Detection of Rank, Sybil and Wormhole Attacks on RPL Based Network Using Trust Mechanism

Anup W. Burange [1], Dr. Ms. V. M. Deshmukh [2]

[1,2] *Department of Computer Science & Engineering, PRMIT&R, Badnera-444701, Maharashtra, India*

Abstract

The amount of constrained devices which exhibit the ability of getting connected to internet are increasing day by day, which makes the routing process challenging and vulnerable to different security threats. The resource constrained nature of low power and lossy network (LLNs) does not make it suitable for traditional security measures. Due to which there is high possibility of different routing and topology attacks. This paper consists of the attack detection of some topological & identity attacks like rank attack, wormhole attack and Sybil attack and also its effect on network parameters like throughput, overhead, delay etc. The attack scenarios are in static as well as in dynamic mode.

Keywords

RPL, Rank Attack, Wormhole attack, Sybil Attack

1. Introduction

One of the major security requirements in the field of low power and lossy networks LLNs is secured routing strategy. IoT devices and its applications have reported much vulnerability and are in danger of extinction to be attacked by some intruder nodes. Rapid growing use of connected devices enables new ways to carry out different vulnerabilities. Ubiquitous use of IoT systems may lead to more serious attacks.[1] Studies have shown that current RPL protocol is susceptible to many routing attacks like Rank attack, Sybil attack, Sinkhole attack, Blackhole attack, Version number attack etc. Moreover there is need of investigation to ensure that trust solutions for constrained devices like IoT, should be scalable across billions of devices. Though quite a few techniques have been developed to counter security concerns in RPL, these techniques also consist of some weaknesses which make them insufficient for constrained devices. To counter the attacks in network, Intrusion Detection Systems are also used, they analyses the activity in network and identifies malicious behavior of node in network. [2] It is also difficult to use well known and traditional security techniques like encryption as it is processing intensive and require high computational resources. An IDS based on the concept of Trust Management, [3] Machine Learning,[4] Fuzzy logic [5]can be useful for mitigating these kind of attacks. This paper shows the implementation of Rank, Wormhole & Sybil attack in RPL involved network and its effects on different parameters related to the network. The order of the paper is as follows: Section 2 consists of RPL protocol working and RPL security issues, which includes Rank, Wormhole and Sybil attack and its related literature. Section 3 consists of implementation details about these attacks. Section 4 includes the results of implementation.

ACI'22: Workshop on Advances in Computation Intelligence, its Concepts & Applications at ISIC 2022, May 17-19, Savannah, United States

EMAIL: anup.burange6@gmail.com (A. 1)

2. RPL and Its Related Work

IoT typically exhibits the IEEE standard while using Routing Protocol for Low Power and Lossy Networks at the network layer, 802.15.4 is used at the physical and data levels (RPL). It is most suitable protocol for IoT and other constrained devices.[6] It creates Destination Oriented Directed Acyclic Graph (DODAG) structure to route data packets. Each DODAG is connected to Border Router (BR) and backbone line connects BR to local internet. The task of selecting and optimizing the routes as per the different metrics is carried out by Objective Function (OF) within DODAG. Placement of a node is getting decided by its Rank in relation to the sink node. For proper functioning of RPL different control messages are being used by the protocol these are DIO (DODAG Information Object), which is used for maintaining and updating the topology; DAO (DODAG Destination Advertisement Object), which is responsible for transmitting destination information upwards for route updating progress; and lastly, DIS (DODAG Information Solicitation), which works for a new node. i.e Before entering the network, a new node might request information on the topology. The primary task of initializing the topology setup is carried out by the DAO and DIS messages.[7] RPL has "Rank" value for every node which determines particular location of every node relative to BR and rest of the nodes in DODAG. Node which has lowest rank will be selected as parent, rank is nothing but the "coordinates" of a node in graph hierarchy. Rank helps to detect and avoid loops during routing process.[8] It works in two ways Storing mode and Non-storing mode. In pre-mode all nodes save the router tables themselves, while in the latest mode only edge-router saves the route table. By default the RPL comes with three security options, these are unsafe, pre-installed and authenticated. [9] These security modes are primary security measures and does not solve all security concerns. In the RPL protocol, routes are stored in two different ways. While messages are sent to the root node in the centralized mode, each node in the dispersed mode has a routing table and shows routing decisions for its subtree.[10]

2.1. RPL Security Issues

IoT includes the threats to existing infrastructure as Routing specific attacks and Resource specific attacks. These are further can be divided into network resources, traffic and topology related attacks.[11]

2.1.1. *Wormhole Attack*

In wormhole attack, attacker nodes forms a channel amongst them and packets are transmitted through it.[12] Malicious nodes try to make believe that they are close to other nodes in the network so that other node should transmit their packet through these malicious nodes.[13]

Pavan pongale et al. a proposed novel system for detecting wormhole attacks, IDS detects threats by using node location and neighbor information. Their system uses acquired signal strength to detect malicious location / attacker on the network. They proposed a hybrid system in which the central modules of 6BR and the other modules are distributed to the sensor nodes. Location information can be helpful for detection of Sybil attack and clone-ID attack. This system considers only static nodes and they claimed to be energy efficient having less energy overhead with high true positives.[14]

Snehal deshmukh bhosale et al. to detect wormhole attacks and attackers, they used an intrusion detection system (IDS). They used only received signal strength as parameter for detection of malicious nodes. The IDS used is hybrid IDS having centralized and distributed module. Centralized module detects attack and distributed module detects attacker node. This system is implemented it in cooja simulator of contiki operating system, success rate of system is claimed to be 90%. [15]

Rupinder singh et al. proposed WRHT, which is a hybrid technique for wormhole detection. This technique is the combination of two techniques called watchdog and Delphi. They calculated

determining the likelihood of packet loss and time delays on each path to determine the probability of a wormhole. [16]

Ruchi Mehta et al. proposed lightweight trust based mechanism consisting of direct and indirect trust. They claimed that their technique is energy efficient and they termed it as lightweight but they tested it on only two parameters namely throughput and packet loss rate. [17]

Prachi shukla, implemented a machine learning approach for wormhole detection. They developed ML based IDS consisting of unsupervised K-means IDS, Supervised tree based IDS and hybrid IDS which combine these two IDS. Claimed detection rate is between 70 to 80%. [18]

2.1.2. *Sybil Attack*

In this attack type, attacker or malicious node exhibit different illegitimate identities and it can execute a variety of malicious activities such as unfair voting, fake route broadcast.[19] Sybil attack can turn out to be the origin of other attacks and it can be more dangerous in dynamic environment thereby degrading the network performance by increasing network traffic overhead.[20]

S. Murali et al, they proposed a lightweight intrusion detection system and a mobile Sybil attack detection system inspired by an artificial bee colony (ABC) were developed for RPL's mobile environment. They examined the effectiveness of RPL and concentrated on three sorts of Sybil attacks based on its behavior. They focused on three categories of the Sybil attack based on its actions and examined RPL's performance, They used bio-inspired analytical model which seems to be complex to implement in resource constrained environment. [21]

Faiza Medjek et al. simulated the impact of Sybil mobile attack. They proposed a new intrusion detection system called trust based IDS (T-IDS). They proposed a new timer and made some additions to RPL control messages. Each node employs a trusted platform module (TPM) for its system identity management module. The TPM requires the manufacturer to create a cryptographic co-processor chip that offers hardware support for storing security parameters and identities, this solution is not feasible as manufacturing unit have their own limitations.[22]

C. wang et al. proposed a technique for Sybil attack detection based on Channel State Information (CSI). Proposed algorithm is claimed for the detection of Sybil attack in static devices. They also proposed a scheme based on channel characteristic for dynamic attackers.[23]

Alekha Kumar Mishra et al. developed analytical model which uses k-mean clustering for finding deployment location of attacker. Identity replacement model is also presented to circumvent fake identity detection. This algorithm achieves very less detection range of nearly 48%.[24]

Ashwini Nikam et al, implemented IDS based on opinion metric for detection and identification of Sybil and DoS attacks. They calculated opinion values (trust) of a node based on its positive and negative experiences. Detection of attacker node done by border router based on metric values. They used centralized approach which may not be effective in case of IoT devices. Failure of BR will result in system breakdown. [25]

2.1.3. Rank Attack

This form of attack involves an attacker node introducing a bogus rank value. A node's distance from the root node is used to calculate its rank value.[26] By misusing the rank value, attacker node attracts the neighboring node to capture the data packets and then it can drop those packets or can send it to the non-destined nodes. Increased rank attack and lowered rank attack are two more categories that can be applied to this attack. Increased rank attack causes the loop creation in DODAG

due to which packet fails to reach its destination. In decreased rank attack, node falsely claims as parent thereby decreasing its rank value and keeping it minimum.[27]

R. Stephen et al., simulated RIAIDRPL algorithm, they claimed that the algorithm is capable of finding the loops in DODAG, created by attacker node. They simulated the performance of this algorithm on cooja simulator. The claimed accuracy is 90% and they compared it with RPL, LRPL based on different network parameters. [28]

Usman Shafique et al. implemented an IDS which is based on sink node, for detection of rank attack. They claimed lower computational overhead and high detection rate. Future work include the addition of more metric like energy, hop count, bandwidth, delay etc. These factors are very important but they mentioned in future implementation.[29]

Anhtuan Le et al, investigated how rank attacks affected network metrics. They claim different types of rank attacks and they analyzed their behavior. They studied; Rank attack may result in path loops, packet collisions, unoptimized paths, increased overhead, and other network performance degradations. [30]

3. Attacks Detection using Trust Mechanism

Below, we present our proposed trust-based method, which is included in the RPL protocol. Determining an individual node's trust value for the RPL network is the mechanism's main objective and embed such values in routing decisions. As seen below, the Direct Trust is calculated.

$$\mathbf{DT\ (i,j)\ (t) = F_{ji}\ (t) / (S_{ij}\ (t) + k[S_{ij}\ (t) - F_{ji}\ (t)])}$$

where,

$F_{ji}(t)$ = Total number of packets forwarded by "j" on behalf of "i".

$\mathbf{S_{ij}\ (t)}$= Total number of packets sent by node "i" to node "j".

k= Penalty value (Depends on frequency of interaction, length of the interaction, Energy consumed).

For indirect trust computation, we considered the parameters like reputation, experience, etc. between the nodes.

Indirect Trust (IT) = Reputation Trust (RT) + Experience Trust (ET)

Where RT depends on the positive and negative recommendations from neighboring nodes and ET is calculated by node's past behavior is routing process analyzed by the sink node. We detected three attacks, namely, Rank, Wormhole, and Sybil, in static and dynamic scenarios, considering 15 and 30 nodes, respectively. It is very important to check the effects of these attacks in a dynamic environment as most of the IoT nodes will be dynamic in the future. three attack types namely as Rank, Sybil and Wormhole with 20 and 40 nodes on cooja simulator of contiki with MRHOF objective function and z1 mote type, radio medium model used is UDGM distance loss. In these attacks we have taken two scenarios of static nodes and dynamic nodes. In static, all the nodes are static whereas in dynamic we implemented Random Way Point model, which is one of the standard mobility model. Following are the screenshots of the attack types.

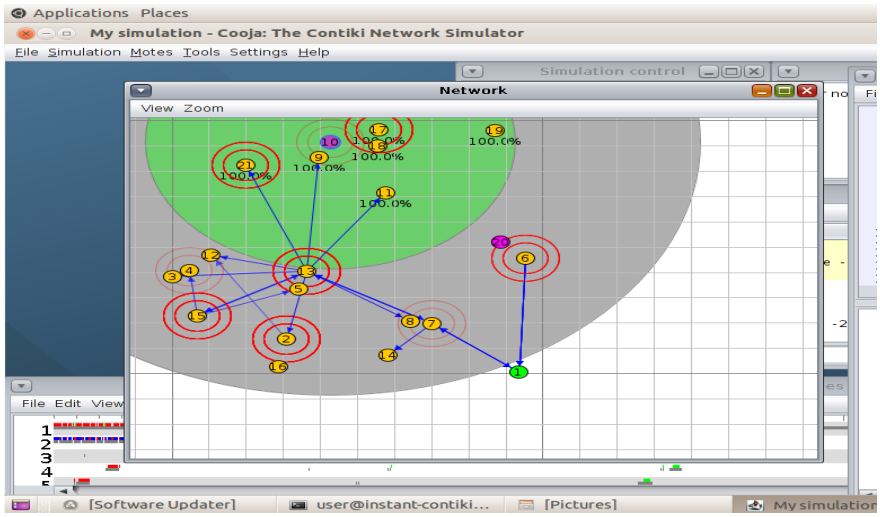

Figure 1: Rank Attack Implementation

Above figure shows the rank attack implementation on cooja simulator.Two scenarios are taken 20 and 40 nodes, in 20 nodes Node 10 & 20 are rank attacker nodes. In 40 nodes, Node 10,20,30,40 are attacker nodes.

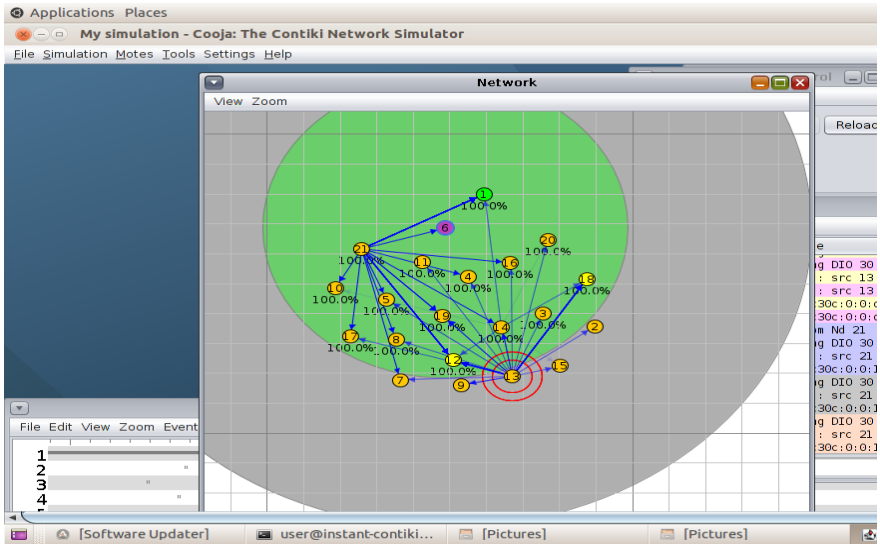

Figure 2: Sybil Attack Implementation

Above figure is the screenshot of Sybil attack implementation on cooja simulator. Node 6 is attacker node in 20 nodes simulation, while Nodes 6 and 24 are attacker nodes in 40 nodes simulation.

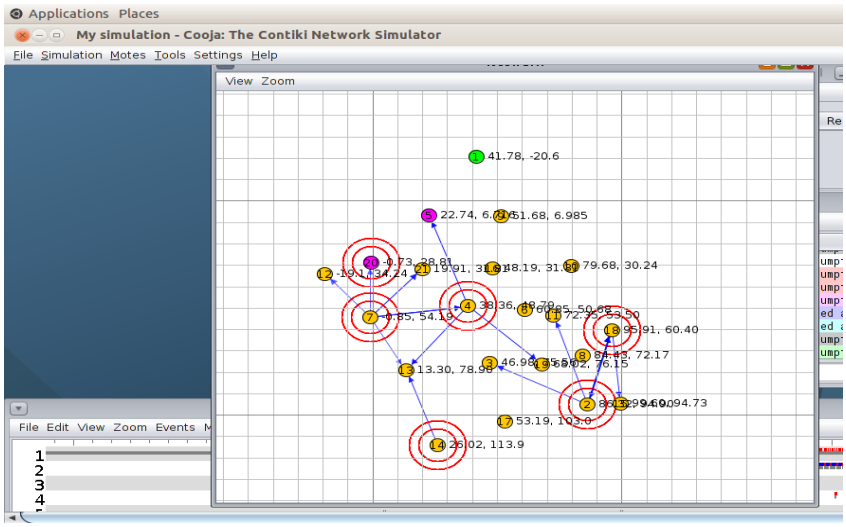

Figure 3: Wormhole Attack Implementation

Above figure is about the Wormhole attack implementation on cooja simulator. Nodes 5 and 20 are attacker nodes in 20 nodes simulation.

4. Results

As stated earlier, we implemented two attack scenarios as static and dynamic with 20 and 40 nodes for each attack. Following are the graphs for the above mentioned attacks in two scenarios. Also we compared it with normal RPL protocol and we named it as “Without attack” for comparison.

We considered the following performance metrics for comparing normal RPL network with attack models**.**

- Packet delivery ratio (Percentage)

PDR in RPL network is the ratio between total packets sent to the total packets received.

- Overhead (Packets)

Overhead in RPL network can be defines as, amount of control packets required for network path initialization. DIO,DAO and DIS packets are said to be a control packets in RPL network.

- Delay(ms)

Delay is the measure of time taken between total time received to the total sent time.

- Throughput(bits/sec)

Throughput is the measure of rate of successful data delivery of data Packets.

- Energy Consumption(joules)

Energy consumption is the total energy or power used to send or receive data packets by a node.

4.1.1. Static Environment

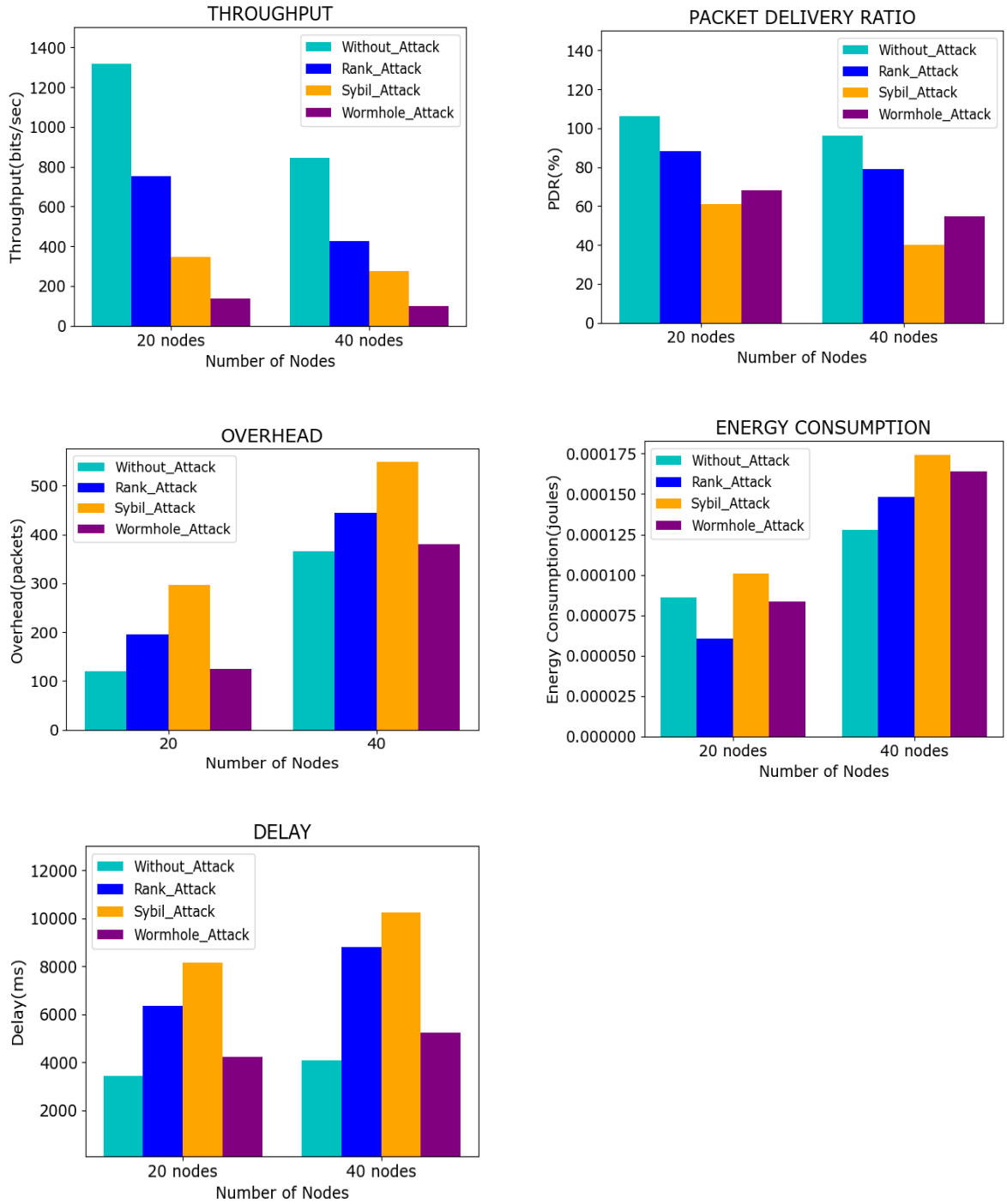

Figure 4: Performance metric comparison in static environment.

4.1.2. Dynamic Environment

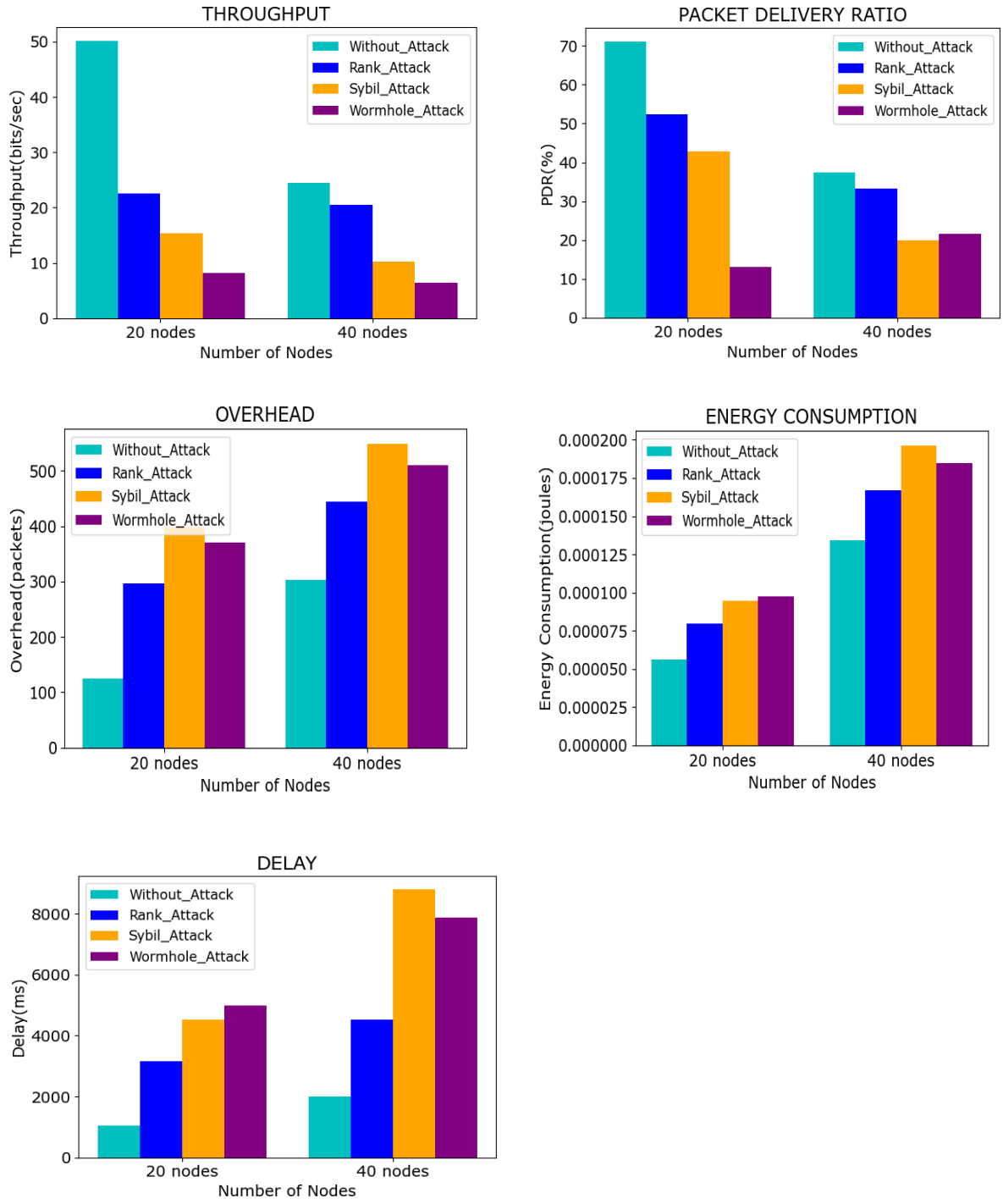

Figure 5: Performance metric comparison in dynamic environment.

4.1.3. Attacks Detection

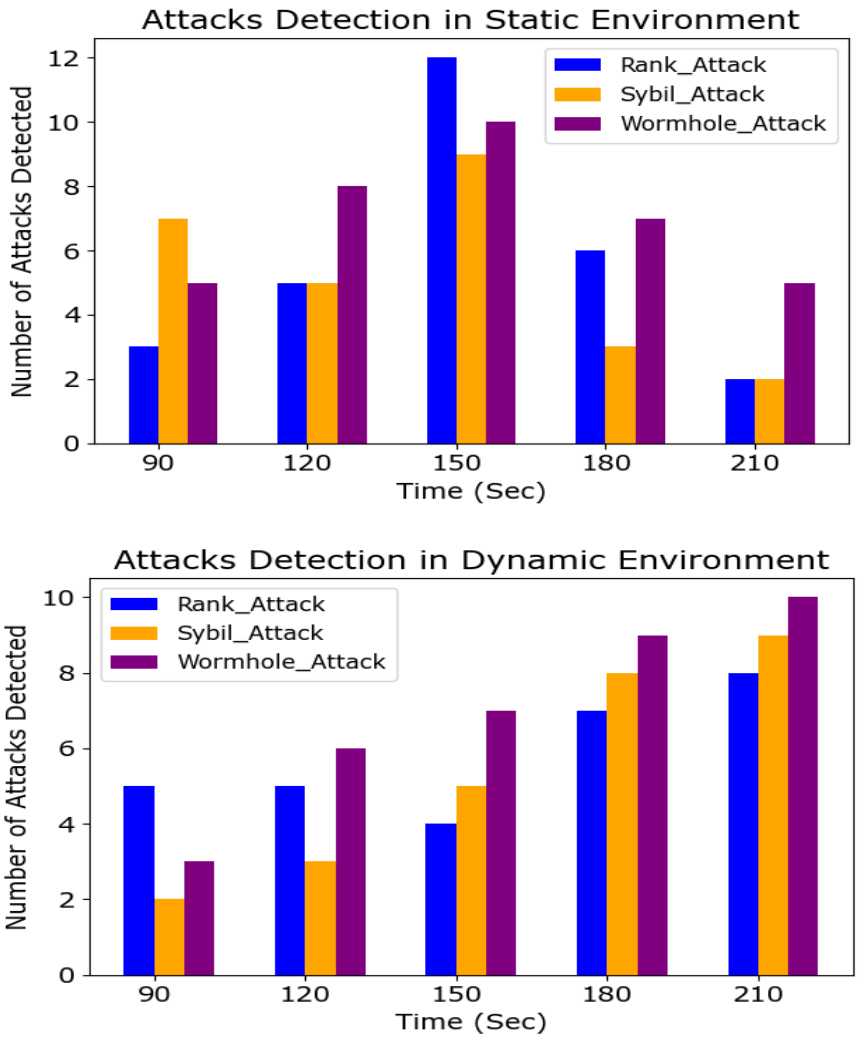

Figure 6: Number of attacks detected in static and dynamic environment.

4.1.4. Result Discussion

Though the graphs are self explanatory, we want to highlight some of the key findings in the result. We have taken two scenarios static and dynamic with 20 and 40 nodes respectively. As shown in figure 4, graph "Without attack" is nothing but the RPL protocol with MRHOF objective function. In this the negative effects by the attacks on performance metrics like throughput, packet delivery ratio, delay, overhead, energy consumption etc are analyzed in static environment, where the nodes are stationary. The same metrics are analyzed in dynamic environment, where all the nodes are moving in some specific manner. We run the simulation many times to perfectly get the values and thus graphs. In static it is found that, these metrics are highly impacted by the attacks compared to normal routing \i.e without attack, whereas in dynamic scenario energy consumption and packet overhead are more. Thus it is important to identify and remove such type of attacker nodes from the network, to improve the overall efficiency of it.

5. Conclusion

Due to low power and computation capabilities IoT devices are more prone to different routing and topology attacks. In this work, we detected three attacks namely rank, wormhole and Sybil, using trust mechanism & also by some attack characteristics. Simulations are done in static and dynamic environment scenarios with 20 and 40 for each attack type. In static and dynamic it is identified from the graph that all the parameters are affected by the attacks. We are also working on the lightweight IDS based on machine learning to indentify and prevent these attacks to make routing safe in IoT environment.

6. References

[1] J. V. V. Sobral, J. J. P. C. Rodrigues, R. A. L. Rabêlo, J. Al-Muhtadi, and V. Korotaev, "Routing protocols for low power and lossy networks in internet of things applications," *Sensors (Switzerland)*, vol. 19, no. 9, pp. 1–40, 2019, doi: 10.3390/s19092144.

[2] M. Miettinen, S. Marchal, I. Hafeez, N. Asokan, A. R. Sadeghi, and S. Tarkoma, "IoT SENTINEL: Automated Device-Type Identification for Security Enforcement in IoT," *Proc. - Int. Conf. Distrib. Comput. Syst.*, pp. 2177–2184, 2017, doi: 10.1109/ICDCS.2017.283.

[3] Z. A. Khan and P. Herrmann, "A trust based distributed intrusion detection mechanism for internet of things," *Proc. - Int. Conf. Adv. Inf. Netw. Appl. AINA*, pp. 1169–1176, 2017, doi: 10.1109/AINA.2017.161.

[4] U. Jayasinghe, G. M. Lee, T. W. Um, and Q. Shi, "Machine Learning Based Trust Computational Model for IoT Services," *IEEE Trans. Sustain. Comput.*, vol. 4, no. 1, pp. 39–52, 2019, doi: 10.1109/TSUSC.2018.2839623.

[5] M. D. Alshehri, F. K. Hussain, and O. K. Hussain, "Clustering-Driven Intelligent Trust Management Methodology for the Internet of Things (CITM-IoT)," *Mob. Networks Appl.*, vol. 23, no. 3, pp. 419–431, 2018, doi: 10.1007/s11036-018-1017-z.

[6] L. Wallgren, S. Raza, and T. Voigt, "Routing attacks and countermeasures in the RPL-based internet of things," *Int. J. Distrib. Sens. Networks*, vol. 2013, 2013, doi: 10.1155/2013/794326.

[7] P. Suganya and C. H. Pradeep Reddy, "A survey and analysis on various objective functions defined for RPL in 6LOWPAN," *Int. J. Recent Technol. Eng.*, vol. 7, no. 6, pp. 403–411, 2019.

[8] A. Verma and V. Ranga, "Evaluation of Network Intrusion Detection Systems for RPL Based 6LoWPAN Networks in IoT," *Wirel. Pers. Commun.*, vol. 108, no. 3, pp. 1571–1594, 2019, doi: 10.1007/s11277-019-06485-w.

[9] S. Y. Hashemi and F. Shams Aliee, "Dynamic and comprehensive trust model for IoT and its integration into RPL," *J. Supercomput.*, vol. 75, no. 7, pp. 3555–3584, 2019, doi: 10.1007/s11227-018-2700-3.

[10] A. Raoof, A. Matrawy, and C. H. Lung, "Routing Attacks and Mitigation Methods for RPL-Based Internet of Things," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 2, pp. 1582–1606, 2019, doi: 10.1109/COMST.2018.2885894.

[11] W. Alnumay, U. Ghosh, and P. Chatterjee, "A trust-based predictive model for mobile Ad Hoc network in internet of things," *Sensors (Switzerland)*, vol. 19, no. 6, pp. 1–14, 2019, doi: 10.3390/s19061467.

[12] M. Goyal and M. Dutta, "Intrusion Detection of Wormhole Attack in IoT: A Review," *2018 Int. Conf. Circuits Syst. Digit. Enterp. Technol. ICCSDET 2018*, pp. 1–5, 2018, doi: 10.1109/ICCSDET.2018.8821160.

[13] S. M. H. Mirshahjafari and B. S. Ghahfarokhi, "Sinkhole+CloneID: A hybrid attack on RPL performance and detection method," *Inf. Secur. J.*, vol. 28, no. 4–5, pp. 107–119, 2019, doi: 10.1080/19393555.2019.1658829.

[14] P. Pongle and G. Chavan, "Real Time Intrusion and Wormhole Attack Detection in Internet of Things," *Int. J. Comput. Appl.*, vol. 121, no. 9, pp. 1–9, 2015, doi: 10.5120/21565-4589.

[15] S. Deshmukh-Bhosale and S. S. Sonavane, "A Real-Time Intrusion Detection System for Wormhole Attack in the RPL based Internet of Things," *Procedia Manuf.*, vol. 32, pp. 840–

847, 2019, doi: 10.1016/j.promfg.2019.02.292.
[16] R. Singh, J. Singh, and R. Singh, “WRHT: A Hybrid Technique for Detection of Wormhole Attack in Wireless Sensor Networks,” *Mob. Inf. Syst.*, vol. 2016, 2016, doi: 10.1155/2016/8354930.
[17] R. Mehta and M. M. Parmar, “Trust based mechanism for Securing IoT Routing Protocol RPL against Wormhole Grayhole Attacks,” *2018 3rd Int. Conf. Converg. Technol. I2CT 2018*, pp. 1–6, 2018, doi: 10.1109/I2CT.2018.8529426.
[18] P. Shukla, “ML-IDS: A machine learning approach to detect wormhole attacks in Internet of Things,” *2017 Intell. Syst. Conf. IntelliSys 2017*, vol. 2018-January, no. September, pp. 234–240, 2018, doi: 10.1109/IntelliSys.2017.8324298.
[19] K. Phani Rama Krishna and R. Thirumuru, “Optimized energy-efficient multi-hop routing algorithm for better coverage in mobile wireless sensor networks,” *J. Integr. Sci. Technol.*, vol. 10, no. 2, pp. 100–109, 2022.
[20] S. Raza, L. Wallgren, and T. Voigt, “SVELTE: Real-time intrusion detection in the Internet of Things,” *Ad Hoc Networks*, vol. 11, no. 8, pp. 2661–2674, 2013, doi: 10.1016/j.adhoc.2013.04.014.
[21] S. Murali and A. Jamalipour, “A Lightweight Intrusion Detection for Sybil Attack under Mobile RPL in the Internet of Things,” *IEEE Internet Things J.*, vol. 7, no. 1, pp. 379–388, 2020, doi: 10.1109/JIOT.2019.2948149.
[22] F. Medjek, D. Tandjaoui, I. Romdhani, and N. Djedjig, “A trust-based intrusion detection system for mobile RPL based networks,” *Proc. - 2017 IEEE Int. Conf. Internet Things, IEEE Green Comput. Commun. IEEE Cyber, Phys. Soc. Comput. IEEE Smart Data, iThings-GreenCom-CPSCom-SmartData 2017*, vol. 2018-Janua, pp. 735–742, 2018, doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2017.113.
[23] C. Wang *et al.*, “Accurate sybil attack detection based on fine-grained physical channel information,” *Sensors (Switzerland)*, vol. 18, no. 3, pp. 1–23, 2018, doi: 10.3390/s18030878.
[24] S. K. Apat, J. Mishra, K. S. Raju, and N. Padhy, “The robust and efficient Machine learning model for smart farming decisions and allied intelligent agriculture decisions,” *J. Integr. Sci. Technol.*, vol. 10, no. 2, pp. 139–155, 2022.
[25] A. Nikam and D. Ambawade, “Opinion Metric Based Intrusion Detection Mechanism for RPL Protocol in IoT,” *2018 3rd Int. Conf. Converg. Technol. I2CT 2018*, pp. 1–6, 2018, doi: 10.1109/I2CT.2018.8529770.
[26] D. Airehrour, J. A. Gutierrez, and S. K. Ray, “SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things,” *Futur. Gener. Comput. Syst.*, vol. 93, pp. 860–876, 2019, doi: 10.1016/j.future.2018.03.021.
[27] W. Choukri, H. Lamaazi, and N. Benamar, “RPL rank attack detection using Deep Learning,” *2020 Int. Conf. Innov. Intell. Informatics, Comput. Technol. 3ICT 2020*, pp. 5–10, 2020, doi: 10.1109/3ICT51146.2020.9311983.
[28] R. Stephen and L. Arockiam, “RIAIDRPL: Rank Increased Attack (RIA) Identification Algorithm for Avoiding Loop in the RPL DODAG,” *Int. J. Pure Appl. Math.*, vol. 119, no. September, pp. 1203–1209, 2018.
[29] U. Shafique, A. Khan, A. Rehman, F. Bashir, and M. Alam, “Detection of rank attack in routing protocol for Low Power and Lossy Networks,” *Ann. des Telecommun. Telecommun.*, vol. 73, no. 7–8, pp. 429–438, 2018, doi: 10.1007/s12243-018-0645-4.
[30] A. Le, J. Loo, A. Lasebae, A. Vinel, Y. Chen, and M. Chai, “The impact of rank attack on network topology of routing protocol for low-power and lossy networks,” *IEEE Sens. J.*, vol. 13, no. 10, pp. 3685–3692, 2013, doi: 10.1109/JSEN.2013.2266399.