International Journal of Grid and Distributed Computing
Vol. 11, No. 8 (2018), pp.43-56
http://dx.doi.org/10.14257/ijgdc.2018.11.8.05

Analysis of Routing Attacks on RPL based 6LoWPAN Networks

Abhishek Verma[1*] and Virender Ranga[2]

[1,2]Department of Computer Engineering, National Institute of Technology, Kurukshetra, India
[1]abhiverma866@gmail.com, [2]virender.ranga@nitkkr.ac.in

Abstract

With the advancement of IPv6 support in constrained wireless nodes, the new networking paradigm has emerged which is known as the Internet of Things. This paradigm is open to many threats because of its open and constrained nature. Routing attacks are one of the major threats to the Internet of Things which aim to disrupt normal routing operations of the network. In this paper, we analyze some well-known routing attacks (Sinkhole, Blackhole, Selective forwarding, Sybil, Clone ID, HELLO flooding and Local Repair) and show their effect on network throughput. Simulation of routing attacks is done using the state-of-the-art Internet of Things simulator, NetSim tool.

Keywords: *Routing attack, 6LoWPAN, RPL, Security, Simulation, Internet of Things, NetSim*

1. Introduction

The Internet of Things (IoT) [1], as it's clear by the term itself, is a growing network of smart objects. It refers that the physical objects are capable of exchanging information with other ones. The connected smart devices use data that they have collected without any help from a human and then transfer to each other over the internet. In the modern technical world, a large number of devices are connected to the network, including smartphone, computer, tablet, cars, smart watches, Nest Smart Thermostat, Smart Bulb which contain different sensors. Things in the IoT are uniquely identifiable objects which sense the physical environment and communicate this data to the Internet. IPv6 [2] with its potentially unlimited address space can connect billion or even trillions of these devices with the IoT. IoT introduces various services such that human's routine life becomes easier. IoT is known for its scalability which comes from its open nature. It enables various smart devices to connect to existing network in just a few time. This property is because of IPv6 support provided by IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) [3], a standard which allows the devices which are heavily constrained to connect to IPv6 network in IoT. Using auto-configuration tendency of IPv6 new nodes can connect to existing IoT network easily. This attracts various insider and outsider attackers to hamper IoT network and disrupt normal routing operation. IoT is based on Low Power and Lossy Networks (LLNs) [4] in which routing is one of the major tasks as it requires a power efficient routing protocol. This problem is solved by Routing over Low Power and Lossy Networks protocol (RPL) [5]. RPL was proposed by Internet engineering task force (IETF). It suffers from loopholes which make it a very good target for attackers. The IoT requires security solutions where the communication is secured with integrity, confidentiality and authentication services. The network is protected against intrusions and disruptions. Also, the data inside a sensor node is stored in an encrypted form. Therefore, the challenge of ensuring secure communication in the IoT network needs to be addressed. The IoT network is secured with authentication and

Received (March 14, 2018), Review Result (May 10, 2018), Accepted (May 15, 2018)

ISSN: 2005-4262 IJGDC

encryption. It cannot be protected against cyber-attacks. Routing attacks have been a very powerful tool for attackers to disrupt wireless networks. These attacks completely or partially affect the network throughput which is a serious issue in case of low power and lossy networks.

IoT uses RPL protocol on its network layer. The RPL protocol is vulnerable to the routing attacks against the IoT as well as to the attacks against the Wireless Sensor Network (WSN). The devices in the IoT are resource constrained in battery power, memory and processing capability and extremely heterogeneous [6]. As IoT is globally connected thus it is much more challenging to secure the IoT. The constrained devices in the IoT are prone to attacks from wireless devices within 6LoWPAN networks and from the Internet. Therefore, a detailed analysis and simulation of such attacks against RPL are worth doing before creating a new light-weight Intrusion Detection mechanism [7] for RPL-based networks. In this paper, we have analyzed the effect of routing attacks on network throughput in IoT. We intend to develop a dataset by collecting the traces of simulated attacks which can be used for the development of effective network intrusion detection systems. In this paper we have analyzed the effect of various routing attacks on RPL networks. We investigate how the network throughput is affected by routing attacks.

1.1. Issues and Challenges in IoT

With each passing day, the internet is becoming an integral part of our lifestyle. The day is not far away from where everything from watches to transportation will be digitalized. A world is very near where possibly every physical thing will have a unique digital entity. IoT is making this possibility of future to be true. According to IDC [8], by 2020 there will be projected 30 billion connected things worldwide. IoT technology expected worth will cross $6 billion by the end of this quarter. The same can also be explained by the need of sensors in cars connectivity by 2020 which is expected to rise to 90%. But the major challenges that lie ahead are the security issues of the IoT. The protocol being used for the IoT, that is RPL, doesn't have any proper security model. There are security issues related to the IoT devices as well. The attacks are present not only on network layer but also on the application, support and perpetual layers. The perceptual layer is present on the first level of the architecture of the IoT. It consists of all the physical devices like sensors, actuators, smart devices *etc*. This layer must be preserved as the sensors are the main source of data, thus the accuracy of this layer is very important. The next layer of the architecture is the network layer. This layer is responsible for the transmission of data, thus it is one of the important layers of IoT. As its functionality is made possible by the use of the Internet in most of the cases, it is very vulnerable to attack and effects the secure transmission of data. The middle layer that is, the Support layer is responsible for the processing of the data. All the intellectual steps are taken on this layer thus, sometimes data is present even in the plain text form. Hence, security of this layer is one of the major concerns. The topmost layer, Application layer deals with the end-users or customers. Thus the responsibility of this layer is to ensure the security and privacy of the user. The enhanced security study is needed to preserve the authenticity of the layer. There are various issues on WSN of IoT like Jamming (on the Physical layer), resource exhaustion (on Data Link layer), Sybil attack, Sinkhole attack *etc.*, (on Network layer) and issues like Flooding (on Transport layer) [9].

2. Recent Work

The research by Mukrimah *et al.*, [10] on IoT gives a complete insight into the components of IoT, its vulnerabilities and how attacks take place at home appliances etc. IoT can be referred as the interconnection of devices which have sensors and contextual awareness. The main four components of IoT *i.e.*, persons, intelligent object, technological ecosystem and process. There are many security issues related to IoT in the

smart home environment, health-care and transportation domain. The reliability, confidentiality and auto-immunity are some of the criteria that are needed to be valued to ensure the security of IoT system in the smart home environment. In the smart home appliance, the access is given to only authorize users. In healthcare domain, the values to be evaluated are automatic data collection and sensing. In case of attacks in the healthcare domain, doctors may end up giving wrong treatments to the patients. There are attacks based on properties of devices like low-end device class attack and high-end class attack. Also, there are attacks based on the access level such as passive attack and active attack. The attacks like internal attacks and external attacks fall under the category of attacks based on adversary location. IoT also has attacks based on host and protocol. Pongle *et al.*, [11], presented a survey on possible attacks on IoT on top of RPL protocol. As 6LoWPAN is a compressed form of IPv6 header thus it is very easy to attack. There are many attacks possible on RPL protocol of IoT like Sinkhole attack, Wormhole attack, Black-hole attack, Sybil attack *etc*. There are many types of Denial of Service attacks (DoS) such as Alteration and Spoofing Attack which can be implemented by Local Repair attack, Rank attack etc. These attacks lead to the formation of an un-optimized path and thus attracting the network towards them. Version attack may even lead to the reduction of the delivery ration of packets by 30%. The attacks like Local Repair lead to the energy exhaustion unnecessarily. Some attacks may even lead to the formation of the loops in the path. Attacks like black-hole increase the instability of the network by increasing the number of DIO messages in the network. There are many other attacks under which this rank based protocol can possibly go down. The survey [11] is based on the simulation of IoT attacks on Cooja simulator [12]. The research by Wallgren *et al.*, [13] on the routing attacks of IoT is done on Contiki Operating System [14] which is shown on the Cooja simulator. During simulation of attacks on IoT, the re-distribution of ranks takes places. In case of routing topology failure, node or link failure the RPL protocol follows the Self-healing mechanism. In case of one node or link failure the RPL performs the local repair mechanism whereas, in case of many failures, global repair mechanism is executed in which the complete DODAG is re-built. There can be many types of inconsistencies in DODAG of RPL protocol. For example, a loop is detected in case of loop detection in the network or when a node joins the network or changing of the rank of a node within a network. To handle such inconsistencies the protocol uses the trickle timer. The trickle timer interval is large enough in case of normal functioning whereas it becomes very less in case of inconsistencies and a large number of DIO messages are sent in the vicinity. The attacks like Selective Forwarding attack, Sinkhole attack, Hello Flooding attack, and Wormhole attack fall under the category of routing attacks. There is no definite measures countermeasure these attacks. Thus, there is a need to find light-weight IDS. Medjek *et al.*, [15] presented an analytical evaluation of Sybil attacks under mobility. This was the first theoretical study by the authors and no simulation results were provided. Further Medjek *et al.*, [16] analyzed the effect of Sybil attacks using mobile nodes by simulating the environment and nodes using Cooja. They concluded that mobile Sybil nodes can disrupt the packet delivery ratio and lead to higher energy consumption. Mayzaud *et al.*, [17] studied the effect of RPL DODAG version attacks. Aris *et al.*, [18] presented an in-depth analysis of RPL version number attacks. They presented the effects of the attacks based on some network performance metrics *i.e.*, Average packet delivery ratio. Average latency, control traffic overhead and average power consumption. There have been many studies done on the analysis of the datasets used for the development of defense techniques for network-based attacks. Verma *et al.*, [19] statistical analysis of CIDDS-001 dataset have been presented. Their motive was to analyze the performance of distance based machine learning classifiers on the dataset. Tavallaee *et al.*, [20] presented the detailed analysis of KDD CUP 99 dataset. They showed the performance of various classifiers on the dataset in terms of accuracy

3. Routing Attacks Description

1. Sinkhole Attack: This attack is implemented by creating a malicious node and adding this node to the existing network. The rank of the malicious node is made such that all the network traffic is directed to the malicious node. Usually, it is assigned the next highest value possible after the gateway. The malicious node advertises a different routing path thus attacking many nearby nodes to attract the traffic. So, the malicious node can misuse those packets which were transmitted to them in any way. This attack alone can't harm the system much but when complemented with other attacks, can have adverse effects [13].

2. Blackhole Attack: Blackhole is referred as a place where incoming data is discarded in such a way that source never comes to know that information doesn't reach the destination. In the same way, in RPL protocol a node is made malicious. This malicious node drops the packets which are directed through it. This attack, when combined with the sinkhole, can have more adverse effects [13].

3. Sybil Attack: Sybil is also called as the "single node with multiple identities" attack. The malicious node can be at multiple places at the same time and it looks like an ordinary node. In other words, the malicious node shows different id at a different time, due to that other nodes will take this node as multiple nodes. This attack degrades the performance of the system [16].

4. HELLO Flooding Attack: The HELLO message is the message a node sends initially before joining the network's DODAG *i.e.*, HELLO message is DIO message. In Hello Flooding attack, the attacker sends a message with a favorable routing metrics. The malicious node in this attack introduces itself as the neighbour to many nodes. However, to some nodes trying to add to the attacker, the attacker might seem very far and the information is lost [13].

5. Clone ID Attack: In this attack, the attacker copies the ID of one logical node onto another. Thus the data which is sent to victim node is now send to malicious node. This attack is carried out to get access to a large network and data [13].

6. Local Repair Attack: The local repair attack uses the poisoning mechanism for its implementation. Attacker maliciously removes the nodes from the network. During this attack, the node makes its rank to be infinite and broadcast this message to the whole network. Now, the node which was children to that removed nodes, have to find a different parent for reaching to the root. This attack degrades the performance of the system as for every node change, the topology is to be updated [13].

7. Selective Forwarding Attack: The selective forwarding attack is a special case of Blackhole. The malicious node drops some of the packets from the incoming traffic and forwards some of them, according to the hash function applied to it. This attack disrupts the routing paths of the system [13].

4. Implementation of Routing Attacks

In this section, we present the methodology used for the implementation of various routing attacks. We have presented pseudo code for each attack. Some attacks have been coupled with another attack so as to generalize their effect on IoT network more clearly as some attacks alone don't affect network performance.

4.1. Sinkhole Attack with Blackhole Attack

For implementing Sinkhole attack with Blackhole attack on RPL protocol, we defined a macro of malicious rank and malicious node. Whenever a Network In Event takes place at Malicious Node ID, the details of the node are changed *i.e.*, the node is assigned the Malicious Rank. Now onwards, all the traffic comes to Malicious Node and all the packets coming on Malicious Node is dropped. So whenever a Network In Event takes the attack logic is executed overtime. Pseudo code of Blackhole attack is illustrated in Algorithm 1.

```
1. If event == Network_In_Event
2. then,
3. if packet == control_packet
4. then,
5. check if node == Malicious Node
6. then,
7. set rank of the current node = Malicious Rank
8. else
9. process the message
10. else
11. if node == malicious node and packet is not empty
12. then,
13. drop the message
```

Algorithm 1. Pseudo Code for Implementation of Sinkhole with Blackhole Attack

4.2. Sybil Attack with Blackhole Attack

Pseudo code for implementation of Sybil attack with Blackhole attack is illustrated in Algorithm 2.

```
1. A malicious node is taken, which is defined as a macro with its ID as well as rank.
2. Hash function is used to randomly generate the rank for the malicious node.
3. So whenever, a Network-in event takes place at Malicious Node and DIO message
is being passed, the random rank generated is assigned to the Malicious Node
4. If randomly generated rank is 1 then, we increment it because rank 1 is always of
gateway of the system.
5. If data packets are coming on malicious node then, those packets are dropped thus
decreasing the throughput of the system
```

Algorithm 2. Pseudo Code for Implementation of Sybil Attack with Blackhole Attack

4.3. Selective Forwarding Attack

Selective Forwarding Attack is a special case of Blackhole attack. In this implementation we made a node malicious node and forwarded some selective data. For selectively forwarding the data, we implemented a hash function. Hash Function is illustrated in Algorithm 3.

1. It generates a random value every time a network-in event takes place at malicious node.

2. If the randomly generated value is divisible by 2, then packet was not allowed to be forwarded. Otherwise, it was forwarded normally.

Algorithm 3. Pseudo Code of the Hash Function used in Selective Forwarding Attack

4.4. HELLO Flooding Attack

In this attack, HELLO messages are forwarded continuously by a malicious node to other nodes to show them that it is the neighbour of all the other nodes. In RPL, Hello messages are DIO messages. So for implementing the attack used methodology is shown in Algorithm 4.

1. Whenever a network-in event takes place at malicious node it keeps on forwarding DIO messages for a finite number of time.

2. In that time it will be added to the neighbour list of other nodes.

Algorithm 4. Pseudo Code of HELLO Flooding Attack

4.5. Local Repair Attack

In this attack the rank of node is made infinity such that children have to find the new parent. In this attack to avoid the situation where all the nodes' rank become Infinity, the rank and ID of previous node are stored. Initially there are null values in previous node ID and rank. So whenever a network-in event takes place the attack logic is executed. Pseudo code of Local Repair attacks is illustrated in Algorithm 5.

4.6. Clone ID Attack

In this attack, the ID of a node is cloned with another ID. Pseudo code of Clone ID attack is depicted in Algorithm 6.

1. if event == NETWORK_IN_EVENT
2.then,
3. if packets == control packets and are DIO messages
4. then,
5. if previous node is not null
6. then,
7. ID and rank of previous node are restored to its previous values
8. The rank and ID of current are stored in prev_node_id and prev_node_rank respectively.
10. The rank of current node is changed to INFINITY.
11. if packets == data packets and current node has rank == INFINITY
12. then, drop the message

Algorithm 5. Pseudo Code of Local Repair Attack

1. A node is made malicious node and whenever a network-in event takes place at this node, the ID of this malicious node is cloned with a another node.

2. This attack creates confusions in the network. This attack results in the changing of rank of both malicious node as well as with whom the malicious node is being cloned.

Algorithm 6. Pseudo Code of Clone ID Attack

5. Simulation Results and Description

The simulation is done on the Desktop computer having Intel(R) 7700 CPU (clock speed of 3.60GHz) with 8GB main memory. The tool used for the simulation of routing attacks is done using NetSim v10.0 [21]. Results have been presented in the form of link throughput graphs to show the clear effect of attacks on the simulated 6LoWPAN network. All the graphs depict throughput (Mbps) on the y-axis and time (ms) on the x-axis. Various link used in the simulated topology as considered for the analysis. Network topology considered for the analytical study is shown in Figure 1.

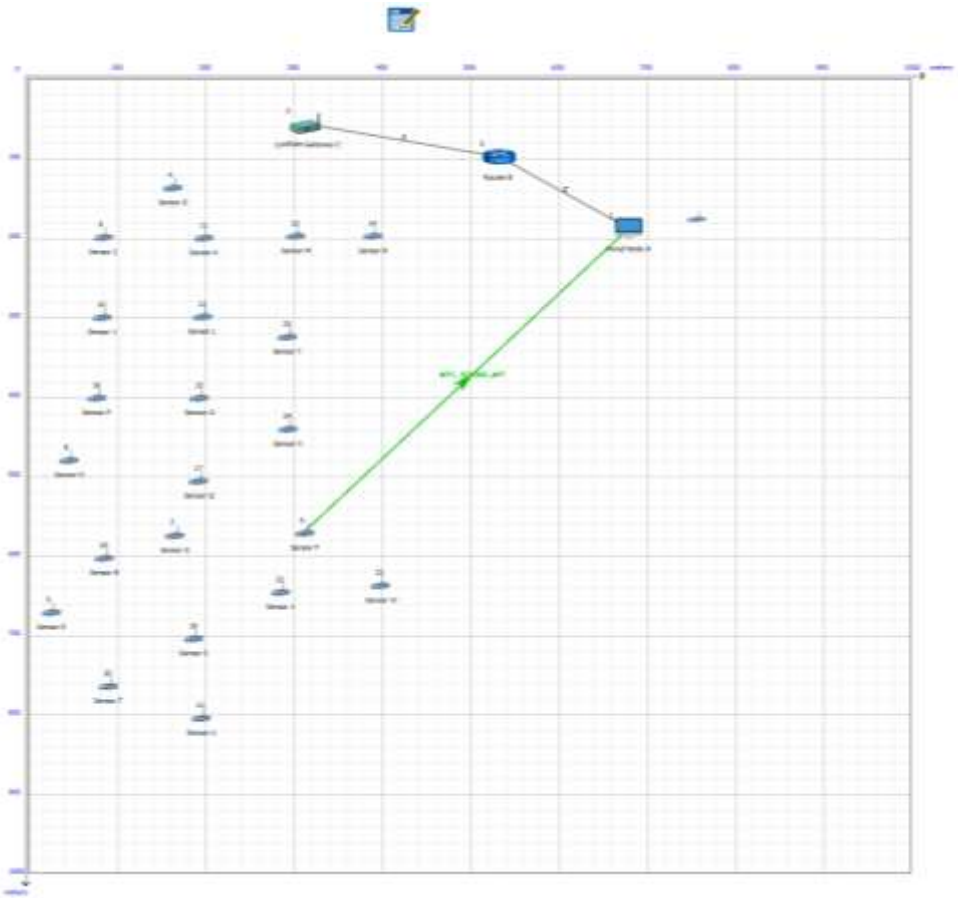

Figure 1. IoT Network Topology for Analytical Study

5.1. Normal Scenario

In Normal Scenario, there will be no malicious node, so initially throughput will increase because of increase in transmission of control data packets which will further decrease with time because number of control packets transmitted decreases as topology becomes stable. The effect of this scenario is illustrated in Figure 2. Initially there is a sudden rise in network throughput and then it goes on a stable state further. This increase is due to initial broadcast of control messages for setting up topology. Once the topology is setup the throughput decreases and comes to a stable state.

Figure 2. Link Throughput in No Attack Scenario

5.2. Network Throughput in Case of Sinkhole and Blackhole Attack

In Sinkhole attack, a malicious node modifies it rank to be the fake destination and when data packets are transmitted to this malicious node, it will drop the packets which in turn will drop the packets due which leads to decrease in throughput with time. In the Link_1_Throughput graph, Throughput is lesser as compared to original one. The scale of throughput is of the order of 10^{-4}. In the normal scenario it is of the order of 10^{-3}. The effect of this attack is shown in Figure 3.

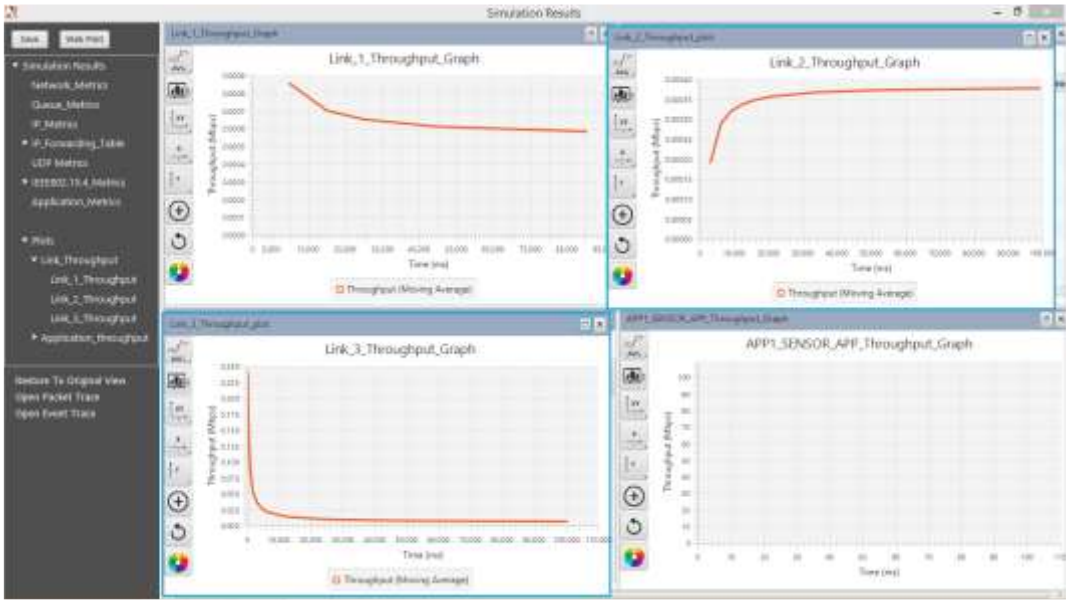

Figure 3. Link throughput in Sinkhole with Blackhole Attack Scenario

5.3. Network Throughput in Case of Clone ID Attack

In Clone ID, Malicious nodes clone the details of other nodes, so that it can get access to data packets of that network and use those data packets for malicious activities which in turn will decrease the throughput. In the Link_1_Throughput graph, Throughput is

lesser as compared to original one. The scale of throughput is of the order of 10^{-4}. In the normal scenario it is of the order of 10^{-3}. The effect of this attack is presented in Figure 4.

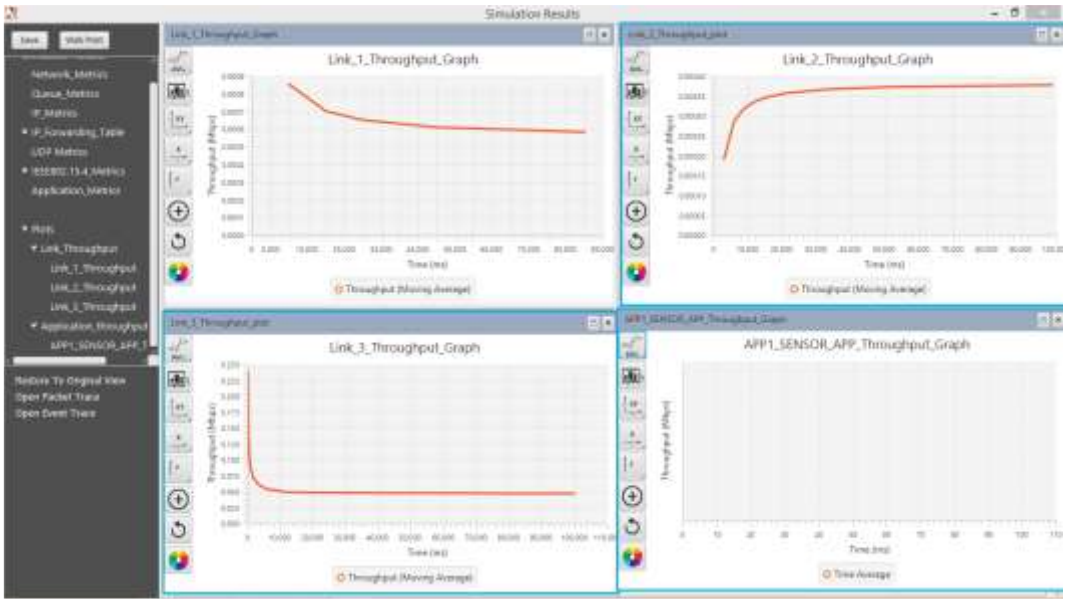

Figure 4. Link Throughput in Clone ID Attack Scenario

5.4. Network Throughput in Case of HELLO Flooding Attack

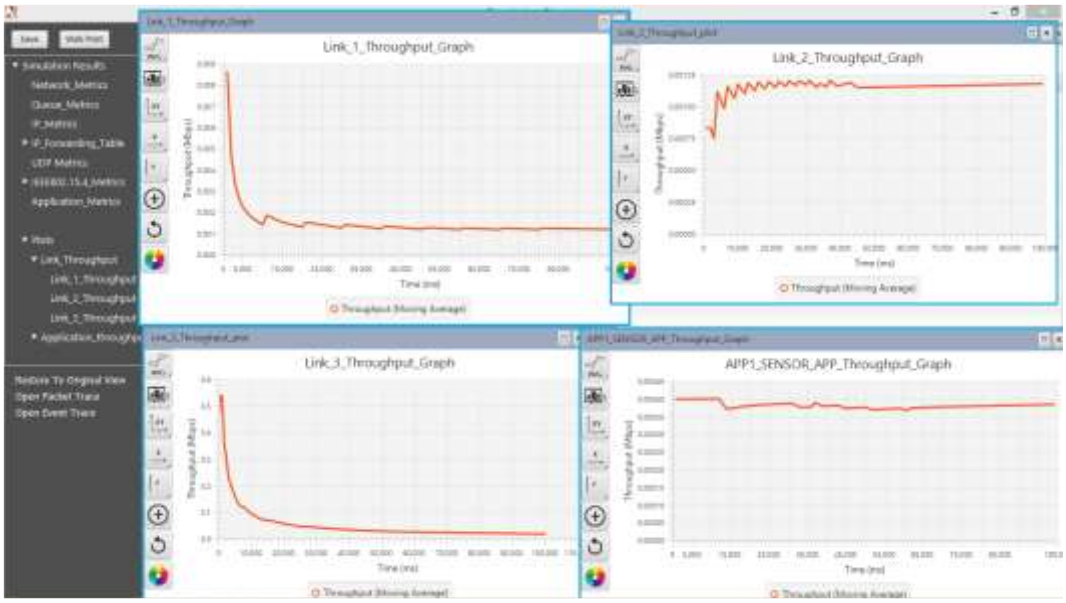

Figure 5. Link Throughput in HELLO Flooding Attack Scenario

In Hello Flooding Attack, throughput is decreasing because data and control packets are not transferred to the destination because of the over flooding of Hello Messages or DIO Control Messages in RPL transmitted by Malicious Node and throughput curve is very steep in this case. On Link_3_Throughput Graph initially throughput decreases at lower rate than the original one due to increase in the DIO message (Hello Message Flooding). The effect of this attack is presented in Figure 5.

5.5. Network Throughput in Case of Selective Forwarding Attack

Figure 6. Link Throughput in Selective Forwarding Attack Scenario

In Selective Forwarding, Malicious node transmits only some selective data packets because of which there is constant drop of data packets from Malicious node in the network and this is the reason for very steep curve in throughput of Selective forwarding. The effect of this attack is shown in Figure 6.

5.6. Network Throughput in Case of Sybil Attack

In Sybil attack, a node pretends to be many nodes by transmitting different ranks to other nodes which will decrease the throughput because of unnecessary data packets transmission that is why throughput is decreasing in the above plot. In the Link_1_Throughput graph, Throughput is lesser as compared to original one. The scale of throughput is of the order of 10^{-4}. In the normal scenario it is of the order of 10^{-3}.and due to unnecessary packet transmission Link_3_Throughput is increasing. The effect of this attack is displayed in Figure 7.

5.7. Network Throughput in Case of Local Repair Attack

In Local Repair when rank is changed to infinity, the nodes find a new parent and this requires the resource exhaustion and thus, decreases the throughput. In the Link_1_Throughput graph, Throughput is lesser as compared to original one. The scale of throughput is of the order of 10^{-4}. In the normal scenario it is of the order of 10^{-3}. The effect of this attack is illustrated in Figure 8.

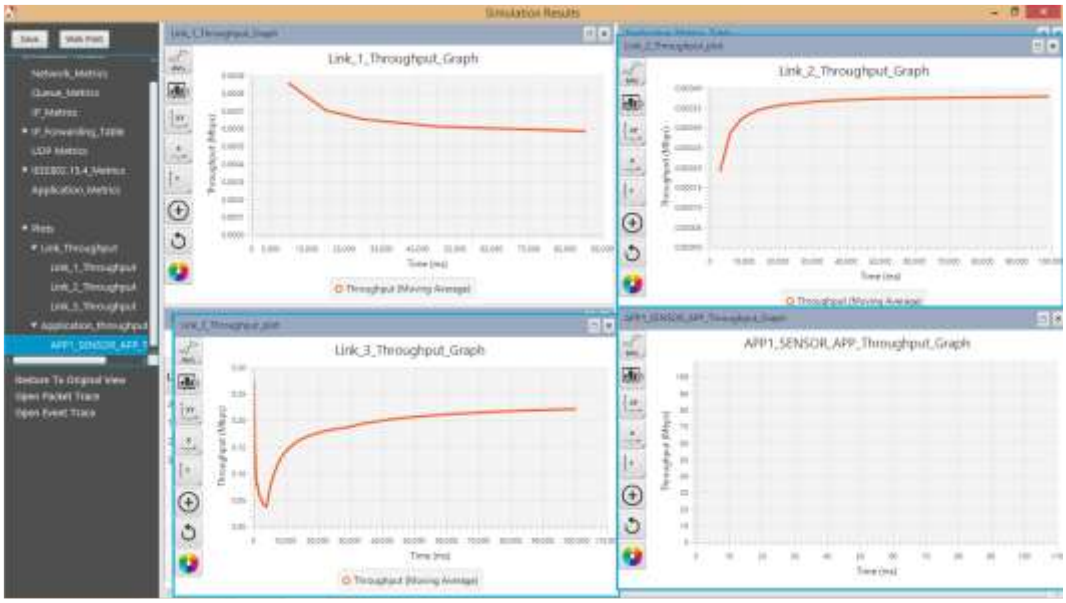

Figure 7. Link Throughput in Sybil with Blackhole Attack Scenario

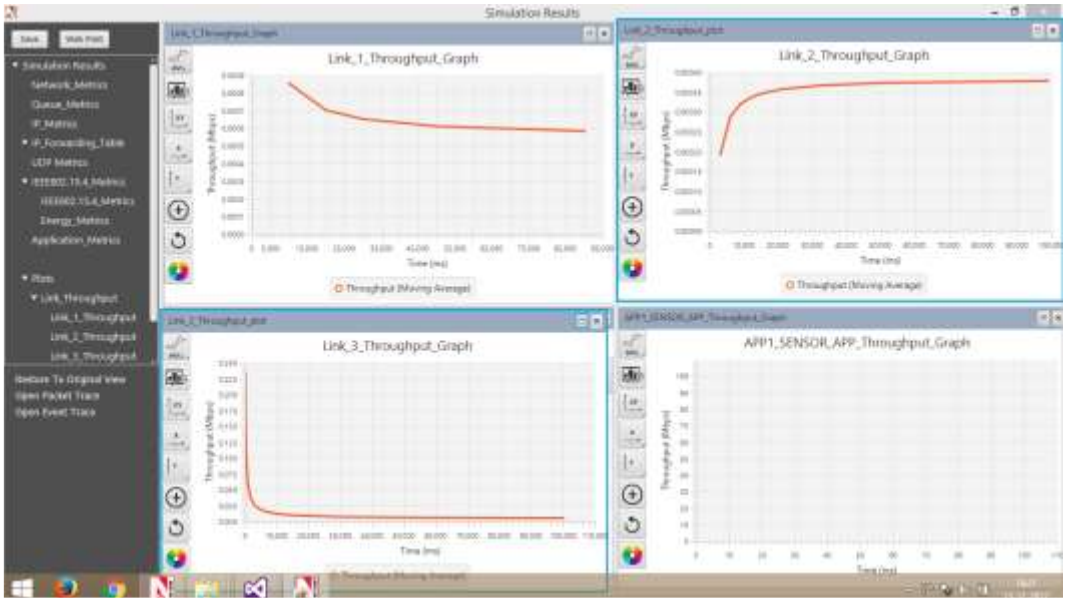

Figure 8. Link Throughput in Local Repair Attack Scenario

6. Conclusion and Future Work

In this paper, the effect of various routing attacks on the 6LoWPAN network is analyzed. It can be concluded from the simulation results that routing attacks disrupt network throughput badly. Hence, the increasing number of attacks on the Internet of Things may disrupt the whole network of smart devices. We need to have a defense system that detects the attacks major routing attacks like Sinkhole, Blackhole, Selective Forwarding, Sybil and Clone ID etc. Traditional Intrusion Detection Systems are heavy-weight and thus unsuitable to be used for Internet of Things security. Our future work includes to the creation of a network intrusion traffic dataset for the evaluation of Network Intrusion Detection Systems for 6LoWPAN networks and develops a collaborative lightweight hybrid network Intrusion Detection System to detecting routing and Distributed Denial of Services attacks on the Internet of Things.

References

[1] L. Atzori, A. Iera and, G. Morabito, "The internet of things: A survey", Computer networks, vol. 54, no. 15, **(2010)**, pp. 2787-2805.
[2] S. E. Deering, "Internet protocol, version 6 (IPv6) specification", IEEE, **(1998)**.
[3] Z. Shelby and C. Bormann, Editor, "6LoWPAN: The wireless embedded Internet", John Wiley & Sons, **(2011).**
[4] J. Ko, A. Terzis, S. Dawson-Haggerty, D. E. Culler, J. W. Hui and P. Levis, "Connecting low-power and lossy networks to the internet", IEEE Communications Magazine, vol. 49, no. 4, **(2011)**.
[5] T. Winter, "RPL: IPv6 routing protocol for low-power and lossy networks", IETF, **(2012)**.
[6] L. Mainetti, L. Patrono and A. Vilei, "Evolution of wireless sensor networks towards the internet of things: A survey", Proceedings of the 19th International Conference on Software, Telecommunications and Computer Networks (SoftCOM), Split, Croatia, **(2011)** September 1-6.
[7] G. Helmer, J. S. Wong, V. Honavar, L. Miller and Y. Wang, "Lightweight agents for intrusion detection", Journal of systems and Software, vol. 67, no. 2, pp. 109-122, **(2003)**.
[8] V. Turner, C. MacGillivray and P. Gorman, "Connecting the IoT: The Road to Success", https://www.idc.com/infographics/IoT, **(2017)**.
[9] A. Mayzaud, R. Badonnel and I. Chrisment, "A Taxonomy of Attacks in RPL-based Internet of Things", International Journal of Network Security, vol. 18, no. 3, pp. 459-473, **(2016)**.
[10] M. Nawir, A. Amir, N. Yaakob and O. B. Lynn, "Internet of Things (IoT): Taxonomy of security attacks", Proceedings of 3rd International Conference on Electronic Design (ICED), Phuket, Thailand, **(2016)** August 321-326.
[11] P. Pongle and G. Chavan, "A survey: Attacks on RPL and 6LoWPAN in IoT", Proceedings of International Conference on Pervasive Computing (ICPC), Pune, India, **(2015)** January 1-6.
[12] F. Osterlind, A. Dunkels, J. Eriksson, N. Finne and T. Voigt, "Cross-level sensor network simulation with cooja", Proceedings of 31st IEEE conference on Local computer networks, Tampa, FL, USA, **(2006)** November 641-648.
[13] L. Wallgren, S. Raza and T. Voigt, "Routing Attacks and Countermeasures in the RPL-based Internet of Things", International Journal of Distributed Sensor Networks, vol. 9, no. 8, 794326, **(2013)**.
[14] A. Dunkels, B. Gronvall and T. Voigt, "Contiki-a lightweight and flexible operating system for tiny networked sensors", Proceedings of 29th Annual IEEE International Conference on Local Computer Networks, Washington, DC, USA, **(2004)** November 455-462.
[15] F. Medjek, D. Tandjaoui, I. Romdhani and N. Djedjig, "Performance Evaluation of RPL Protocol under Mobile Sybil Attacks", Proceedings of Trustcom/BigDataSE/ICESS, Sydney, Australia **(2017)** August 1049-1055.
[16] F. Medjek, D. Tandjaoui, M. R. Abdmeziem and N. Djedjig, "Analytical evaluation of the impacts of Sybil attacks against RPL under mobility", Proceedings of 12th International Symposium on Programming and Systems (ISPS), Piscataway, New Jersey, **(2015)** April 1-9.
[17] A. Mayzaud, A. Sehgal, R. Badonnel, I. Chrisment and J. Schonwalder, "A study of RPL DODAG version attacks", Proceedings of IFIP international conference on autonomous infrastructure, management and security, Berlin, Heidelberg, **(2014)** June 92-104.
[18] A. Aris, S. F. Oktug and S. B. O. Yalcin, "RPL version number attacks: In-depth study", Proceedings of Network Operations and Management Symposium (NOMS), Krakow, Poland, **(2016)** April 776-779.
[19] A. Verma and V. Ranga, "Statistical analysis of CIDDS-001 dataset for Network Intrusion Detection Systems using Distance-based Machine Learning", Procedia Computer Science, vol. 125, pp. 709-716, **(2018)**.
[20] M. Tavallaee, E. Bagheri, W. Lu and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set", Proceedings of IEEE Symposium on Computational Intelligence for Security and Defense Applications, Ottawa, ON, Canada, **(2009)** July 1-6.
[21] NetSim Simulator and Emulator, http://www.tetcos.com/netsim-std.html, **(2018)**.

Authors

Abhishek Verma, he received the B.Tech degree in Computer Science & Engineering in 2014 from UPTU, Lucknow, India and M.Tech degree in Computer Engineering in 2016 from National Institute of Technology, Kurukshetra, India. Currently, he is working towards the PhD degree at the Department of Computer Engineering, National Institute of Technology, Kurukshetra, India. His research interests include Wireless Sensor Networks, Internet of Things security and Machine Learning.

Virender Ranga, he received his PhD degree in 2016 from Computer Engineering Department of National Institute of Technology, Kurukshetra, Haryana, India. He has published more than 40 research papers in various International SCI Journals in the area of Computer Communications as well as reputed International Conferences. Presently, he is Assistant Professor in the Computer Engineering Department since 2008. He has been conferred by Young Faculty Award in 2016 for his excellent contributions in the field of Computer Communications. He has been acted as a member of TPC in various International conferences of repute. He is a member of editorial board various reputed journals like Journal of Applied Computer Science & Artificial Intelligence, International Journal of Advances in Computer Science and Information Technology(IJACSIT), Circulation in Computer Science (CCS), International Journal of Bio-Based and Modern Engineering (IJBBME) and International Journal of Wireless Networks and Broadband Technologies. Currently, he has been selected Guest Editor for a special issue to be published in International Journal of Sensors, Wireless Communications and Control (Bentham Science Publication) He is an active reviewer of many reputed journals of IEEE, Springer, Elsevier, Talyor & Francis, Wiley and InderScience. His research area includes Wireless Sensor & Adhoc Networks, IoT security, and FANET security.