International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-10 Issue-2, December 2020

The Impact of Mobile DIS and Rank-Decreased Attacks in Internet of Things Networks

Christopher Mitchel, Baraq Ghaleb, Safwan M. Ghaleb, Zakwan Jaroucheh, Bander Ali Saleh Al-rimy

ABSTRACT: ***With a predicted 50 billion devices by the end of 2020, the Internet of things has grown exponentially in the last few years. This growth has seen an increasing demand for mobility support in low power and lossy sensor networks, a type of network characterized by several limitations in terms of their resources including CPU, memory and batter, causing manufactures to push products out to the market faster, without the necessary security features. IoT networks rely on the Routing Protocol for Low Power and Lossy Network (RPL) for communication, designed by the Internet Engineering Task Force (IETF). This protocol has been proven to be efficient in relation to the handling of routing in such constrained networks, However, research studies revealed that RPL was inherently designed for static networks, indicating poor handling of mobile or dynamic topologies which is worsen when introducing mobile attacker. In this paper, two IoT routing attacks are evaluated under a mobile attacker with the aim of providing a critical evaluation of the impact the attacks have on the network in comparison to the case with static attacker. The first attack is the Rank attack in which the attacker announces false routing information to its neighbour attracting them to forward their data via the attacker. The second attack is the DIS attack in which the attacker floods the network with DIS messages triggering them to reset their transmission timers and sending messages more frequently. The comparison were conducted in terms of average power consumption and also the packet delivery ratio (PDR). Based on the results collected from the simulations, it was established that when an attacking node is mobile, there's an average increase of 36.6 in power consumption and a decrease of 14 for packet delivery ratios when compared to a static attacking node.***

Keywords: DIS attack, Internet-of-Things; IoT attacks, Mobile attacker, Rank attack.

I. INTRODUCTION

The Internet of Things (IoT) is a system of physical devices designed to allow data communication over a network without interference from the end-user [1], [2] [3]. The use of IoT devices has grown exponentially in recent years, and it is predicted that there will be 50 billion such devices by the end of 2020 [4]. IoT is progressively affecting our daily lives, from home security systems to personal fitness devices.

The development of the Internet of Things is based on a desire to control and automate everything with minimal effort. This has led to the rapid growth of and competition amongst IoT markets, where devices are being developed and deployed quickly without the appropriate security considerations, leaving many vulnerable to a multitude of attacks. A substantial amount of these devices are sensors designed to record and communicate environmental data, described as wireless sensor networks (WSN). WSN comprise of a few to a massive deployment of sensor nodes that are interconnected, allowing data to collectively pass through a network to the central location called the sink, where the data can then be analyzed. However, wireless sensor networks involve cheap low power sensors meaning they're constrained by battery capacity, processing speed, computational power, and bandwidth, suggesting an attacker can exploit the limited nature of these devices, which can exhaust the network of resources leading to the suboptimization of the system [5]. Wireless sensor networks rely on the Routing Protocol for Low Power and Lossy Network (RPL) for communication designed by the Internet Engineering Task Force (IETF). RPL aims to address the issues the constrained sensors face by taking into consideration the problem areas surrounding the sensors such as limited battery life and processing powers however the RPL protocol is proven to be vulnerable to many common routing attacks as proven by [6], [7]. "RPL was mainly designed to comply with the primitive requirements of static IoT applications, and it behaves poorly in confronting with the severe alterations in mobile conditions [7], [8]. In this paper, the RPL protocol will be evaluated in terms of security with respect to different classifications of routing attacks with mobility as a factor.

The paper will attempt to answer the following research questions:

- How is the outcome of a given attack affected by a malicious node being mobile in terms of packet delivery ratio and power consumption?
- Under which scenarios and operating conditions can the attack be more destructive for the network

The rest of the paper is organized as follows: an overview of the RPL protocol is presented in Section II highlighting its main principles.

Revised Manuscript Received on November 25, 2020.
* Correspondence Author
Christopher Mitchel*, School of Computing at Edinburgh Napier University, 10 Colinton Road, Edinburgh, EH10 5DT, UK,
Baraq Ghaleb, School of Computing at Edinburgh Napier University, 10 Colinton Road, Edinburgh, EH10 5DT, UK,
Safwan M. Ghaleb, Faculty of Ocean Engineering Technology and Informatic, University Malaysia Terengganu,
Zakwan Jaroucheh, School of Computing at Edinburgh Napier University, 10 Colinton Road, Edinburgh, EH10 5DT, UK,
Bander Ali Saleh Al-rimy, Faculty of Business and Technology, UNITAR International University, Selangor 47301, Malaysia,

Section III presents an overview of related work. Section IV introduces detailed description of the simulation environment and the obtained results. Finally, Section V overviews the entire study and then presents conclusion reached.

II. RPL OVERVIEW

RPL or the Routing Protocol for Low Power and Lossy Networks is an internet protocol version six based wireless network routing protocol designed for low power and lossy networks, which runs on IEEE 802.14.4. The Internet Engineering Task Force (IETF) ROLL working group proposed RPL in order to tackle the issues large scale power-constrained networks experience as LLN's can contain millions of nodes interconnected together by lossy links characterised by their rates of high loss, low data rates, and unstable nature - existing protocols are not designed to deal with these issues. In addition, by establishing several energy-aware routing metrics, RPL takes energy consumption into account by decreasing routing complexity in order to reduce the amount of memory used. This also includes integrated energy-saving mechanisms in the processing of routes, such as the Trickle algorithm, which can be used to distribute information across the network. When designing RPL, the IETF aimed to achieve the objectives outlined in [RFC5867], [RFC5826], [RFC5673], and [RFC5548] which cover routing requirements for building, home, industrial and urban environments respectively [9]. The basic working principle is to provide multipoint to point routing to a central point and vice versa, therefore allowing upwards and downwards bidirectional links.

A.DODAG Construction

As a distance-vector protocol RPL uses a proactive approach in order to build a DAG (Directed Acyclic Graph) that creates optimal routes for packets sent or received at the sink, every DAG is divided into one or more DODAG (Destination Oriented Directed Acyclic Graph) with one sink node per DODAG. In RPL, the DODAG will compute bidirectional downward and upward routes [10]. The construction of a DODAG begins with the multicasting of the RPL control message DODAG Information Objects (DIO) to its neighbors; these messages hold the necessary routing information and configuration, which is required to construct the DODAG [11]. Once the root sends a local multicast DIO message to the nearest nodes to the root, the following steps will be undertaken. Upon receiving a DIO message a node will add the address of the DIO sender to its potential list of parents where the node will then calculate its rank in relation to the DODAG root based on the rank of the sending node and the Objective Function. Based on the calculations just made the node will set its preferred parent from the list of potential parents. The final step involves the node sending out its own DIO message with the new information learned, in turn allowing other nodes to repeat this process – building the DODAG [12].

B. Rank and Objective Function

The rank value of a node is represented by a scalar number; the number depicts the location of the node within the DODAG. The rank value assists in loop avoidance and detection, route optimization, and manages control overheads. Packet forwarding selection can only be based on the rank of nodes [13]. The researchers also state the nodes must "monotonically increase from the sink to leaf nodes in downwards direction" and vice versa. RPL's Objective Function determines the optimal path (OF) as it calculates the cost of the path, what parent to select and how the rank is chosen for each node [14]. The Objective function allows for a range of routing metrics to be used, such as the Expected Transmission Count (ETX). If selected, all nodes will use this routing metric based on a minimum transmission count value in order to determine the next hop [13]. The authors in [15] improved the work in [13] by adding a statement and explaining the other routing metrics that can be considered by the objective function such as latency or energy. They also give a more detailed explanation of expected transmission count, defining it as the quality of links between nodes and that the rank value is decided based on lower ETX values.

C.RPL Security

Due to the constrained nature and the complex deployment environments [16] states that IoT devices are more vulnerable than the traditional internet as a threat can come from a variety of stages. This is a common theme throughout the literature as other authors such as [17] have agreed that " Providing security to IoT networks is challenging, due to their constrained nature and connectivity to the unsecured internet" [17] study into the security of RPL concludes that in order to make RPL secure, future work and research must take place as the security functionality of RPL as it stands is basic. In the literature, many research papers suggest improvements and revisions of the current state of RPL. This suggests that RPL has significant security vulnerabilities that need to be addressed. A large number of existing studies in the literature have examined the effects of RPL being un-secure where [18] states that the protocol is vulnerable to a large variety of attacks with the consequences being significant in terms of network performance and resources however the author does state that "The RPL protocol defines several mechanisms that contribute to its security." The security mechanisms RPL employs have been heavily scrutinized within the literature arguing that the reason RPL is vulnerable is due to the poor implementation and lack of authentication mechanisms. Work carried out by [19] confirms [18] findings in that the researchers also found that the RPL protocol it stands is exposed to numerous attacks which may degrade resources and performance leading to the output being unreliable. The work carried out by [19] aimed to develop a 'lightweight Trust based mechanism,' implying that RPL's current mechanisms are not safe or functioning correctly. The research in [20] concluded that the security mechanism deployed by RPL are very fragile, and additional security measures are needed to enhance the reliability of RPL. The current security measures RPL employs will be further examined.

D.RPL Security Modes

RPL, by default, offers three different security modes as described by [17].

Authenticated Mode comes with pre-Installed keys which are used to join an RPL instance, but only as a leaf node. In Pre-Installed Mode nodes require pre-installed keys to join an RPL Instance in order to process and generate the RPL security control messages. The final mode is Unsecured Mode where control messages are not sent with any security mechanisms.

The default security mode for RPL is Unsecured, meaning RPL must rely on link-layer security. The research in [17] states that these security modes are not enough to mitigate all types of RPL routing attacks, leaving networks vulnerable. The study in [20] describes the security modes RPL offers; they describe them as weak, which makes RPL vulnerable to many security issues such as routing information exposure and attacks on integrity. Authenticated and Pre-Installed mode poses the ability to exchange secure RPL control messages. These modes assist with the control messages in terms of integrity and confidentiality through the use of AES with 128-bit keys in order to produce Message Authentication Codes (MAC), which are used to ensure the integrity of said messages. For confidentiality, RPL uses RSA with SHA-256 for digital signatures. A study carried out by [21] founds that most current implementations of RPL use unsecured mode, with even the most popular OS's such as not having these security measures in place, the researchers implemented Pre-Installed mode into Cooja and evaluate the performance, they found that there is no adverse effect of having these extra security measures in terms of power consumption and overhead. This paper, however, does not address authenticated mode; therefore, it cannot say that the implementation of security modes does not affect a network as the most secure mode has not been functionally implemented.

III. RELATED WORK: RPL SECURITY SOLUTION

The authors in [20] propose a new lightweight trustbased security algorithm called TmRPL++, which is designed to prevent RPL routing attacks and to strengthen already existing security aspects of the protocol. The researchers felt this was needed as the security mechanisms in RPL are fragile, and more are needed. The proposal enhances network performance under attack with minimum signalling overhead, power consumption, and delay. In order to counteract rank attacks and version attacks, the authors in [22] propose a specification-based IDS for detecting attacks of these types. The researchers built the IDS to gather information on the normal operations of a network in order to detect malicious behaviour, which does not fit the model of normal behaviour. The IDS successfully detected both attacks under multiple different topologies with reasonable overhead. The theme of IDS to detect attacks is very prevalent in the literature with [23] designing an anomaly-based IDS for detecting RPL based attacks. The IDS works through creating an overview of the network and monitoring normal behaviour, with this information gathered, the IDS sets threshold values, which, if exceeded, will trigger the IDS to identify that node as an attacker. They used the DIS attack to test the IDS where they detected three DIS messages was the standard behaviour within a set period, once mounting the attack anything over three was detected to be an attacker with a true positive rate of 100%. Within the literature, there exist many papers on RPL security and how it can be exploited or made stronger with revisions of the current version or added mechanisms. There also exist many papers on mobility, and how it affects networks, how it can be exploited or mechanism which help handle mobility. However, there exists very little literature on how mobility would affect an attack on a network. Literature does exist on attacks on VANET's; however, the papers only detail the principals and dangers of the attacks, no literature surrounding the testing or simulation of these networks was found. Many papers suggest improvements on RPL in order to make it more capable of handling mobility, these papers focus mainly on packet delivery ratios and overheads and not energy consumption despite it being the most crucial factor in such a resource constricted environment. Assumptions can be made based on the reviewed literature concerning the outcomes and effects of attacks; however, no definitive research has been carried out – exposing a gap in the literature, this paper aims to further research into by answering the question "Does mobility affect the outcome of a given attack on a WSN in terms of packet delivery and energy consumption?"

IV. PERFORMANCE EVALUATION AND DISCUSSION

Figure 1 is a graph representing the power consumption across each node in millivolts. For this simulation, all nodes are static, and no routing attacks are currently mounted; the total average power consumption recorded across all nodes was 1.68 mV. By analysing the power consumption across each node, its visible nodes 6,7,12 and 20 are consuming considerably more power than average. This is caused by the mentioned nodes having a low rank, meaning they are situated in areas of high network convergence near the sink; therefore, traffic is funnelling through them to reach the sink.

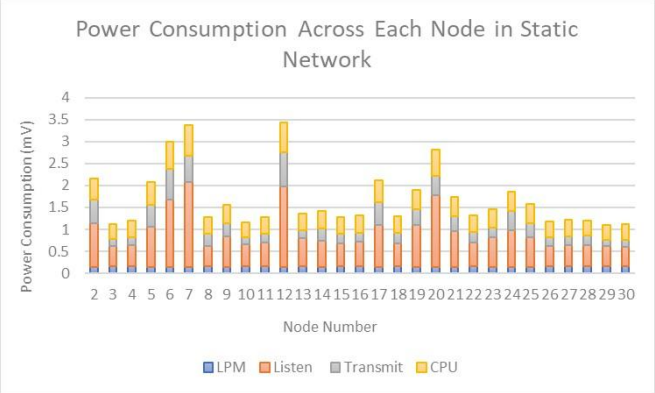

Figure 1: Power Consumption Across Nodes for Static Network

A.DIS attack

The DIS attack focuses on draining resources, therefor higher power consumptions are expected. The results displaying the power across the nodes with the DIS attack mounted is shown in Figure 2.

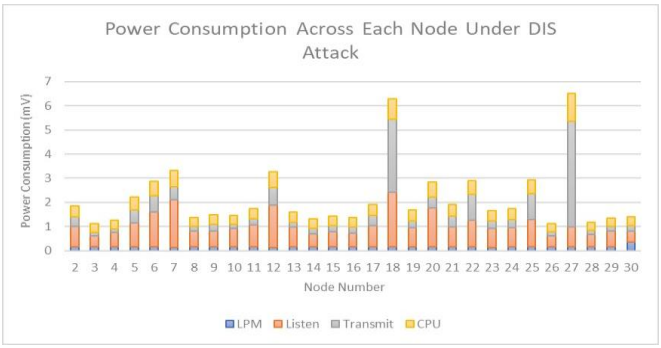

Figure 2: Power Consumption Across Nodes for DIS Attack

The attacking node (node 27) power consumption has risen to 6.496 mV from the testbed network consumption of 1.125 mV, which is a 477% increase in power consumption when compared to the static testbed network. The overall power consumption of the network has increased 24.4% overall in seed one from 1.68 mV to 2.09 mV and a 23.3% increase from 1.742 mV to 2.166 mV. Its visible from the figure that node 18 has a largely increased power consumption. However, this is due to node 27 sending all DIS control messages to node 18 as it was selected as the parent of node 27 based on metrics since all DIS messages are sent to node 18, DIO control messages must be sent back therefor explaining the high transmit and listen power consumption. Research conducted by [24] revealed that the when a spam DIS attack is mounted the power of the attacking node can increase 10x that of a network without the attack. The scale of this aligns with the results collected in this paper as the power increased nearly 6x when the DIS attack is mounted – showing the true scale of the attack. However, the results in [24] are taken from simulations that ran for 5000 seconds which is considerably longer than the simulations in this paper. With the increase of time, a higher power consumption is expected, this has been taken into consideration. With the introduction of mobility into the DIS attack, the results have been collected, as seen in Figure 3 and Figure 4 The attacking node has increased power consumption by 97% on the DIS attack from 6.496 mV to 12.8 mV. The overall power consumption has increased from the DIS attack 32% in seed one from 2.093 mV to 2.77 mV and increased 31.4% in seed 2 to from 2.166 mV to 2.847 mV. Notice from Figure 3 that node number 18 no longer has a high power consumption, this is due to the malicious node following the random walk model meaning there is a constant switching of parents as the node moves around the network spreading out DIS messages to other nodes – producing a more even spread of the power across the network. Figure 4 presents how each simulation type compares on average in terms of power consumption; the results are as expected with the DIS attack coupled with mobility consuming the most power.

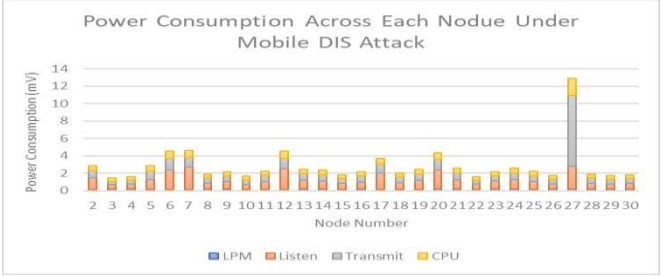

Figure 3: Power Consumption Across Nodes for Mobile DIS Attack

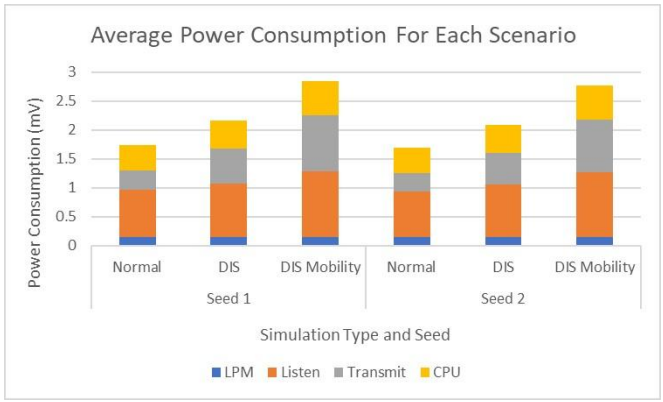

Figure 4: Comparison of Power between Static Network, DIS Attack, and Mobile DIS Attack

- **DIS Attack PDR**

The packet delivery ratio for each seed was recorded as seen in Figure 5 to understand how the attack with mobility affects how many packets are lost across the network. As reviewed previously, the DIS attack does cause high levels of network congestion due to the amount of traffic caused by the attack, meaning packet loss is expected. The PDR recorded for the testbed network is 86% and 84.5% from seed 1 and 2, respectively. The PDR recorded for each DIS attack for seed 1 and 2 are both 74%, which means a 9.3% decrease in successfully delivered packets in the most severe case compared to the testbed network. With the introduction of mobility, the packet delivery ratio suffers a further decrease in both seeds 1 and 2 with a 7% and 3.2% decrease respectively when compared against the static DIS attack. This aligns with the hypothesis constructed, but mobility does not impact packet delivery ratios as much as initially predicted. Fotohi, Ebazadeh and Seyyar [25] simulated the DIS attack in a VANET mobile architecture to determine how well the tool they created performs in protecting against DIS attacks. The results recorded shows packet delivery ratios dropped 50% when the denial of service attack was implemented when compare to the network with no attack, the simulations were performed for 400 seconds. When compared to the results collected in this paper, the researchers result show a much steeper decrease in packet delivery ratios, however both results show the trend towards the negative impact on packet delivery ratios. The results could differ due to the dissimilarities in architecture, however both topologies are dynamic.

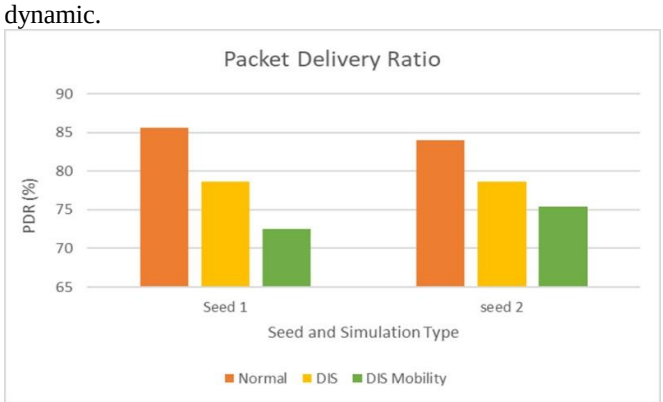

Figure 5: PDR for DIS Attacks

B. Rank Attack

From reviewing the literature, many papers fail to mention the impact the Decreased Rank attack has on energy consumption, however as there will be nodes switching parents constantly to the attacking node, we can assume that will contribute to the overall increase of power consumption. This could be the case even more so with the introduction of mobility as the attack node will attract new children as it moves around out of its own sub-DODAG. The Decreased Rank Attack falls under the category of attacks against traffic, meaning the PDR is expected to be affected profoundly. Upon reviewing Figure 6 , which shows the power consumption across each node, three nodes do not have any power consumption – nodes 10, 18, and 22. All of the mentioned nodes are located within the transmission range of the attacking node meaning they were forced to select node 27 as their parent based upon the rank advertised. Node 25 also selected 27 as a parent but was that section of the DODAG's link up to the rest of the DODAG meaning any node within the transmission range of node 27 was cut off from the rest of the network thus explaining the nodes which have no power consumption. All the traffic meant for the three cut off nodes reached node 25 and were dropped, the root node could have recognized this and tried repairs using DIO messages which explains the abnormally highpower consumption across node 25. However, the pull of node 27 was too strong for the attack to be repaired globally or locally – showing the strength and damage of the attack. The overall power consumption compared to the testbed network increased by 8.9% in seed one from 1.68 mV to 1.83 mV and decreased 5.7% in seed two from 1.74 mV to 1.64 mV. The results show that the decreased rank attack does not influence power consumption. However, it must be noted that the readings taken are missing three power consumption values from the nodes, as mentioned above, which may influence the results collected. Research was conducted with the aim of investigating the work of others concerning the effects of the decreased rank attack. However due to the decreased rank attack focusing on attacking traffic, no literature was found relating to the effects of power consumption as they were mainly interested in packet delivery ratios and other metrics.

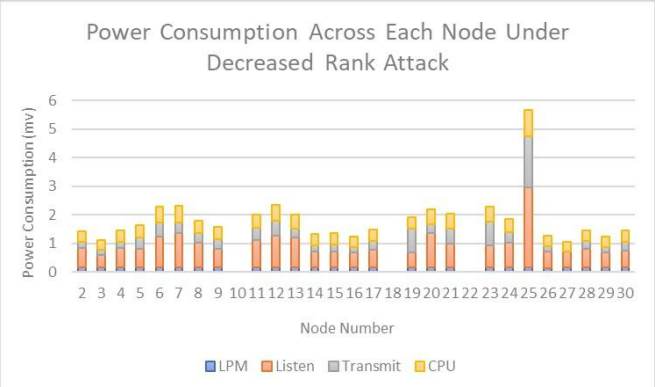

Figure 6: Power Consumption Across Nodes for Decreased Rank Attack

- **Rank Attack with Mobility**

Figure 7 shows the power consumption across each node with the mobile Decreased Rank attack mounted. Firstly, all nodes have power consumption, and this can be attributed to the introduction of mobility, as node 27 is free to move around and leave its original sub-DODAG, the nodes in the mentioned sub-DODAG are free to choose new parents who are more suitable as they are not falsely advertising rank values. The overall power consumption of the network has increased 34.4% in seed one from 1.83 mV to 2.460 mV and 49% in seed two from 1.64 mV to 2.45 mV as depicted in Figure 8. Both simulations show substantial increases in power consumption showing the true effect mobility has on an attack. This is also confirmed by reviewing the increase in power consumption for the mobile node, which is 867.4% from 1.044 mV to 10.1 mV. As previously mentioned in the paper the literature concerning mobility and attacks is very light therefore causing difficult in evaluating results against the work of others. The effects of mobility have been investigated heavily, however. The research conducted by [26] revealed when a mobile node is introduced the average power consumption was excessively high for some nodes which can be seen below in Figure 7 in respect to node 27. This is an interesting relationship showing that when the decreased rank attack is coupled with mobility, nodes can become part of the network again that were previously isolated.

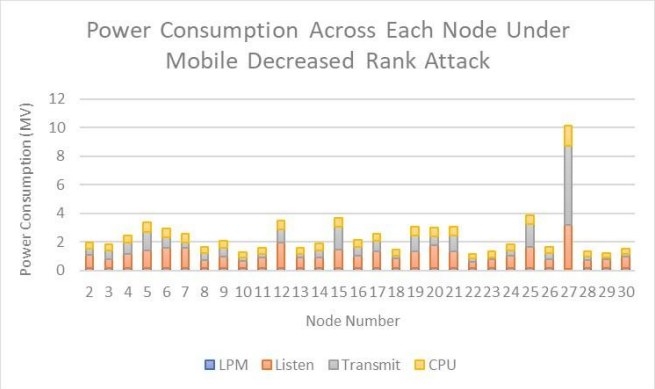

Figure 7: Power Consumption Across Nodes for Mobile Decreased Rank Attack

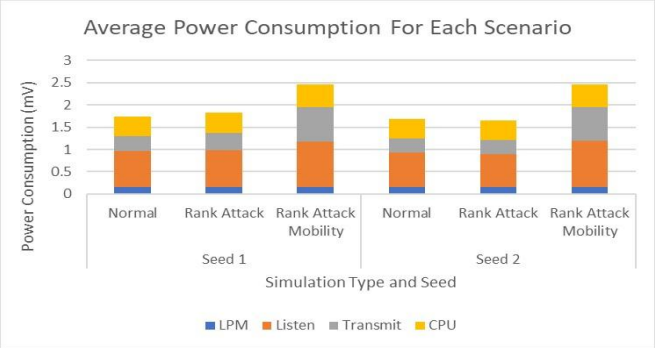

Figure 8: Comparison of Power between Static Network, Decreased Rank Attack and Mobile Decreased Rank Attack

- **Rank Attack PDR**

The Decreased Rank Attack falls under attacks on traffic, meaning the impact of the attack will focus around the downgrading of the network performance in terms of packet delivery ratios. The PDR recorded for the testbed network is 86% and 84.5% from seed 1 and 2, respectively, as shown in Figure 9. The PDR recorded for the Decreased Rank Attack is 77% and 79% from seed 1 and 2 which shows a decrease of 10.46% and 6.5% respectively.

With the introduction of the mobility node seed 1 saw a further decrease of 21% from the static rank attack and seed 2 also seen a decrease of 24.7%. Rehman et al.[13] carried out research where they investigated the effect on different objective functions in RPL while having the Decreased Rank Attack mounted. They uncovered the attack can cause packet delivery ratios to decrease from 30%-57%, dependent on the position on the attacking node. These results align with the collected results from the simulations in terms of the overall result but with a larger decrease. However, the architecture of [13] is differed greatly from this paper as they used 100 nodes with 6 packets sent per minute. The attacking node in their simulation was placed in an area of high network convergence near the sink whereas the attacking node in this paper was placed at the edge of the network – explaining the difference in decrease. The effects of the rank attack were also investigated by [27]. They simulated and collected the results of a normal network, then evaluated it against the same network with the attack mounted. The results showed the normal network had a packet delivery ratio of 97.76% whereas, during the rank attack the delivery ratio had decreased down to 92.84% which is a 5% decrease overall. The results in this paper aligned with those of Rai and Asawa works [27] meaning the attack was implemented properly and the results collected were accurate.

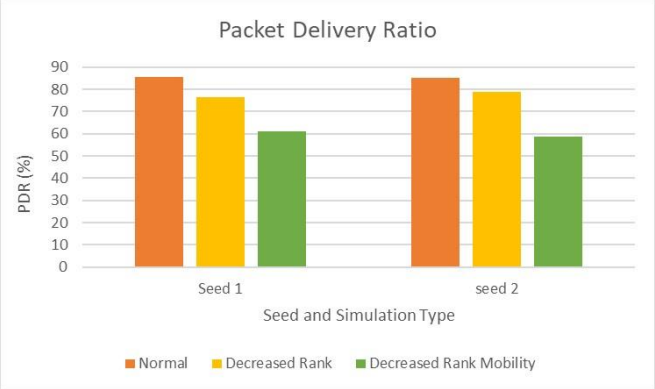

Figure 9: PDR under Rank Attack

V. CONCLUSION

It was hypothesized in this paper that the mobility of a malicious node will affect the outcome of a given attack in terms of dropped packets and power consumption in an adverse way implying a malicious mobile node is destructive for a network. We have tried to prove that through extensive simulation scenarios under different conditions. The analysis of the results above proves the hypothesis correct. For each attack, the introduction of mobility node affected the network in an adverse way in terms of power consumption and packet delivery ratios. On average, from static attack scenarios to mobile attack scenarios power consumption increased 36.7% overall, and packet delivery ratios have decreased 13.98% on average across all scenarios. Hence, it is vital to any future studies when addressing the attacks to pay more attention to the case with mobile attacks...

REFERENCES

1. S. M. Ghaleb, S. Subramaniam, M. Ghaleb, and A. M. E. Ejmaa, "An efficient group-based control signalling within proxy mobile IPv6 protocol," *Computers*, vol. 8, no. 4, 2019, doi: 10.3390/computers8040075.
2. S. M. Ghaleb, S. Subramaniam, Z. A. Zukarnain, and A. Muhammed, "Mobility management for IoT: a survey," *Eurasip Journal on Wireless Communications and Networking*, vol. 2016, no. 1. Springer International Publishing, p. 165, Dec. 11, 2016, doi: 10.1186/s13638-016-0659-4.
3. S. M. Ghaleb, S. Subramaniam, Z. A. Zukarnain, and A. Muhammed, "Load balancing mechanism for clustered PMIPv6 protocol," *Eurasip J. Wirel. Commun. Netw.*, vol. 2018, no. 1, 2018, doi: 10.1186/s13638-018-1137-y.
4. I. Yaqoob *et al.*, "Internet of Things Architecture: Recent Advances, Taxonomy, Requirements, and Open Challenges," *IEEE Wirel. Commun.*, vol. 24, no. 3, pp. 10–16, 2017.
5. S. M. Ghaleb, S. Subramaniam, Z. A. Zukarnain, A. Muhammed, and M. Ghaleb, "An efficient resource utilization scheme within PMIPv6 protocol for urban vehicular networks," *PLoS One*, vol. 14, no. 3, 2019, doi: 10.1371/journal.pone.0212490.
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. 9, no. 8, p. 794326, 2013, doi: 10.1155/2013/794326.
7. S. Stoyanov, B. Ghaleb, and S. M. Ghaleb, "A Comparative Performance Evaluation of A load-balancing Algorithm using Contiki:'RPL vs QU-RPL,'" *Int. J.*, vol. 9, no. 4, 2020.
8. B. Safaei, A. A. Mohammad Salehi, A. M. Hosseini Monazzah, and A. Ejlali, "Effects of RPL objective functions on the primitive characteristics of mobile and static IoT infrastructures," *Microprocess. Microsyst.*, vol. 69, pp. 79–91, 2019, doi: https://doi.org/10.1016/j.micpro.2019.05.010.
9. T. Winter *et al.*, "IPv6 routing protocol for low-power and lossy networks," *RFC6550 IETF*, 2012.
10. I. Zaatouri, N. Alyaoui, A. Benfradj Guiloufi, and A. Kachouri, "Performance evaluation of RPL objective functions for multi-sink," in *2017 18th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA)*, 2017, pp. 661–665.
11. B. Ghaleb, A. Al-Dubai, E. Ekonomou, M. Qasem, I. Romdhani, and L. Mackenzie, "Addressing the DAO Insider Attack in RPL's Internet of Things Networks," *IEEE Commun. Lett.*, vol. 23, no. 1, pp. 68–71, 2019.
12. B. Ghaleb *et al.*, "A Survey of Limitations and Enhancements of the IPv6 Routing Protocol for Low-Power and Lossy Networks: A Focus on Core Operations," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 2, pp. 1607–1635, 2019.
13. A. Rehman, M. M. Khan, M. A. Lodhi, and F. B. Hussain, "Rank attack using objective function in RPL for low power and lossy networks," in *2016 International Conference on Industrial Informatics and Computer Systems (CIICS)*, 2016, pp. 1–5.
14. I. Kechiche, I. Bousnina, and A. Samet, "An Overview on RPL Objective Function Enhancement Approaches," in *2018 Seventh International Conference on Communications and Networking (ComNet)*, 2018, pp. 1–4.
15. S. Shukla, S. Singh, A. Kumar, and R. Matam, "Defending Against Increased Rank Attack on RPL in Low-Power Wireless Networks," in *2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC)*, 2018, pp. 246–251.
16. G. Ma, X. Li, Q. Pei, and Z. Li, "A Security Routing Protocol for Internet of Things Based on RPL," in *2017 International Conference on Networking and Network Applications (NaNA)*, 2017, pp. 209–213.
17. S. Mangelkar, S. N. Dhage, and A. V Nimkar, "A comparative study on RPL attacks and security solutions," in *2017 International Conference on Intelligent Computing and Control (I2C2)*, 2017, pp. 1–6.
18. A. Kamble, V. S. Malemath, and D. Patil, "Security attacks and secure routing protocols in RPL-based Internet of Things: Survey," in *2017 International Conference on Emerging Trends Innovation in ICT (ICEI)*, 2017, pp. 33–39.
19. R. Mehta and M. M. Parmar, "Trust based mechanism for Securing IoT Routing Protocol RPL against Wormhole Grayhole Attacks," in *2018 3rd International Conference for Convergence in Technology (I2CT)*, 2018, pp. 1–6.
20. M. C. R. Anand and M. P. Tahiliani, "TmRPL++: Trust based smarter-HOP for optimized mobility in RPL," in *2016 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, 2016, pp. 1–6.

21. P. Perazzo, C. Vallati, A. Arena, G. Anastasi, and G. Dini, "An Implementation and Evaluation of the Security Features of RPL," in *Ad-hoc, Mobile, and Wireless Networks*, 2017, pp. 63–76.
22. A. Le, J. Loo, Y. Luo, and A. Lasebae, "Specification-based IDS for securing RPL from topology attacks," in *2011 IFIP Wireless Days (WD)*, 2011, pp. 1–3.
23. B. Farzaneh, M. A. Montazeri, and S. Jamali, "An Anomaly-Based IDS for Detecting Attacks in RPL-Based Internet of Things," in *2019 5th International Conference on Web Research (ICWR)*, 2019, pp. 61–66.
24. C. Pu, "Spam DIS Attack Against Routing Protocol in the Internet of Things," in *2019 International Conference on Computing, Networking and Communications (ICNC)*, 2019, pp. 73–77.
25. R. Fotohi, Y. Ebazadeh, and M. Seyyar, "A New Approach for Improvement Security against DoS Attacks in Vehicular Ad-hoc Network," *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 7, 2016, doi: 10.14569/ijacsa.2016.070702.
26. I. Wadhaj, I. Kristof, I. Romdhani, and A. Al-Dubai, "Performance Evaluation of the RPL Protocol in Fixed and Mobile Sink Low-Power and Lossy-Networks," in *2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing*, 2015, pp. 1600–1605.
27. K. K. Rai and K. Asawa, "Impact analysis of rank attack with spoofed IP on routing in 6LoWPAN network," in *2017 Tenth International Conference on Contemporary Computing (IC3)*, 2017, pp. 1–5.

AUTHOR PROFILE

Safwan M. Ghaleb He is currently a Senior Lecturer with the Department of Computer Science, Faculty of Ocean Engineering Technology and Informatics, Universiti Malaysia Terengganu (UMT). He received the B.Sc. degree in computer science from Jordan University, Jordan, in 2009, and the M.Sc. from Jordan University of Science and Technology, Jordan, in 2012 and Ph.D. degrees in communication technology and networks from Universiti Putra Malaysia, in July 2019, respectively. He began his pursuit in his career with the appointment at Universiti Science Islam Malaysia (USIM), Malaysia, in September 2019 as a post-doc. He has published a number of articles in high-impact factor scientific journals. His research interests include IP Mobility Management protocols, Routing Protocols and IP wireless networks, IP Networks, WSN, the IoT, and Machine Learning.