iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** III **Month of publication:** March 2025

DOI: https://doi.org/10.22214/ijraset.2025.67961

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue III Mar 2025- Available at www.ijraset.com

A Groundbreaking Approach to Counter Blackhole Attacks in RPL

Abhishek C.V[1], Dr. Sudheer Marar[2]
[1]*MCA Scholar,* [2]*HOD, Department of MCA, Nehru College of Engineering and Research Centre, Pambady*

Abstract: ***By connecting our physical environment to computer-based systems, the Internet of Things (IoT) decreases human intervention and boosts productivity across a range of sectors, including manufacturing, smart cities, agriculture, automotive, and healthcare. Fitness tracking devices, Bluetooth, and near-field communications (NFC) are changing the Internet of Things environment and affecting many different types of enterprises. However, there are significant privacy hazards associated with the network of IoT devices, which emphasizes the need for reliable network security solutions and legal and secure data packet routing techniques. Additionally, IoT networks are susceptible to both internal and external attacks due to resource constraints, necessitating a careful review of safety assurance measures and enhancement of trust mechanisms, like the Routing Protocol for Low Power and Lossy Networks (RPL), to protect against blackhole intrusion while maintaining the functioning of the protocol. This research presents an enhanced mechanism for that using the Refined Optimal Trust Factor (ROTF) algorithm.***
Keywords: Internet of Things (IoT), Network Security, Routing Protocol for Low Power and Lossy Networks (RPL), Refined Optimal Trust Factor (ROTF)

I. INTRODUCTION

Through the use of the Internet of Things, our physical world is being incorporated into systems based on computers, making objects more logical and remotely controlled over existing networks. It reduces the need for human involvement while increasing efficiency.

The improvement of IoT is related to some industries, including manufacturing, smart cities, farming, healthcare, and the automotive sector. Products from the Internet of Things, such as fitness trackers, Bluetooth, Near Field Communications, and other gadgets in household appliances, have changed the world. This will alter how IoT ecosystems are constructed. IoT-connected devices pose a significant privacy risk, underscoring the necessity of a reliable technique for safely transferring data packets throughout the network. It makes the need for a trustworthy network security solution even more pressing. Due to a lack of resources like power for processing, energy, etc.

IoT networks are susceptible to attacks from the inside as well as the outside [4]. As a result, they have carried out a comprehensive analysis of the most common security techniques and how they affect widely used protocols and standards such as IEEE 802.15.4, 6LoWPAN, B-MAC, RPL, CTP, and BCP. There has been a discussion of the current defenses and possible security threats. The authors of [5] discuss upholding and managing trust to offer reliable data transfer, privacy, and enhanced information security. The goal of this work is to strengthen the current trust mechanism for the Routing Protocol for Low Power and Lossy Networks (RPL) of the Internet of Things, which is vulnerable to blackhole attacks [1]. Furthermore, the existing trust-based method must be sufficiently straightforward to avoid interfering with the operation of the protocol.

II. LITERATURE SURVEY

A study by N Bhalaji et al. in [1] tackles a serious security risk: the blackhole attack in the Internet of Things (IoT) networks that employ RPL for network layer data packet routing. According to recent studies, manufacturers do not prioritize security enough, which leaves them open to possible assaults. This is resolved by combining the RPL protocol with a trust-based technique that lessens the harm caused by black holes. The efficiency of the suggested strategy in strengthening security against blackhole attacks is demonstrated by experimental analysis carried out using the Cooja Network simulator on Contiki OS.

In contrast to both ad hoc and traditional wired networks, the study by JP Vasseur et al. [2] suggests novel routing metrics and limitations specifically designed for Low-Power and Lossy Networks (LLNs). This paper outlines a set of link and node routing constraints and metrics suitable for LLN, as opposed to common Interior Gateway Protocol (IGP) metrics like link metrics or hop counts. These are intended to be utilized by the Routing Protocol for Low-Power and Lossy Networks (RPL).

Ericsson et al. (2013)[3] predict that over 50 billion interconnected devices will transform daily life by offering features like interactive navigation, healthcare, and connected wallets. This will improve safety, sustainability, and access to services. Operators are preparing to offer customized connectivity bundles, as data usage is expected to surge with the rise of M2M interactions and new services. I. Tomic et al. (2014) investigate security issues in communication protocols for Wireless Sensor Networks (WSNs), focusing on IEEE 802.15.4 and RPL. They analyze network layer attacks, assess their impact on performance using the Cooja simulator, and suggest new research opportunities to enhance WSN security[4].

Zheng Yan et al.'s paper [5] outlines goals for trust management and suggests an examination of the aspects of trust in the Internet of Things (IoT). It surveys the body of research on reliable IoT developments, points out open problems, outlines research obstacles, and projects future developments. It also presents a research paradigm that focuses on context-aware services, dependable data fusion, and enhanced user security and privacy to manage trust holistically inside the IoT ecosystem.

In [6] K. Kabilan et al., three mobility models (Manhattan Grid, Gaussian Markov, and Random Waypoint) are tested in order to assess RPL performance in IoT networks using the Cooja simulator. It concludes that the Manhattan Grid model preserves RPL's functionality while offering the optimum performance.

Because of their exposure to the untrusted Internet, resource limitations, and new IoT technologies, 6LoWPANs connected to IPv6/RPL are subject to security concerns that are examined in [7] by Linus Wallgren, Shahid Raza, et al. It contains an examination of possible attacks as well as the Cooja simulator's demonstration of routing attacks on RPL in Contiki OS. It also demonstrates the use of new IPv6 security capabilities for intrusion detection, as demonstrated by a lightweight heartbeat protocol.

To improve communication security within an RPL network, Sebastian Seeber et al.'s paper [8] suggests utilizing the security characteristics of a Trusted Platform Module (TPM). The Low-power and Lossy Networks (LLNs) protocol RPL, developed by the IETF, is useful for Cyber-Physical Systems (CPSs), which are frequently made up of devices with limited resources. RPL enables secrecy and message integrity, but it ignores issues like key management and signatures. This method allows for strong security features in RPL implementations without sacrificing complexity or space limitations by using TPM to outsource security duties.

III. METHODOLOGY

This study proposes an enhancement to the trust-based IPv6 Routing Protocol (RPL) architecture to prevent blackhole attacks in IoT networks. Blackhole attacks are particularly harmful because they can drain resources, lead to significant packet overhead, and cause substantial packet loss. These attacks destabilize the network by inducing rank changes, resulting in excessive packet delays and disrupting the network topology. When a rank change occurs, the ranks must be recalculated, triggering a local repair process, which then initiates a global repair from the root node. This frequent maintenance can severely impact the network's overall effectiveness and stability. The study highlights that traditional cryptographic techniques, validation, and verification methods are not effective in preventing security breaches in RPL, leaving billions of IoT devices worldwide vulnerable to attacks. Furthermore, these security solutions often prioritize energy efficiency and weight reduction, making them unsuitable for networks with nodes that have limited resources. As a result, the study emphasizes the need for more effective security solutions tailored to the specific constraints and requirements of IoT devices, particularly those with limited processing power and energy resources.

A. Low Power and Lossy Network Routing Protocol (RPL)

The Internet Engineering Task Force (IETF) established this RPL for IPv6 in the Internet of Things. A tree-like structure called the Destination Oriented Directed Acyclic Graph (DODAG) is made up of the paths that the RPL network takes when it first starts. Every RPL network node performs a parent selection process that considers specific parameters in order to choose a path [7]. To make it easier for packets to reach their destination, the selected parent then acts as a conduit for packet forwarding from and to the kid nodes.

B. The Security Mechanism of RPL

The RPL protocol is susceptible to many types of routing attacks [7]. Among its most notable examples are selective forwarding attacks, wormhole attacks, rank attacks, denial of service attacks, and black hole attacks. The Trusted Platform Module (TPM) technique, introduced by the creators of [8], ensures message integrity and authenticity in an environment that is vulnerable to attacks by providing unaltered data. Selective forwarding, sinkhole, and black hole attacks are addressed by the Intrusion Detection System proposed in [9], which necessitates the cautious deployment of IDS nodes. This may not be possible, though, if IoT devices are scattered at random, rendering any attempts to prevent routing attacks pointless. Furthermore, [10–12] offers defenses against black hole and sinkhole attacks, among others.

C. *Trust Factor in Algorithm*

The performance of the wireless sensor network must be tested and studied to determine the appropriate value for the trust factor in the trust calculation function. The trust factor should be based on the network's specific needs and characteristics. There are several steps to calculate the trust factor:

1) Understand the behavior of networks: Analyze the behavior of the wireless sensor network. Think about communication dependability, packet delivery patterns, and how quickly confidence should change in reaction to current events.
2) Trust Sensitivity: Establish the appropriate level of sensitivity for the trust calculation to variations in the packet delivery ratio. While a lesser value lessens the trust calculation's responsiveness to market fluctuations, a bigger trust factor makes it more sensitive.
3) Iterative Changes: By progressively altering the trust component and monitoring the impact on the trust metric. Change the network gradually while keeping an eye on how it responds. Iterate further until you find a value that aligns with the desired dynamics of trust.
4) Pay attention to network dynamics: Take into account how the network functions. For instance, a higher level of trust would be necessary in a rapidly evolving setting to react quickly to variations in the caliber of communication.
5) Sensitivity and Equilibrium Stability: Strive for a balance between sensitivity and stability. While an extremely stable computation may take longer to adjust to changing network conditions, an overly sensitive trust calculation may produce unforeseen and frequent changes.
6) Experimentation and confirmation: Conduct extensive testing in a variety of scenarios to ensure the chosen trust factor is dependable. Utilize historical data, simulate different network conditions, and verify that the trust computation works as expected.
7) Repeating based on results: Adjust the trust factor as necessary, accounting for ongoing observations and any changes to the network's characteristics. As the network evolves, the optimal trust factor might need to be modified. The optimal trust factor will be determined by the specifics of the wireless sensor network. Adjust this value to the needs of the application and the network's behavior this study, the trust factor is a number between 0 and 10.

D. *Finding the Best Trust Factor using the ROTF Algorithm*

The function "findOptimalTrustFactor" is defined; it takes three parameters—reply, sent, and targetTrust—and returns the optimal trust factor. BestDifference is set to INFINITY at startup, while BestTrustFactor is set to 0. The iteration has a step size of 0.1 and covers a range of trust factor values, inclusive, from 0 to 10. A trustValue is calculated for every trustFactor using the TrustCalculate function. The precise difference between the calculated trust value and the target trust is calculated. If the difference is less due to the current trust factor, bestTrustFactor and bestDifference are updated. The ROTF algorithm ultimately returns the bestTrustFactor.

IV. RESULTS AND ANALYSIS

To create a trust-based framework for RPL, the simulation is conducted on the Instant Contiki 3.0 platform [13, 14]. The simulation's parameter configuration is displayed in Fig. 2. A network with a transmission range of 40–50 m and an interference range of 90–100 m was built using type Z1 (Cooja simulator) motes. The protocol has already been simulated at the DODAG level of the network using an appropriate topology configuration. A DODAG network was created with one server mode and a few client modes. Because some of the clients are evil motes—that is, they refuse to accept data packets from other clients—a non-cooperation assault occurs. To identify malicious motes, the trust value is calculated by considering the quantity of packets sent and received. The UDP server (green), UDP clients (yellow), and harm client (purple) are depicted in Fig 1. Every message sent by its neighbors is abandoned by the attacker motes.

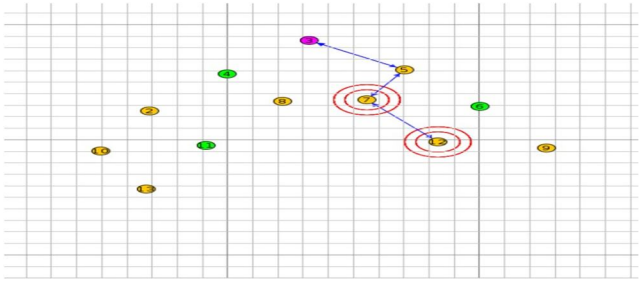


Fig 1

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue III Mar 2025- Available at www.ijraset.com

Simulation Parameters	
Simulation tool	Coniki/Cooja 3.0
Mote type	Z1-Mote
Run time	5400 seconds
Interference range	100 m
Transmission range	50m
Network protocol	IP Based
Routing protocol	RPL
Transport Layer protocol	UDP

	With in-DODAG LevelTrust
Total number of motes	*12*
Root node (sink)	*1 (Mote ID-3)*
Attacker clients motes	*3(Mote ID-4,6,11)*
Genuine client motes	*8*

Fig 2

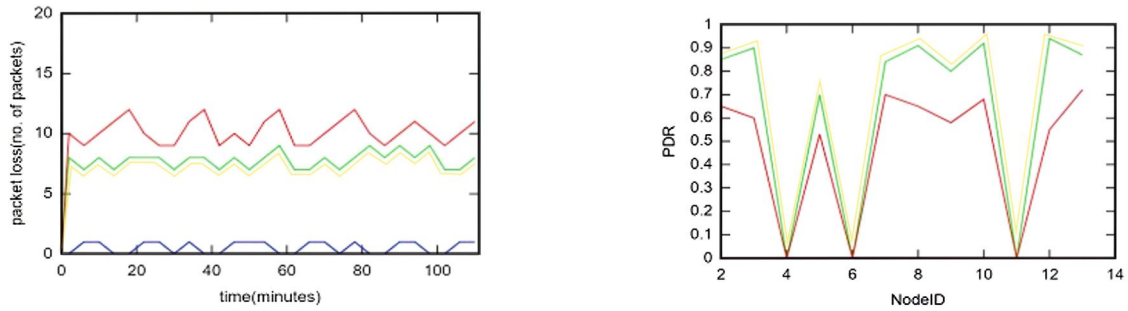


Fig 3

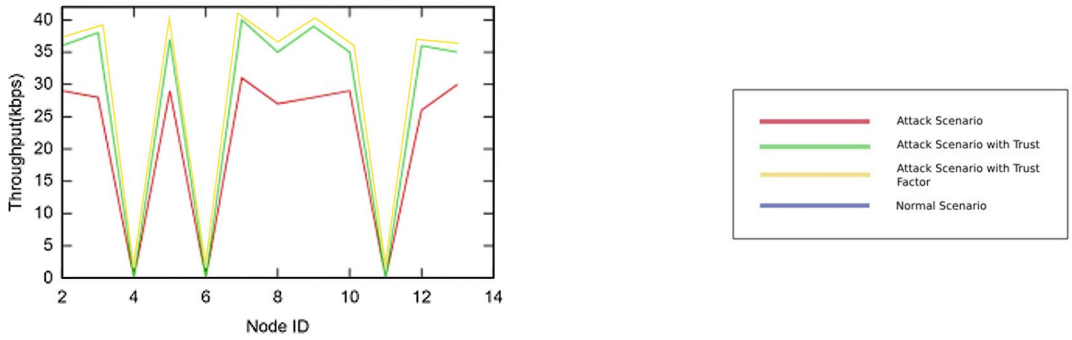


Fig 4

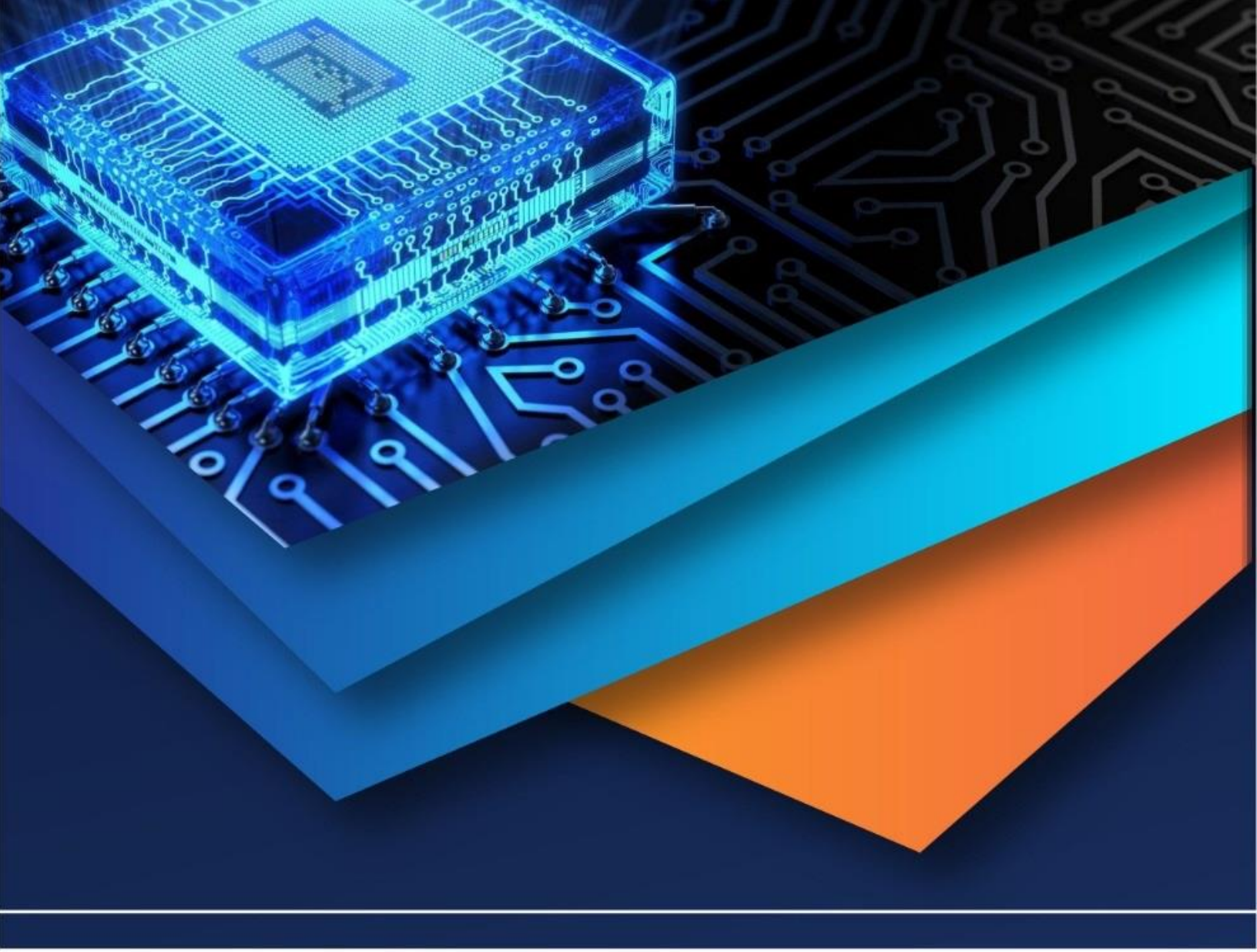
After analyzing the entire packet log, the RPL simulation's outcomes are shown in the graphs in Figures 3, 4, and 5. Five minutes at a time, the simulation ran for ninety minutes. Figure 3 displays the packet drop % associated with blackhole attacks. While the trust component included in the trust-based RPL protocol demonstrated an observed 25 percent frequency of packet loss, the standard RPL protocol based on trust recorded a 27 percent frequency of packet loss. According to the data below, the RPL protocol based on a trust mechanism with a trust factor performs better under blackhole attacks than the standard version of the RPL protocol based on a trust mechanism without a trust factor. The packet delivery ratio for the assault and trust-based scenarios with and without a trust factor is shown in Figure 4. Genuine motes have PDR values between 0.5 and 0.7, while attackers, such as motes 4, 6, and 11, have PDR values that fall to zero. Due to the substantial packet loss, the PDR in the attack scenario without trust factor is lower than the conditions of the attack with trust factor, falling between 0.61 and 0.96. Figure 5 illustrates that the throughput is reduced in the attack scenario compared to the trust factor. In an assault scenario when the trust factor is low, a throughput of 35 to 40 kilobytes per second is seen. In the attack scenario, the trust factor is found to be between 36 and 42 kilobytes per second.

V. CONCLUSION AND FUTURE WORKS

Malicious nodes can jeopardize Internet of Things networks' dependability. This also impacts routing since the attacker can delete all packets, publish erroneous routing information, or impede data flow. It has been demonstrated that using cryptographic algorithms is inefficient and insufficiently secure. Consequently, the proposed method provides a routing protocol that functions better on trust measures. Each network mote calculates a trust value based on the packet delivery ratio (PDR). This trust metric serves as the basis for differentiating malicious motes from routing choices. According to the results of the Contiki simulation, the trust factor integrated protocol performs better than the trust integrated variation in terms of throughput, PDR, and percentage of lost packets. Therefore, the proposed approach provides a workable protection against black hole attacks. Energy measures may be used in future studies to enable the integration of these. values that vary between the packets being sent and received and can provide a precise trust value, aiding in the routing decision-making process. Furthermore, the trust-based framework can be extended to protect against additional routing dangers like selective forwarding, among others.

REFERENCES

[1] In ICICCT 2019—System Reliability, Quality Control, Safety, Maintenance, and Management: Applications to Electrical, Electronics, and Computer Science and Engineering (Springer, 2020), pp. 457–464, N. Bhalaji, K. Hariharasudan, and K. Aashika discuss "A trust-based mechanism to combat blackhole attack in rpl protocol."
[2] "Routing metrics used for path calculation in low-power and lossy networks," Tech. Rep.(2012), by J.-P. Vasseur, M. Kim, K. Pister, N. Dejean, and D. Barthel.
[3] L. Ericsson, White Paper 14, 124 (2011), "More than 50 billion connected devices."
[4] IEEE Internet of Things Journal 4, 1910–1923, "A survey of potential security issues in existing wireless sensor network protocols," by I. Tomic and J. A. McCann (2017).
[5] "A survey on trust management for Internet of things," Journal of Network and Computer Applications42, 120–134 (2014), Z. Yan, P. Zhang, and A. V. Vasilakos.
[6] "Performance analysis of IoT protocol under different mobility models," Computers & Electrical Engineering 72, 154–168 (2018), K. Kabilan, N. Bhalaji, C. Selvaraj, M. Kumaar, and P. Karthikeyan.
[7] "Routing attacks and countermeasures in the rpl-based internet of things," International Journal of Distributed Sensor Networks 9, 794326 (2013), L. Wallgren, S. Raza, and T. Voigt.
[8] "Towards a trust computing architecture for rpl in cyber-physical systems," by S. Seeber, A. Sehgal, B. Stelte, G. D. Rodosek, and J. Schönwälder, in Proceedings of the 9th International Conference on Network and Service Management (CNSM 2013) (IEEE,2013), pp. 134–137.
[9] In the International Journal of Computer Science and Network Security (IJCSNS) 16, 1 (2016), A. R. Dhakne and P. N. Chatur published "Tcnpr: trust calculation based on nodes properties and recommendations for intrusion detection in a wired sensor network."
[10] In Proc. of the Sixth International Conference on Emerging Security Information, Systems and Technologies (SECURWARE), Rome, Italy (August 2012), K. Chugh, L. Aboubaker, and J. Loo, "Case study of a black hole attack on lowpan-rpl," Vol. 7 (2012), pp. 157–162.
[11] K. Weekly and K. Pister, "Assessing sinkhole defense strategies in RPL networks," 20th IEEE International Conference on Network Protocols (ICNP) 2012, pp. 1–6.
[12] "Trust-based strategy to resist collaborative black hole attack in manet," by N. Bhalaji, A. V. Kanakeri, K. P. Chaitanya, and A. Shanmugam, in Information Processing and Management: International Conference on Recent Trends in Business Administration and Information Processing, BAIP 2010, Trivandrum, Kerala, India, March 26-27, 2010. Proceedings, 468–474 (Springer, 2010).
[13] H. Ali, "RPL in Contiki: A Performance Evaluation" (2012).
[14] "Security vulnerabilities and countermeasures in the rpl-based internet of things," by W. Yang, Y. Wang, Z. Lai, Y. Wan, and Z. Cheng, in the 2018 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC) (IEEE, 2018), pp. 49–495.
[15] "Prevention of black hole attack in manets using enhanced aodv protocol," International Journal of Applied Engineering Research 10, 2037–2042(2015), A. Liya, N. Sabana, and V. Leena.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY