DIS Flooding Attack in IOT Networks Running RPL

Software Recommended: NetSim Standard v14.1, Visual Studio 2022

Project Download Link:

https://github.com/NetSim-TETCOS/DIS-Flooding-RPL-v14.1/archive/refs/heads/main.zip

Follow the instructions specified in the following link to download and set up the project in NetSim:

https://support.tetcos.com/en/support/solutions/articles/14000128666-downloading-and-setting-up-netsim-file-exchange-projects

1 Introduction

In RPL, DIS messages are used by nodes to join the network. A node sends a DIS message to its neighbor nodes to request the routing information so that it may join the existing DODAG. Thus, a new node continuously transmits DIS messages with a fixed interval until it receives a DIO message from any neighbor node. Once a node receives a DIO message, it stops transmitting DIS messages and joins the network by sending DAO to the solicited node.

A malicious node can utilize this feature to degrade the network performance by choosing different DIS transmission intervals for periodically transmitting DIS messages to its neighboring nodes; this is called a DIS flooding attack. This leads to an increase in the network's control packet overhead and power consumption.

2 Implementation in RPL (for 1 sink)

- In RPL the transmitter broadcasts the DIO during DODAG formation.
- The receiver on receiving the DIO from the transmitter updates its parent list, sibling list, rank and sends a DAO message with route information.
- Malicious node upon receiving the DIO message instead of joining existing DODAG just Drops DIO and frequently transmits DIS messages. Which forces normal nodes to reset their trickle timers and flood the network with DIO messages.

A file Malicious.c is added to the RPL project.

The file contains the following functions:

- **fn_NetSim_RPL_MaliciousNode( );** //This function is used to identify whether a current device is malicious or not in order to establish malicious behavior.
- **rpl_drop_msg( );** //This function is used to drop the DIO messages received by the malicious nodes instead of replying with a DAO message.

You can set any sensor as malicious Node, and you can have more than one malicious node in a scenario. Device IDs of malicious nodes can be set inside the fn_NetSim_RPL_MaliciosNode() function in malicious.c file.

3 Example

The **DIS-Flooding-Workspace** comes with a sample network configuration that is already saved.

To open this example, go to Your work in the home screen of NetSim and click on the **DIS_FLOOD_Case1_Example** from the list of experiments.

The saved network scenario and the settings done is explained below:

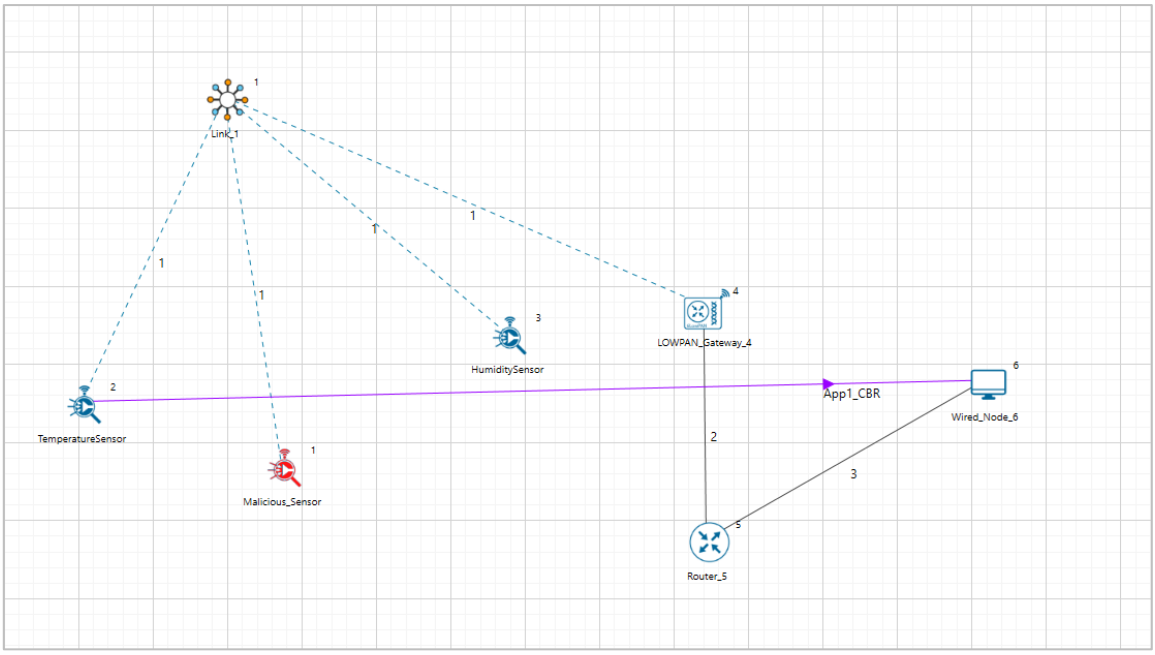

Figure 1: Network scenario showing a DIO Suppression attack in IoT RPL project. Includes 3 sensors (one malicious), a wired node, a router, and a LoWPAN gateway.

Application Properties	
Source ID	2
Destination ID	6
Transport Protocol	UDP
Other Properties	Set Default
Link Properties	
Channel Characteristics	Pathloss only
Pathloss Model	Log distance

Pathloss Exponent	3.5

Table 1: Application and link properties.

- Set Network Layer Routing Protocol to RPL in both sensor and LowPan_Gateway
- Device Properties: Go to Sensor Properties -> Network Layer -> DIS Interval -> 10ms.
- Run the Simulation for 100 seconds.

4 Results and Discussion

1. In packet trace, you will find that the malicious node (Device id 1) even after receiving DIO from neighbor nodes it just Drops DIO and the malicious node frequently transmits DIS messages to the neighbor nodes.
2. This will have a direct impact on the Application Throughput and Delay which can be observed in the Application Metrics table present in the NetSim Simulation Results window.

Simulation instructions in Visual Studio:

- For **With DIS,** Run the simulation of the imported workspace.
- For **Without DIS,** Reset the binaries of the imported workspace and run the simulation.
- To reset the binaries, go to your Work -> Source Code -> Reset Binaries

To recheck the impact of the network performance **With DIS,** Rebuild the **RPL** project in source code, Go to your Work -> Source Code -> Open-Source Code.

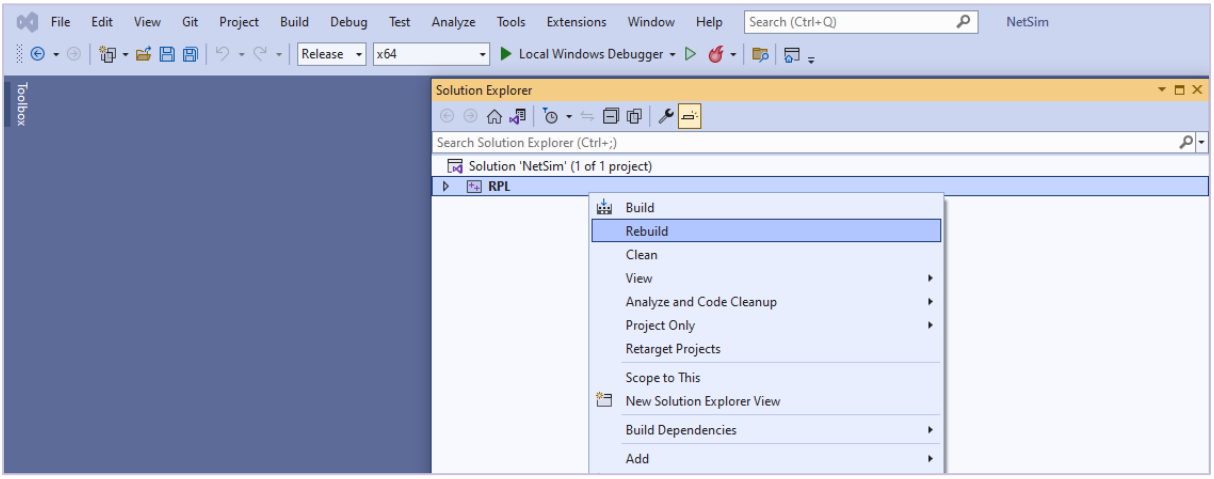

Figure 2: Source code of current Workspace.

Case 1: Application generation rate Vs. Application throughput:

We fix the DIS interval to 10 milliseconds and vary the application generation rate to see the impact of DIS flooding on the network performance.

	Throughput (Mbps)		Delay (ms)	
Generation Rate(Kbps)	**With DIS**	**Without DIS**	**With DIS**	**Without DIS**
60	0.0419	0.0597	7023.682	51.932
80	0.0460	0.0798	14518.141	52.009
100	0.0498	0.0997	19147.977	52.106
120	0.0515	0.1181	23208.916	726.934

Table 2: Throughput and delay with and without DIS flooding vary with the generation rate.

This can be further understood with the help of following plots:

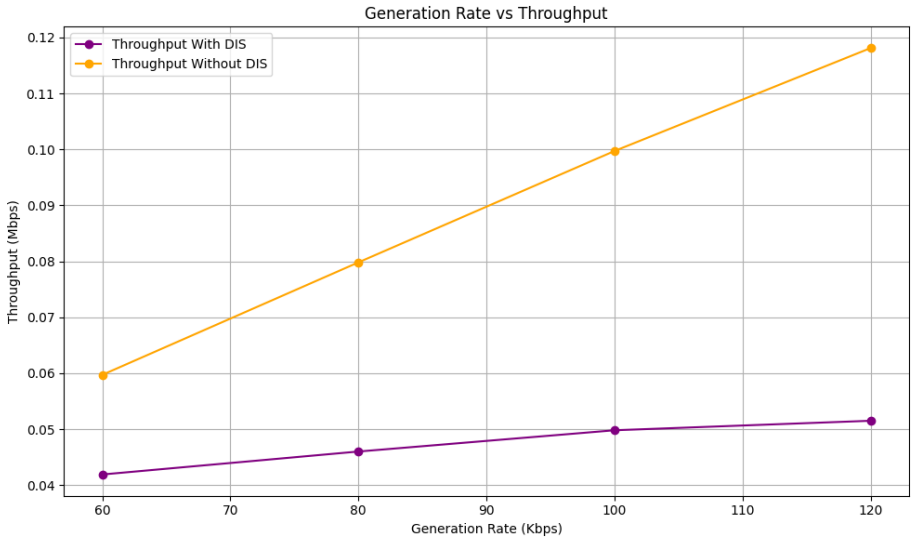

Figure 3: Figure shows as the generation rate increases, the throughput with DIS flooding is less compared to without DIS flooding.

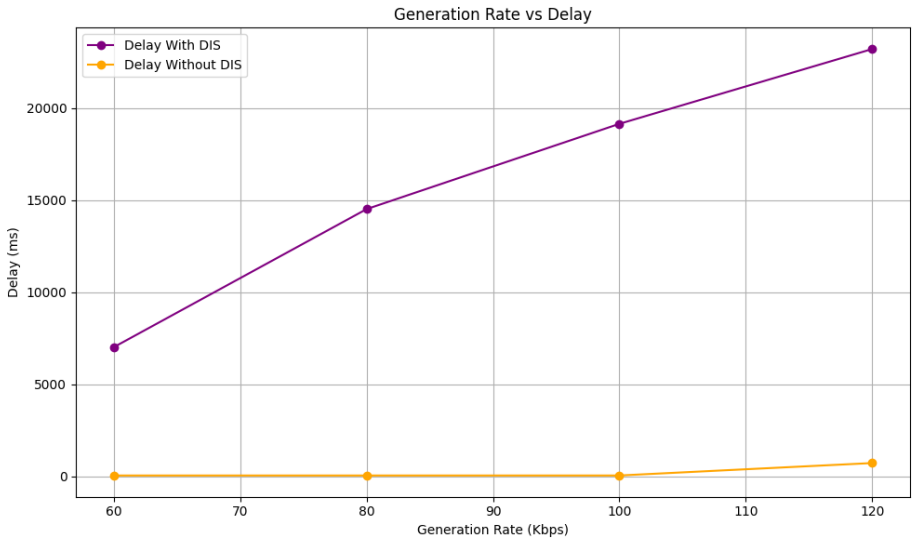

Figure 4: Figure shows as the generation rate increases, the delay with DIS flooding is more compared to without DIS flooding.

We can observe that the application throughput decreases in case of DIS flooding when compared with the usual simulations for various application traffic generation rates.

Delay is comparatively high in the case of DIS flooding and increases with the increase in generation rate. This is because the nodes are busy receiving and responding to DIS messages from malicious nodes frequently. The nodes that receive DIS messages are forced to reset their trickle timers and flood the network with DIO messages.

Case 2: DIS Interval Time Vs. Application throughput:

We fix the application generation rate to 250 Kbps and vary the DIS interval to see the impact of DIS flooding on the network performance.

To change the DIS Interval parameter, go to Sensor Properties -> Network_Layer -> DIS_Interval -> 20ms.

DIS Interval (ms)	Throughput (Mbps)
25	0.091
20	0.085
15	0.075
10	0.058
5	0.056

Table 3: DIS interval vs Throughput

This can be further understood with the help of the following plots:

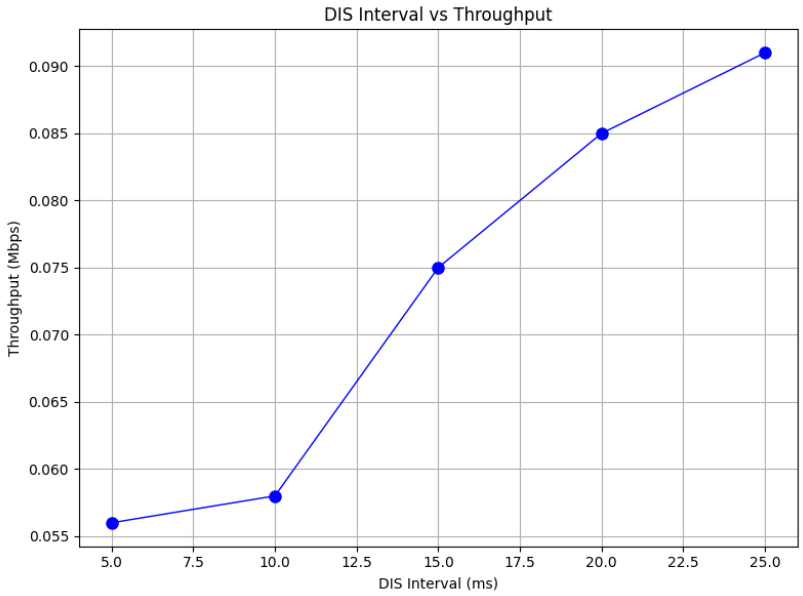

Figure 5: Figure shows as the DIS Interval increases the application throughput increases.

We can observe that the application throughput decreases as we decrease the DIS Interval time. Upon decreasing the DIS interval, more DIS messages will be sent by the malicious

nodes more frequently. Legitimate sensors spend more time processing and responding to DIS messages than sending the data packets.

DIS flooding severely degrades the performance of Low Power and Lossy Networks (LLNs) because of the increase in control packet overhead.

C Code for defining the malicious node

```
#include "main.h"
#include "RPL.h"
#include "RPL_enum.h"

#define MALICIOUS_NODE1 1

int fn_NetSim_RPL_MaliciousNode(NetSim_EVENTDETAILS*);
void rpl_drop_msg();

int fn_NetSim_RPL_MaliciousNode(NetSim_EVENTDETAILS* pstruEventDetails)
{
	if (pstruEventDetails->nDeviceId == MALICIOUS_NODE1)
	{ /*For multiple malicious nodes use if(pstruEventDetails->nDeviceId == MALICIOUS_NODE1
|| pstruEventDetails->nDeviceId == MALICIOUS_NODE2)*/
		return 1;
	}
	return 0;
}

void rpl_drop_msg()
{
	fn_NetSim_RPL_FreePacket(pstruEventDetails->pPacket);
	pstruEventDetails->pPacket = NULL;
}
```

Changes to rpl_process_ctrl_msg(),in RPL_Message.c file, within RPL project

```
void rpl_process_ctrl_msg()
{
	switch (pstruEventDetails->pPacket->nControlDataType % 100)
	{
	case DODAG_Information_Object:
		if (fn_NetSim_RPL_MaliciousNode(pstruEventDetails))
			rpl_drop_msg();
		else
			rpl_process_dio_msg();
		break;
	case Destination_Advertisement_Object:
		rpl_process_dao_msg();
		break;
	case DODAG_Information_Solicitation:
		rpl_process_dis_msg();
		break;
	default:
		fnNetSimError("Unknown rpl ctrl msg %d in %s",
					pstruEventDetails->pPacket->nControlDataType,
					__FUNCTION__);
		break;
	}
}
```