2021
Revised: 15.04.2021
Accepted: 4.05.2021
Published: 25.05.2021

Journal of Information Technology and Digital World (2021)
Vol. 03/ No. 02
Pages: 67-76
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2021.2.001

[12] Bhalaji, N. (2020). A Novel Hybrid Routing Algorithm with Two Fish Approach in Wireless Sensor Networks. *Journal of trends in Computer Science and Smart technology (TCSST)*, *2*(03), 134-140.

[13] Shakya, S., & Pulchowk, L. N. (2020). The Robust Routing Protocol with Authentication for Wireless Adhoc Networks. *Journal of ISMAC*, *2*(02), 83-95.

[14] Shakya, S., & Pulchowk, L. N. (2020). The Robust Routing Protocol with Authentication for Wireless Adhoc Networks. *Journal of ISMAC*, *2*(02), 83-95.

ISSN: 2582-418X
Submitted: 21.03.2021
Revised: 15.04.2021
Accepted: 4.05.2021
Published: 25.05.2021