Case Study of a Black Hole Attack on 6LoWPAN-RPL

Karishma Chugh
Engineering and Information Science
Middlesex University
London, UK. NW4 4BT
karishma.chugh@ymail.com

Aboubaker Lasebae
Engineering and Information Science
Middlesex University
London, UK. NW4 4BT
a.lasebae@mdx.ac.uk

Jonathan Loo
Engineering and Information Science
Middlesex University
London, UK. NW4 4BT
j.loo@mdx.ac.uk

***Abstract*—This paper throws light on shortcomings of the Contiki Operating system and ContikiRPL routing protocol, which may lead to an easy injection of malicious activity similar to black hole attack in wireless sensor network. Contiki and ContikiRPL are components for microcontroller devices belonging to the 6LoWPAN group and Internet of Things (IoT). Directed acyclic graph Identification Object (DIO) packets are a part of routing metrics and form an integral part of ContikiRPL. Increased number of DIO messages reflect instability in the network routing topology and their decreasing frequency reflects stable network. In unstable networks, re-formation of path for data packets is initialised by RPL. In this case study it was found that malicious nodes, which continue to send self-generated data packets cause an increase in the number of DIO messages exchanged between nodes while malicious nodes, which supress self-generated data packets are able to disguise the instability of network by having no effect on the number of DIO messages or packet delay. Scenario with malicious node sending self-generated data packets showed 8% increase in total number of DIO packets exchanged amongst nodes while scenario with malicious node not generating any data packets had less number of DIO messages exchanged thus falsely presenting a stable network topology. It was also found that data packets suffer delay in presence of malicious activity in the network. Data packets generated by malicious nodes were 4.3 times higher delayed as compared to data packets from their counterparts in clear network. Data packets from non-malicious nodes also suffered considerably higher delay. Thus, increased packet delay and increase in exchange of DIO messages can be treated as preliminary indicators of malicious activity but more concrete parameters are required to identify malicious nodes. This case study may be helpful in designing an effective defense system against known attacks on wireless sensor networks.**

Keywords- *IoT; 6LowPAN; Contiki; RPL; ContikiRPL; Wireless sensor network; Black hole attack.*

I. INTRODUCTION

Internet of Things (IoT) is a network of billions of small and big communicating devices. Wireless sensor networks are a subset of IoT. Devices in wireless sensor networks are small sensor nodes, having power and memory constraints and ad-dressed using Internet Protocol version 6 (IPv6) [2]. Sensor nodes communicate with each other as per specifications provided by IEEE 802.15.4 [2]. Protocols corresponding to physical and data link layer are specified in IEEE 802.15.4. Specialised task group formed by Internet Engineering Task Force (IETF) has defined header compression and framing technique to facilitate communication between sensor nodes using IPv6 over a network of low power and low rate devices. This group is called 6LoWPAN [1][2]. Specialised operating systems and routing protocols have been designed and implemented to facilitate communication between sensor nodes as per 6LoWPAN specification. Contiki [7] operating system is one such open source operating system. Contiki provides a multi-threaded, event based multi-tasking environment [7][8]. Routing protocols are important building block for communication in any network. Routing for low Power and Lossy networks (RPL) protocol has been designed to support cost effective routing over low power and lossy networks (LLN) [9]. ContikiRPL is one of the many implementations of RPL. Black hole attack [10] in a network would imply that one or more malicious nodes would partially or fully drop data packets being routed through it causing disruptions in the normal data flow in the network. Malicious node advertises itself as the best route towards the control node (called sink node) just like other sensor nodes. Some nodes (sender nodes) select the malicious node as their parent node (next in line node in the routing topology) and start forwarding their data packets; these data packets are then dropped [3]. Securing IoT, especially sensor network is essential. This required detailed understanding of the functioning as well as shortcomings of various building blocks of the network such as operating system, device properties and routing mechanism.

This work would strengthen the knowledge of various forms of attacks, their effect on wireless sensor network, parameters to facilitate identification of attack and attacking nodes, and ultimately help introduce a strong defence system. Section II explains the simulated environment of the study and the parameters, which are observed. Section III tabulates the findings from the logs obtained as a result of the simulation. Section IV elaborates the observations and helps draw a conclusion by connecting them to the known behaviour of the system. Section V concludes the results obtained from the case study. Finally, Section VI tries to give directions towards elaborating the work for more detailed analysis of attacks on sensor networks.

 ISBN: 978-1-61208-209-7

II. METHODOLOGY

Certain features of Contiki and ContikiRPL are exploited to simulate and monitor malicious behaviour in this work. Contiki deals with each type of data packet differently. Each node processes data packets, which are generated by other node but routed through it in a different manner than processing self-generated data packets. In order to simulate malicious activity, modifications are made in contiki OS such that data packets from neighbouring nodes are completely dropped by the malicious node. Malicious node continues to take part in the route formation by sending consistent DIO packets. This ensures that nodes are live and continue to advertise themselves to neighbours. Malicious sensor nodes may or may not continue to send data packets generated by itself [4]. DIO messages are an integral part of RPL and play a critical role in formation of a topology. They contain metrics, which is used by nodes to form a route. Number and frequency of DIO messages decrease as the route stabilises [4][5][6]. A light weight simulator called Cooja is used to monitor the network under various scenarios. All signal messages are collected in the Log Listener plug-in of Cooja and used for analysis. Parameters under observation are packet delay, packet delivery fraction and rate of a specific control message called the DIO message. There are three types of scenarios created to record and compare the above stated parameters. First scenario called Clear Network is free from any malicious activity and consists of 1 sink node and 10 sender nodes. Sender nodes were randomly placed covering a large distance. Figure 1 shows sink node (ID: 1) and its position with respect to other sender nodes. Highlighted area denotes the radio coverage of sink node. Cooja offers different types of radio coverage; standard radio coverage with default values is used for this case study. Nodes are randomly placed covering all sides of the sink node. Some nodes fall in direct range of sink node while others fall out of it and data packets from nodes outside direct radio coverage reach the sink node via other neighbouring nodes. The second scenario has one of the sender nodes randomly selected out of the 10 sender nodes to behave in a malicious way. Node 5 from Figure 1 is replaced by a new node (ID: 12) with malicious activity. All data packets from neighbouring nodes destined to sink node were dropped by this malicious node, which continues to send data packets generated by itself towards the sink. Third scenario had malicious node, which took part in route formation but did not sent any self-generated data packets across the network. Malicious node in scenario 2 (ID: 12) was replaced by modified malicious node (ID: 13) in scenario 3. Relative location of all nodes remains same across scenarios. Malicious nodes in second and third scenario are active nodes as they exchanges DIO messages and takes part in route formation. Scenario 2 represents selective forwarding attack. Selective forwarding is a special case of black hole attack where some data packets are dropped while others are forwarded successfully. Scenario 2 forwards self-generated data packets and drops data packets from other nodes. Scenario 3 represents complete black hole attack where none of the data packets are forwarded. Simulation in each scenario is allowed to execute for 25,000 seconds during which nodes are allowed to exchange data and control information. Clear network scenario serves as a benchmark and would help understanding deviation in values of selected parameters obtained from other scenarios. Effect of malicious activity on delay of data packets reaching the sink node is analysed. Increase in packet delay can serve as an indicator of presence of attacking nodes. Also, packet delay of data packets originating from Node 12 (malicious node) in scenario 2 is compared to delay of data packets from its counterpart node (ID:5) in clear network scenario. This would help indicate effect of malicious behaviour on delay suffered by data packets from malicious node itself thus helpful in identification of malicious node in an attacked network. Scenarios 2 and 3 are compared to scenario 1 in terms of frequency of DIO messages. This helps to identify if malicious activity have an effect on exchange of DIO messages. Count and frequency of DIO messages indicates route stability. Packet delivery fraction (PDF) is another parameter, which is monitored to check if values in PDF deviate significantly and if it can be used to identify possibly attacked networks.

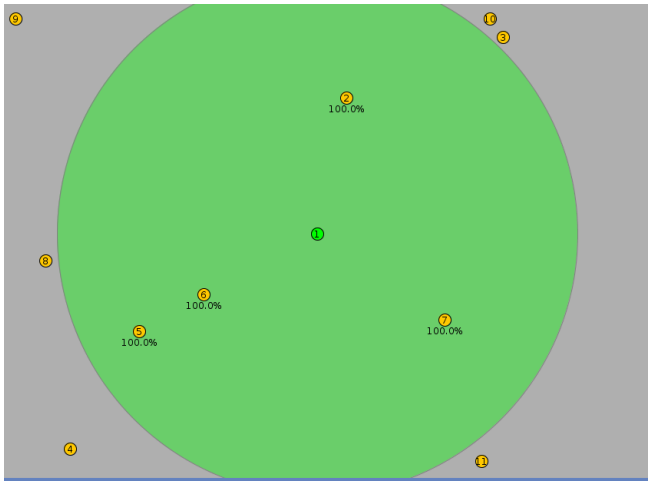

Figure 1. Placement of Sensor nodes w.r.t. Sink Node

III. OBSERVATION

Number of DIO messages sent by each sender node and time at which each of these was released, was recorded. Time of DIO message sent helps calculate and analyse the frequency of DIO messages. Number of DIO messages released by nodes across scenarios are summarised in Table 1. Increase in the number of DIO messages exchanged is a

 ISBN: 978-1-61208-209-7

Table I
DIO PACKETS RELEASED IN SCENARIOS

Node	Scn-1	Scn-2	Scn-3
2	61	68	64
3	69	72	72
4	69	77	70
5/12/13	62	78	58
6	62	63	64
7	66	65	68
8	64	88	63
9	77	87	71
10	69	65	63
11	73	70	70

Table II
SUMMARY OF TOTAL CONTROL MESSAGES RELEASED IN A SCENARIO

Scenario No.	Scenario 1	Scenario 2	Scenario 3
Total DIO Messages	674	733	663
% Increase w.r.t. 1	Benchmark	+8.75%	-1.63%

direct indicator of instability in the routing topology. DIO messages released per node show that whether each node had knowledge of network instability and whether those nodes were attempting to stabilise the network by sending their own DIO packets or not. Clear network scenario would serve as a benchmark for the other two scenarios. Table 2 shows the results of this analysis. Increasing the granularity of this analysis, table 3 tabulates the number of DIO messages released by each individual node. Node 12 is the malicious node in scenario 2 and node 13 is the malicious node in scenario 3. Nodes 8 and 9 are the affected nodes in both scenarios 2 and 3. Node 4 is affected only in scenario 3. Node 5 is the counterpart of node 12 and 13 and is present in clear network scenario alone. Table 4 presents the extract of the log where node 4 in scenario 3 is trying to find a stable parent for its data packets. Figure 2 shows the neighbouring nodes of node 4 in scenario 3. This extract from the log helps explain that malicious nodes suppressing self-generated data packets have better routing metrics thus would be preferably chosen by other nodes as preferred parent. Delay of packets was monitored to analyse whether increase in packet delay could be treated as an alarm for presence of malicious activity. Delay of packets originating from malicious nodes was analysed separately and delay for data packets from non-malicious nodes was done separate. Table 5 tabulates the delay of packets from node 12 in scenario 2 and compares it to data packets from a healthy node i.e., node 5 from scenario 1. Malicious node from scenario 3 is not considered in calculation of packet delay as malicious node in scenario 3 does not generate any data packets of its own. Table 6 shows delay of data packets from all nodes in all scenarios. Entries with infinity imply that none of the data packets of

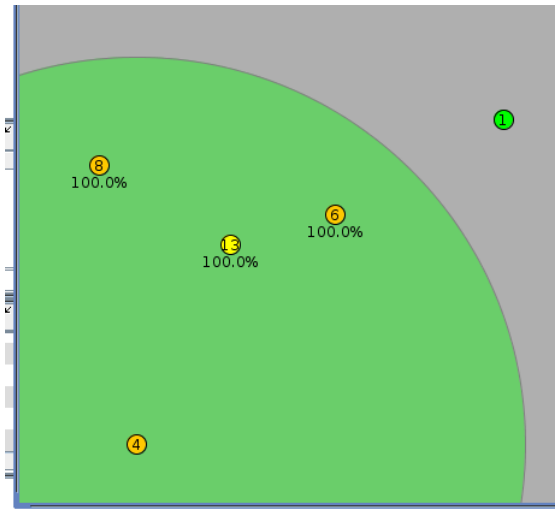

Figure 2. Node 4 and Neighbours

Table III
SUMMARY OF DIO MESSAGES RELEASED BY MALICIOUS AND AFFECTED NODES ALONE

	5/12/13	Node 4	Node 8	Node 9
Sc 1	62	69	64	77
Sc 2	78	77	88	87
sc 3	58	70	63	71

that particular node reached their destination. Packet delivery fraction is the ratio of number of data packets sent from all nodes to number of data packets received successfully at sink. Table 7 tabulates the total number of data packets received at sink and those sent by nodes across scenarios.

Table IV
EXTRACT FROM LOG FILE: PREFERRED PARENT FOR NODE 4

Node Id	Remarks	Time(ms)
ID:4	The preferred parent is Node 13	27624
ID:4	The preferred parent is Node 6	43351
ID:4	The preferred parent is Node 13	48695
ID:4	The preferred parent is Node 13	52562
ID:4	The preferred parent is Node 13	91360
ID:4	The preferred parent is Node 13	157143

Table V
AVERAGE PACKET DELAY FOR NODE 5 AND 12 IN SCENARIO 1 & 2 RESPECTIVELY

Scenario No.	Packets Sent	Packets Recvd	Delay(ms)
Node 5 in Scenario 1	416	416	4081.77
Node 12 in Scenario 2	416	346	17557.91

 ISBN: 978-1-61208-209-7

Table VI
DELAY IN MS FOR PACKETS FROM NON-MALICIOUS NODES

Node No.	Scenario 1(ms)	Scenario 2(ms)	Scenario 3(ms)
2	3481.25	4694.31	4291.95
3	4053.11	57222.43	4443.84
4	4651.91	14927.13	Infinity
6	4045.55	4734.45	3800.53
7	4013.45	4068.08	4795.66
8	3881.56	Infinity	Infinity
9	48298.87	Infinity	Infinity
10	3354.77	3505.75	3917.08
11	9898.37	49145.86	43700.46

Table VII
PACKET DELIVERY FRACTION ACROSS SCENARIOS

Scenario No.	Packets Sent	Packets Recvd	Lost %
Scenario 1	4160	4155	0.12%
Scenario 2	4160	3249	21.9%
Scenario 3	3744	2492	33.4%

IV. ANALYSIS AND RESULT

As per the working of ContikiRPL routing protocol, various control messages are exchanged between sender nodes and sink nodes to form a topology. DIO messages are formed when nodes send and receive control information from each other. Round trip time (RTT) of these control packets helps identify distance from neighbours and hop count of control packets from sink is instrumental in determining nodes own relative position to sink node. Once the topology is deemed stable, the frequency of DIO messages decrease.

Analysing the rate and frequency of DIO messages released by nodes in various scenarios, it is evident that due to malicious activity introduced by node 12 in scenario 2, all the nodes experienced unstable network topology. Scenario 2 experienced an overall increase in the number of DIO messages. Data plotted in Figure 3 shows that all nodes in scenario 2 released higher number of DIO messages when compared to clear network scenario. In scenario 3, total number of DIO messages released during the simulated time was lower than those released in scenario 1 and 2. This indicates that despite malicious node in scenario 3 dropping all data packets from its neighbours, there was no effect on the perception of other nodes, which presumed that the network was stable. This lead to the rate of DIO messages being closely comparable to rate of DIO packets in clear network scenario. This argument is further supported by Figure 4, which shows that it took much longer time for Node 5 in scenario 1 to release the same number of DIO messages than its counterpart malicious node in scenario 2; and even longer for malicious node in scenario 3. Considering the DIO messages by one of the nodes, node 8 selected malicious node as its parent in scenario 2 as well as in scenario 3. First 50 DIO messages were released in a very short span of time in scenario 2 as compared to the same first 50 DIO messages in scenario 1 and 3. Figure 5 illustrates this observation. Another important aspect noticed was the selection of preferred parent by node 4. Parent is selected on the basis of metrics extracted from DIO messages. Malicious node in scenario 3 was successful in advertising itself as preferred parent. Table 4 elaborates on the above stated fact. Table 4 shows that node 4 did consider non malicious node with ID: 6 as its preferred parent but soon changed back to malicious node 13. This implies node 13 in scenario 3 offered better routing metrics as compared to its competitive node 6 in the same scenario. Also, node 13 showed better route metrics than nodes 5 and 12 of scenario 1 and 2 respectively. Figure 2 shows nodes in direct range of node 4 available to be selected as preferred parent. This further confirms the argument that malicious node of scenario 3 was successful in performing undetected harmful activities.

Table VIII
PDF ACROSS SCENARIOS FOR NON-AFFECTED NODES

Scenario No.	Packets Sent	Packets Recvd	Lost %
Scenario 1	4160	4155	0.12%
Scenario 2	3328	3249	2.37%
Scenario 3	2496	2492	0.16%

In terms of delay, data packets from malicious node in scenario 2 (Node 12) suffered much higher delay than its corressponding node in scenario 1. The data is tabulated in table 5. Delay in packets of node 12 is around 4.3 times higher than its counterpart node 5 of scenario 1. Increased packet delay was not restricted to data packets from malicious nodes alone. Non malicious packets placed far or near to the malicious node also experienced higher delay in scenario 2. As shown in table 6, all nodes in scenario 2 suffered a much higher delay compared to other scenarios. Reason behind packet delay could be buffer queues. Packets might have been in the queue waiting to be processed while sink node was generating and processing DIO packets, and attempting to stabilise the network topology, longer waiting times result in an expired packet based on time to live (TTL). Since network was deemed stable in scenario 3, packet delay for most of the nodes was also comparable to clear network. In order to analyse Packet Delivery Fraction (PDF = packets received / packets sent), data packets released generated from all nodes were considered. Sink node does not release any data packets. Also, malicious node in scenario 3 had supressed forwarding of any self-generated data packets. Total numbers of packets received at the sink node are counted in each scenario. Loss of packets can be due to longer waiting times at buffer queue, or being dropped by malicious node or even might have been successful if the

 ISBN: 978-1-61208-209-7

simulation was allowed to run for longer. Table 7 has data which is self-explanatory; scenario 3 had higher number of packets dropped by malicious node, thus higher loss%. All nodes in a network are affected by the malicious activity. Since the simulation supports idealistic conditions; some nodes selected non malicious nodes as their next hop. Such sender nodes are initialised as non-affected nodes in this paper for better understanding. Most of the data packets from non-affected sender nodes are expected to reach the sink node. It was also observed that while scenario 2 had loss of packets from affected nodes as well as large number of packets from non-affected nodes were also lost; scenario 3 had only affected nodes contributing to the low PDF. This includes all nodes except nodes 8 and 9. For scenario 3, node 4 is also being excluded since it selected malicious node as its preferred parent, and thus had its packets dropped. Nodes not in direct range or path of malicious node in scenario 2 suffered packet loss compared to respective nodes of scenario 3, which had PDF% comparable to the clear scenario (scenario 1). Data is tabulated in table 8. These nodes suffered loss despite having idealistic conditions. The reason may be longer waiting times in the buffer queue of sink when sink was engaged in exchanging control messages to stabilize the routing topology, just like packet delay. Scenario 3 despite having malicious behaviour was seen stable by all other nodes, as malicious node (ID: 13) was able to support ideal routing metrics (similar to clear network). Thus malicious behaviour in scenario 2 disturbed the routing topology, while the same did not occur in scenario 3. As intended, packets from the nodes directly affected by the malicious node did not reach the sink node but other nodes had low packet loss, almost similar to loss% in scenario 1. Scenario 2 had high loss% .

Thus, it is clear that increased rate of DIO messages, increased packet delay along with falling packet delivery fraction are indicators of malicious activity but simple provisions such as supressing self-generated data packets can help a malicious node disguise its behaviour.

V. Conclusion

This work concludes that 6LoWPAN network with RPL protocol is prone to black hole attack, which can be effectively disguised and may lead to an attacked network behave very similar to a healthy network. Increased delays in most packets being delivered at sink, an overall decreased packet delivery fraction and also an increased frequency of DIO messages being exchanged amongst peers can serve as primitive indicators but do not form an exhaustive list of parameters sufficient to identify attack. These indications may be treated as signature of an attack, especially black hole attack. Packet delay and frequency of DIO messages may behave near normal if the malicious node reduces its own packet sending behaviour to NULL. Such a case would make it difficult to detect malicious behaviour. This case study considers a single malicious node in a small network. The extent of damage that could be caused in case of increase in the number of attacking nodes would be exponential. Such a network may continue to exchange control information only while most or all data packets get dropped.

VI. Future Work

The project was undertaken in a simulator with highly idealistic conditions. Elaborating the work on a real test bed would reveal better data for analysis. It has been learnt that malicious activity can be easily disguised so, analysis of additional parameters would help increase the understanding about the signature behaviour of black hole attack.

References

[1] Z. Shelby and C. Bormann, *6LoWPAN: The Wireless Embedded Internet*, UK: John Wiley & Sons Ltd. , 2010. pp. 2-18. Retrieved: Mar,2012.

[2] E. Callaway; et.al, Home networking with IEEE 802.15.4: a developing standard for low-rate wireless personal area networks, *Communications Magazine, IEEE*, Vol 40,No. 8, Aug 2002. pp. 70-77. Retrieved: Mar,2012.

[3] S. Misra; I. Woungang and S.C. Misra; *Guide to Wireless Ad Hoc Networks*, Netherlands: Springer, 2009. Retrieved: May,2012.

[4] Ward Van Heddeghem, *Cross-Layer link Estimation for Contiki Based Wireless sensor networks*; PhD Thesis, Vrije University, Brussels,2009. Retrieved: May,2012.

[5] T. Clausen and U. Herberg, Some considerations on Routing in Particular and Lossy Environments, *Proceedings of the 1st IAB interconnecting Smart Objects with the Internet Worksop*, Pgargue, Czech Republic, March 2011. Retrieved: May,2012.

[6] T. Winter (Ed.), P. Thubert (Ed.), and RPL Author Team, RPL: IPv6 Routing Protocol for Low power and Lossy Networks, *Internet Draft draft-ietf-roll-rpl-17*, work in progress. http://tools.ietf.org/html/draft-ietf-roll-rpl-17 Retrieved: June,2012.

[7] Contiki Operating system Official website : http://www.contiki-os.org Retrieved: Feb,2012.

[8] A. Dunkels, B. Gronvall, and T. Voigt,Contiki a lightweight and flexible operating system for tiny networked sensors, *In Proceedings of the First IEEE Workshop on Embedded Networked Sensors*,Tampa, Florida, USA, Nov. 2004. Retrieved: May,2012.

[9] T. Winter (Ed.) et.all, RPL: IPv6 Routing Protocol for Low power and Lossy Networks,*Internet Draft draft-ietf-roll-rpl-19*, work in progress. http://tools.ietf.org/html/draft-ietf-roll-rpl-19. Retrieved: May,2012.

[10] Al-Shurman, Mohammad, Yoo, Seong-Moo, Park, and Seungjin, Black hole attack in mobile Ad Hoc networks, *Proceedings of the 42nd annual Southeast regional conference, ACM-SE 42*,2004,isbn 1-58113-870-9,Huntsville, Alabama, pp 96–97. Retrieved: May,2012.

 ISBN: 978-1-61208-209-7

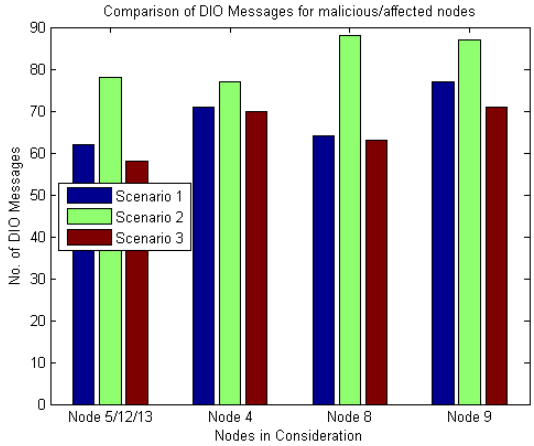

Figure 3. Comparison of DIO messages for Malicious/Affected nodes

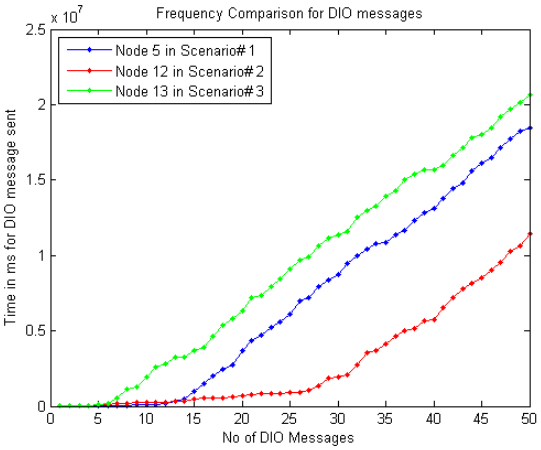

Figure 4. Frequency Comparison of DIO messages sent by Malicious nodes and Counterparts

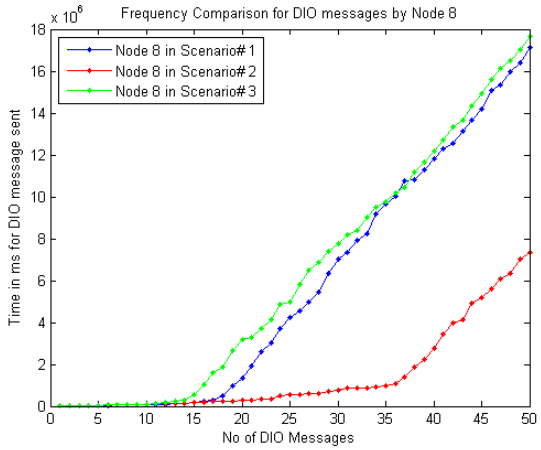

Figure 5. Frequency Comparison for DIO messages w.r.t Node 8