"Analysis and Handling Worst Parent Attack in Routing Protocol for Low power and Lossy networks"

Project report submitted in partial fulfilment of the requirement for the degree of Bachelor of Technology

In

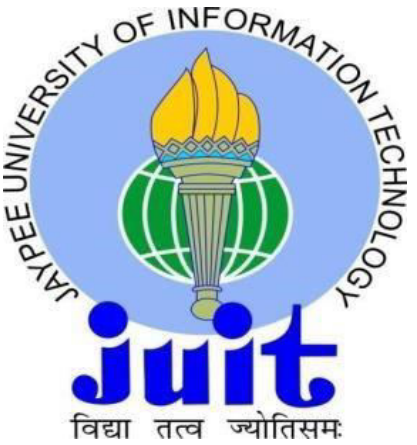
Computer Science and Engineering/Information Technology

By

Tanush Choudhary(141401)

Under the supervision of

Mr. Arvind Kumar *To*



Department of Computer Science & Engineering and Information Technology
Jaypee University of Information Technology Waknaghat, Solan- 173234, Himachal Pradesh

Candidate's Declaration

I hereby declare that the work presented/written in this report entitled "Analysis and Handling Worst Parent Attack in RPL" in partial fulfilment of the requirements for the award of the degree of Bachelor of Technology in Computer Science and Engineering/ Information Technology submitted in the department of Computer Science & Engineering and Information Technology, Jaypee University of Information Technology Waknaghat is an authentic record of my own work which carried out over in the period from August 2017 to May 2018 under the supervision of Mr.Arvind Kumar(Associate Professor, Computer science and Engineering).The matter embodied in the report has not been submitted for the award of any other degree or diploma.

Tanush Choudhary (141401) .....

This is to certify that the above statement made by the candidates is true to the best of my knowledge.

Mr. Arvind Kumar
Associate Professor
Computer Science & Engineering Dated:

ACKNOWLEDGEMENT

I would like to express my special thanks of gratitude to our project guide Dr. Arvind Kumar who helped us in conceptualizing the project and actual building of procedures used to complete the project. I would also like to thank our Head of department of Jaypee university of information technology for providing us this golden opportunity to work on a project like this, which helped us in doing a lot of research and we came to know about so many things.

Secondly we would like to thank our family and friends who guided us throughout the project so as to complete our project on time.

Thanking you,

Tanush Choudhary (141401)

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATIONS

S.NO	ABBREVIATIONS	DESCRIPTIONS
1.	RPL	ROUTING PROTOCOL FOR LOW POWER AND LOSSY NETWORK
2.	IOT	INTERNET OF THINGS
3.	DODAG	DESTINATION ORIENTED DIRECTED ACYCLIC GRAPH
4.	LLN	LOW POWER AND LOSSY NETWORK
5.	WPAN	WIRELESS PERSONAL AREA NETWORK
6.	MP2P	MULTIPOINT TO POINT TRAFFIC
7.	P2MP	POINT TO MULTIPOINT TRAFFIC
8.	WPA	WORST PARENT ATTACK
9.	RA	RANK ATTACK
10.	DIO	DESTINATION ORIENTED DAG INFORMATION OBJECCTIVE
11.	DIS	DODAG INFORMATION SOLICITATION
12.	IDS	INTRUSION DEECTION SYSTEM
13.	6LoWPAN	IPv6 OVER LOW-POWER WPAN
14.	OS	OERATING SYSTEM

ABSTRACT

The interest is growing rapidly in IOT which now comes in a large-scale deployment of LLNs. These networks(LLNS) exchange communications between objects from the real world(devices), examples of these such devices areembedded sensors and automation devices used in homes , and the connection with Internet. In this exchange of data we use an distance vector standard routing protocol called RPL, which submitted by IETF in order to accomplish the specific constraints and properties of these networks(LLNs). However, this RPL is open to a large category of attacks. Their results could be quite significant in terms of resources and network performance . In this projectreport, we propose to make a taxonomy of the Worst Parent attack(WPA) against RPL, considering how this attack modify the topology of network,behavior changes of nodes in network attacks modify. We describe this attack, analyse its affects and compare its properties like power consumption and hop used ,radio traffics etc, discuss existing counter-measure.

1.INTRODUCTION

1.1 Internet of things

As this project is directly related to Internet of things so lets take a brief about IOT. We can define the Internet of Things as the future stage use in the Internet as now a days most people believe, where the sensors are embedded in different things and objects which are connected to Internet which get the data , gather the data and analyse the data which leads to a smart solution.

There are hundreds of examples and uses of IOT like:

- In Industrial uses
- In manage the process take place in design of infrastructure
- Processes in factories in manufacture
- Management of energy resources
- Medical and health caresystems
- In Home and building automation
- In transportation devices

Benefits of IOT-

- **Ubiquitous networks** :personalWi-Fi or local area network on every phone ,laptops and on many of the other devices. Everyone and everything wants as well as needs to be connected.

- **Connected different computing** :as we all want all devices like mobile phones, televisions(color or black and white), players like audio and DVD, transportation vehicles etc. to keep history record and collect data of how we are using these devices and what we are interested in as per time ,with place and time data .

- **Intelligence in the topology of the network** : a guy named jimgray , the innovative expert in database from Microsoft, made smart sensors that behaving as a small-databasewith embedded algorithms and consume minimum power consumption. 10 years ago he quotes: "Intelligence is swaying to the boundary of the networks. Each of the disk systems and each sensor component will be a competitive database machine."

- **Analytics as a Service** the various Apps and interfaces economies are growing at an big rate ,so with the help of IOT and devices we get the collected data from API and different apps and then analyse that data and give preferred solutions and changes thata should be made.

- **Automation in marketing**: most of the android and other technologies are developing apps are all developing apps and network which store the information data regarding users like : time and location, what consumer want ata what time, as well as buying schedule(as we can see in e-commerce sites like amazon.,com etc) . Obviously, the geological location based data needs to maintain the user privacy as well as the right delivery of best and right product and service to the all the user.

1.2 INTRODUCTION OF IOT WITH LLN

The IOT defines a new model we can say that is so growing in the terms of networks and services. It contains in the upgrade of the Internet to objects from the real ongoing world by the help of devices and sensors, which interacts with each and every device to get a common goal. The high interest for this whole paradigm has resulted in the large-numbered deploymen LLNs.

example: wireless sensor networks and home automation systems. These networks helps in high resource constraints (such as ETX.memory, processing power,tim etake to commumnicate) and their communication links are made such that they have high loss rate and low through put that results in low power consumption . Also with that, the patterns of topology are not as same as to a point to point schema. In many cases, sometimes the devices also communicate according to point to multipoint and multipoint to points schemas or pattern. Other present routing protocols are not suite to deal with requirementrequire in IOT sensors and devices.

So in total there are many such protocols has been deployed which also have the IEEE 802.15.4 standard numbers of protocol for the layer in WPAN and the 6LowPAN protocol which defines mechanism likeheader compression ,encapsulation and all other requirements between IPv6 and 802.15.4(IEEE). But most importantly for routing layer, the “ROLL1” working ropups gives a protocol called RPL works on IPv6 , which we will discuss in detail , its working and different terms associate with it.

1.3INTRODUCTION TO RPL

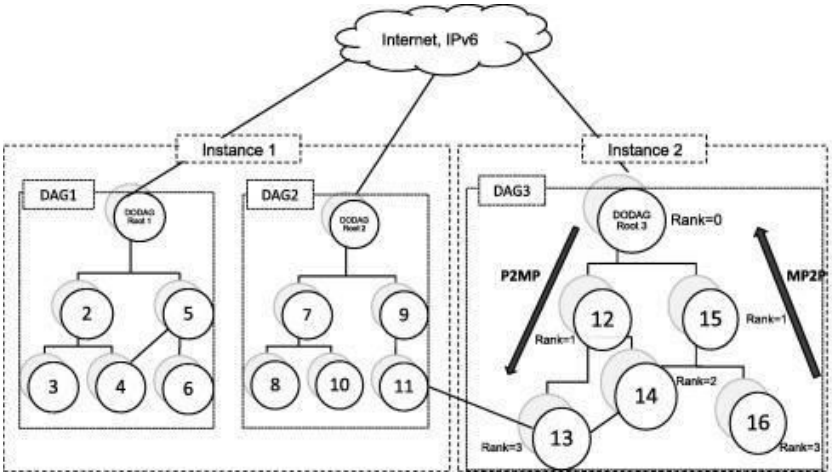
The RPL, as by its name it is clear that it is a distance vector routing protocol which is based on IPv6.. The IOT devices like sensors and other devices which runs on LLNsare interconnected according to a topology which is a combination of both tree and mesh topologies called DODAG. A DODAG graph is unidirectional and acyclic so there are no loop conditions in this topology, it starts froma or many root node which is also called sink of the graph, where all collected data is stored. A network can have one or more RPL instances , which have multiple DODAG graphs .There is an objective functionof each DODAG RPL instance ,which is responsible to find the best path for the packets to the sinkwhich depends on the sets of metrics or constraints. For any instance, this function can be designed to minimize energy consumptions by nodes or designed simply to compute the path which is shortest. Several instances can be joind by RPL node at the same time, but only one DODAG graph can be joined at a time per instances. These multiple DODAG instances combined to result in the RPL protocol to perform various optimized task , such as low power consumption or to perform low ETX. The RPL packets forwarded as per these three traffic pattern :

(i) Multipoint to point from leafs to the root by upward paths.

(ii) Point to multipoint from the root to leafs using downward paths

(iii) Point to point both up and downward paths .

A demonstration is given below:



2.

1.4 WORKING OF RPL

As this whole project sorrounds by RPL so here we first discuss the working of an RPL,

but Before that there are some important terms we have to look at:

- DAG: Directed Acyclic Graph: A directed acyclic graph which have the property that all edges(or nodes path) are in such a way that no cycles or loop exist.
All node paths are contained in paths goes toward end node or we can say
Sink node.

- DAG root: A DAG root is one or more node within the graph that has no outgoing Arrow which represent no outgoing packets . as the graph is acyclic, so atleast one dag node should be there in a DAG.

- Destination-Oriented DAG (DODAG): A DAG have only one destination and has only a single DAG like:
at a single DAG root (the DODAG root)
withno outgoing edges.

- Rank: A node's Rank given by topology of network which given by the fact that what is node's position relative to the dink or root node of that Rank increases in the Down direction , anode has as big as rank as it is far from the root node and decreases as it goesin the Up direction. The Rank is computed by its OBJECTIVE FUNCTION as it depends on it.

- Objective Function (OF): An OF defined as what is our objective that what should this routing focus on as power consumption , shortest path or , ETX etc ,this function is used to calculate rank optimization objectives. also, the OF decides how nodes in theDODAG are selected as child's parent.

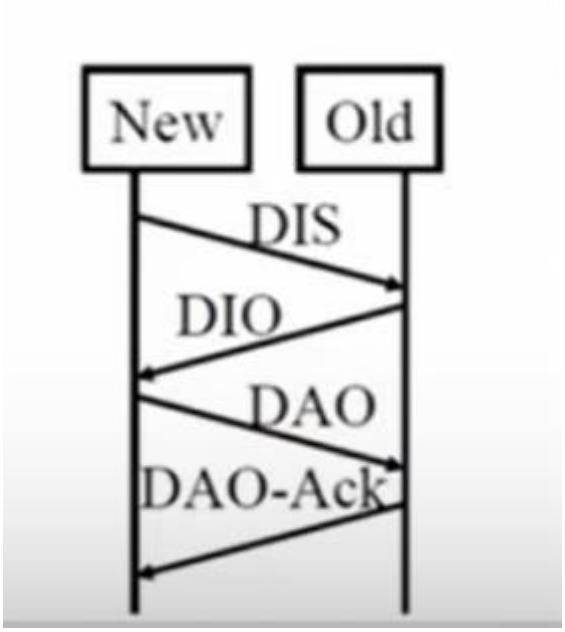
There are four types of messages by which the nodes of an DODAG communicates with each other:

- DIO or DODAG Information Object
- DAO or Destination Advertisement Object
- DIS or DODAG Information Solicitation
- CC Consistency Check

The working of these four is as follow:

The DODAG Information Object carry information, data that gives any node chance to find an RPL Instance and see all parameters it contains.DAO is used to transfer destination information Upward with the DODAG. TheDAO message may bemake a request or an error, that can be seen by its destination node with a Destination AdvertisementAcknowledgement (DAO-ACK) message which sender sends back of the DAO.

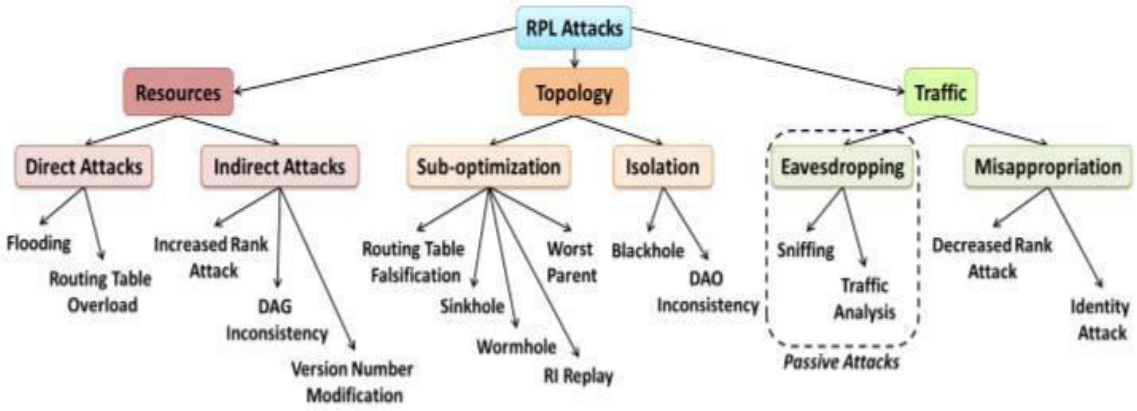
The DAO-ACK message works as a packet that is send as a packet which is unicast by a DAO node which is parent or root of DODAG in response to a unicast DAO message.The CC message cheks that is the mmessage is secure or not?. A CC message should be sent as a secured RPLmessage.



3.

1.5 ATTACKS ON RPL:

As this RPL is still is not fully attacks free and is updating day by day, it is open to Various kind of attacks , the attacks are characterized into three categories : Resources,Topology and Traffic and further subcategorized in various categories shown below -



4.

Our project focus on sub-optimzation category in topology attack which is called “WORST PARENT ATTACK”

1.6 WORST PARENT ATTACK:

So what is worst parent attack?

In this attack the nodes or children of any dodag consists in choosing not the best but its worst parent according to the objective function. This results in that resulting path is not best path which comes in poor performance

like : more power consumption and more hop used to transfer the data

These worst parent attack is not easy to tackle and handle because the rank of child depends on its parent and does not rely on nieghbor.

As this attack is a topology network type attack so it affect the topology of network that how the pack -ets would be transfer ,in this attack the malicious node attacks on objective function of the graph so the parent choosing criteria changes ,instead to choose its best parent it will choose the worst parent of the topology which results in :

- Packet Delay
- More power consumptions by nodes
- More hops so more resources used

  And many more disadvantages

In this project we compare all these characters like power consumption hops used when there is no attack and when attack is happening,also we will see a solution to find the node in which attack happens. We use a simulation to show a topology network and to collect data and show collect view of each node.

2LITERATURE REVIEW

2.1 A Taxonomy of Attacks in RPL-based Internet of Things:Anthea Mayzaud, Remi Badonnel, and Isabelle Chrisment.

(Received June 23, 2015; revised and accepted July 30 & Aug. 12, 2015)

The above paper stated a way to classify different types of attack in the RPL protocol in three main categories: resource ,topology ,traffic. These attacks low the network lifetime with the generate of fraud messages and the building of infinite loops. The attacks within the topology make the nodes converge by a sub optimal way to config and trap nodes. Finally, attacks against network confriguration let a malicious node trap and analyse large part of the confriguration . Based on this taxonmy, we compared the properties of the all attack and also it tells differnet scenarios to avoid or reduce their affect .

2.2 The Impact of Rank Attack on Network Topology of Routing Protocol for LowPower and Lossy Network Anhtuan Le, Jonathan Loo, Aboubaker Lasebae, Alexey Vinel, Yue Chen, and Michael Chai

(EEE SENSORS JOURNAL, VOL. 13, NO. 10, OCTOBER 2013)

Directing convention for low power and lossy systems (RPL) is the primary utilized steering convention of 6LoWPAN, a center correspondence for the IOTs. RPL beats different remote sensor and specially appointed directing conventions in nature of administration (QoS), gadget administration, and vitality sparing execution. The Rank idea in RPLserves multiplepurposes, including course streamlining, avoidance of circles, and overseeing control more load as overhead. In this paper, we dissect a few distinct sorts of inside dangers that are gone for the Rank property and concentrate their effect on the execution of the remote sensor arrange. Our investigation brings up the issue of a RPL shortcoming, which is the absence of a checking guardian in each hub. In RPL, the youngster hub just gets the parent data via various control messages, yet it can't check the administrations that its parent give thus it will take after an awful quality course in the event that it has a noxious parent. Our outcomes demonstrate that distinctive sorts of the

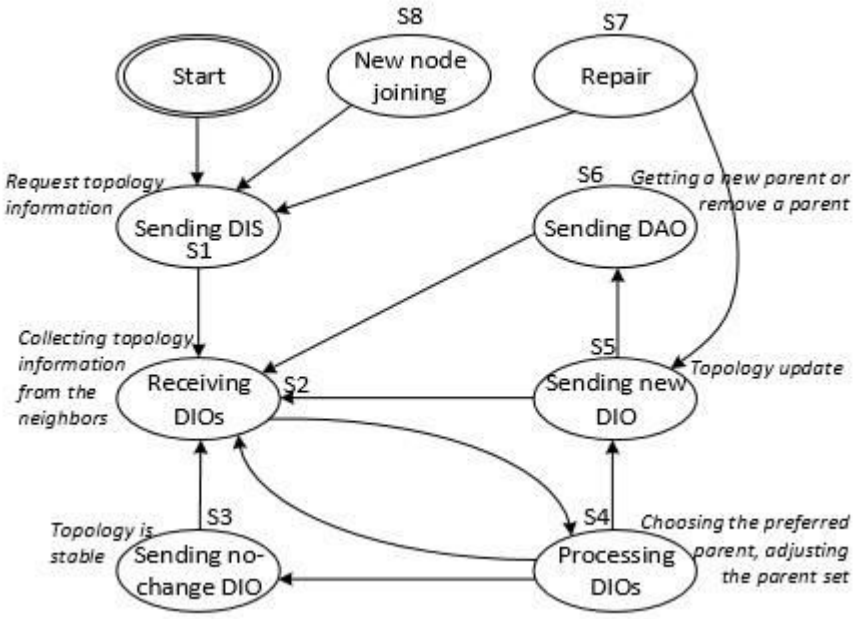
Rank assaults can be utilized to deliberately minimize particular various quality parameters. This paper additionally uncovers that assault in a high sending load territory will have more effect on organize execution than assault in different zones. The protectors can utilize the learning of such relationship between's assault area and its results into establishment of higher security levels at specific positions by observing touchy system parameters and recognizing the anomalie.

2.3 Real-time Intrusion Detection in the Internet of Things :(SVELTE)

Shahid Razaa, Linus Wallgrena, Thiemo Voigta

(Swedish Institute of Computer Science, Kista, Sweden Department of Information Technology, Uppsala University, Sweden „June 14, 2013)

In the IoT, asset compelled things are associated with the untrustworthy and untrusted Web by means of IPv6 and 6LoWPAN systems. Notwithstanding when these protocols and network secured with encryption and confirmation, these things are presented both to remote assaults from inside the 6LoWPAN system and from the Web. Since these assaults may succeed, IDS are vital. As of now, there are no IDSs that meet the prerequisites of the IPv6-associated IoT since the accessible methodologies are either altered for WSN or for the traditional Web. We configuration, actualize, and assess a novel interruption identification framework for the IoT that we call SVELTE. We execute SVELTE in the Contiki OS and completely assess it. Our assessment demonstrates that in the mimicked situations, SVELTE identifies every single pernicious hub that dispatch our actualized sinkhole as well as specific sending assaults. In any case, the genuine positive rate isn't 100%, i.e., we have some false alerts amid the location of malignant hubs. Additionally, SVELTE's overhead is sufficiently little to convey it on obliged hubs with constrained vitality and memory limit



.

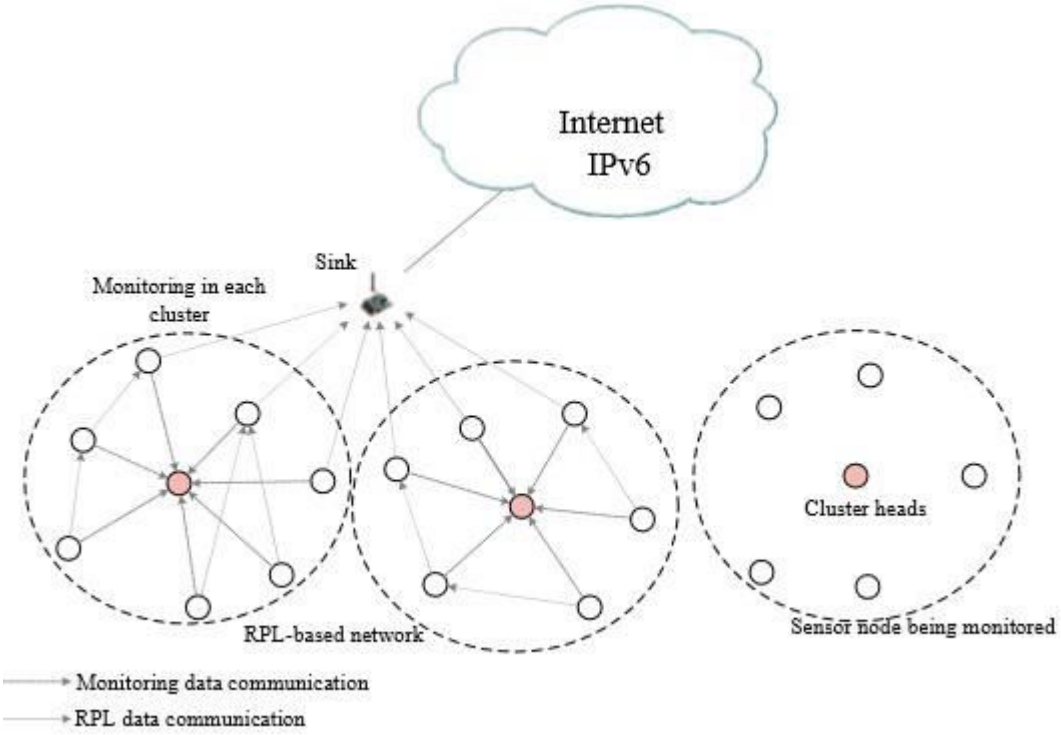
5.

2.4 **A Specification-Based IDS for Detecting Attacks on RPL-Based Network Topology**

(Anhtuan Le , Jonathan Loo , Kok Keong Chai and Mahdi Aiash - March 2016; Accepted: 5 May 2016; Published: 12 May 2016)

RPL topology assaults can minimize the system execution altogether by disturbing the ideal conve -ntion structure. To identify such dangers, we propose a RPLspecification, got bya semi-autoprofiling strategy that develops an abnormal state unique of activities through system reproduction follows, to use as reference for confirming the hub practices. This particular, including all the genuine convention states and changes with comparing insights, will be actualized as an arrangement of principles in the interruption location specialists, as the bunch makes a beeline for screen the entire system. With a specific end goal to spare assets, we set the bunch individuals to report related data about itself and different neighbors to the group head as opposed to making the head catching all the correspondence. Accordingly, data about a group part will be accounted for by various neighbors, which permit the bunch go to do check again We propose to record the succession in RPL DIO and DIS messages to dispose of the synchronized issue made by

the postponement in transmitting the report, in which the bunch head just crosses keep an eye on data that originate from sources with a similar grouping. Reproduction comes about demonstrate that the proposed IDS has a high exactness rate in identifying RPL topology assaults, while just making inconsequential overhead (around 6.3%) that empower its adaptability in extensive scale arrange.



6.

3. SYSTEM DESIGN

3.1 Tools and Technologies used

3.1.1 Software Used

1.Instant Contiki OS :

Instant Contiki is an entire Contiki development environment in a just one downloadIt is a Ubuntu Linux virtual machine that keeps running in VMWare player and has Contiki and all the improvement instruments, compilers, and test systems utilized as a part of Contiki advancement introduced. Moment Contiki is convenient to the point that even in-your-face Contiki designers utilize it.

Contiki is a remote sensor organize working structure and contains the part, libraries, the program loader, and a course of action of methodology. It is used as a piece of composed embedded systems and insightful objects.Contiki gives instruments that help with programming the savvy question applications. It gives libraries to memory assignment, connected rundown control and correspondence reflections. It is the main working framework that gave IP correspondence. It is created in C, every one of its applications are additionally created in C programming dialect, and in this manner it is exceptionally compact to various structures like Texas Instruments MSP430.Contiki is an occasion driven framework in which forms are actualized as occasion handlers that hurried to finishing. A Contiki framework is parceled into two sections: the center and the stacked projects. The center comprises of the Contiki portion, the program loader, the dialect run-time, and a correspondence stack with gadget drivers for the correspondence equipment.

The Program loader stacks the projects into the memory and it can either get it from a host utilizing correspondence stack or can acquire from the appended stockpiling gadget, for example, EEPROM.

The Contiki working framework gives modules to various undertakings (layers). It gives the steering modules in a different directory "contiki/center/net/rpl" and comprises of various records. These records are isolated legitimately in view of the functionalities they accommodate occasion rpl-dag.c contains the usefulness for Coordinated Non-cyclic Diagram (DAG) development, rpl-icmp6.c gives usefulness to bundling ICMP messages and so on.

2. Cooja Simulator

COOJA is C dialect based test system intended for reproducing sensor systems running the Contiki sensor arrange working framework. The test system is actualized in Java however permits sensor hub programming to be composed in C. One of the separating highlights is that COOJA takes into account synchronous reproductions at three unique levels: System Level, Working Framework Level and Machine code guideline level. COOJA can likewise run Contiki programs either assembled locally on
the host CPU or arranged for MSP430 emulator.

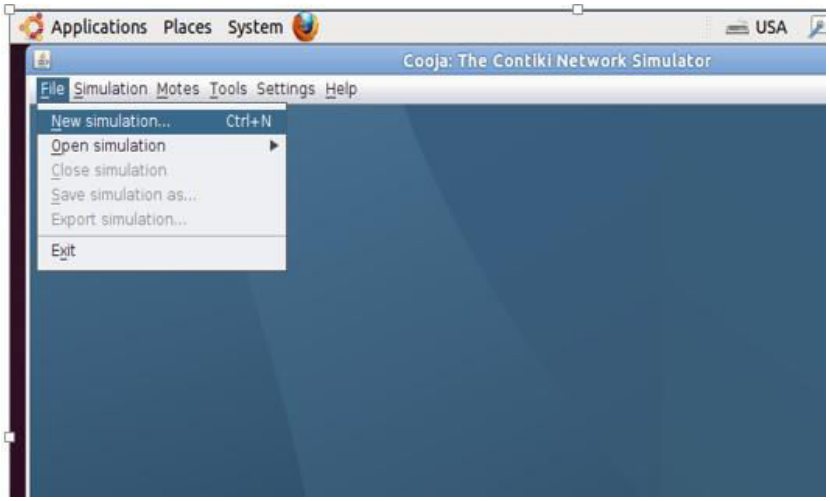
In COOJA every one of the collaborations with the reproduced hubs are performed by means of modules like Reproduction Visualizer, Course of events, and Radio lumberjack. It stores the reproduction in a xml record with augmentation 'csc' (COOJA reenactment design). This record contains data about the reenactment condition, modules, the hubs and its positions, irregular seed and radio medium and so on.

COOJA Test system runs the Contiki applications whose documents are put in another catalog and may likewise contain a "task conf.h" record which gives the capacity to change RPL parameters in a single place.

3.1 Getting Started:-

3.1.1 Create new simulation

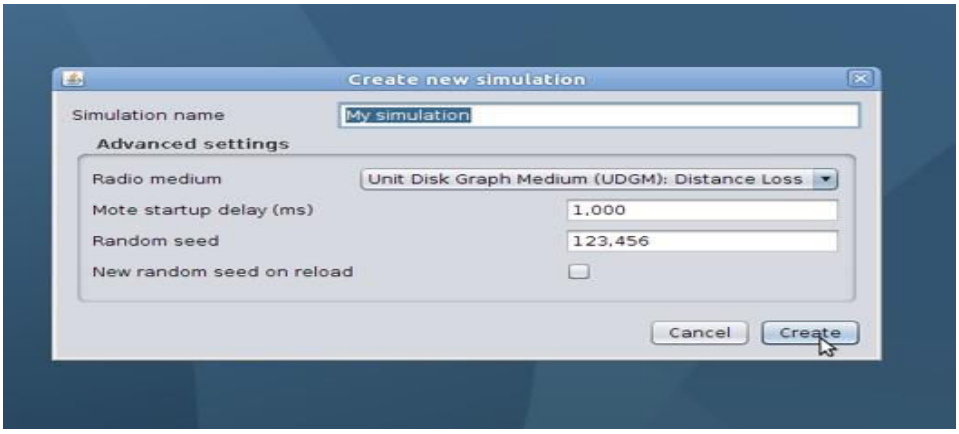
Click the File menu and click New Simulation.



7.

3.1.2 Set simulation options

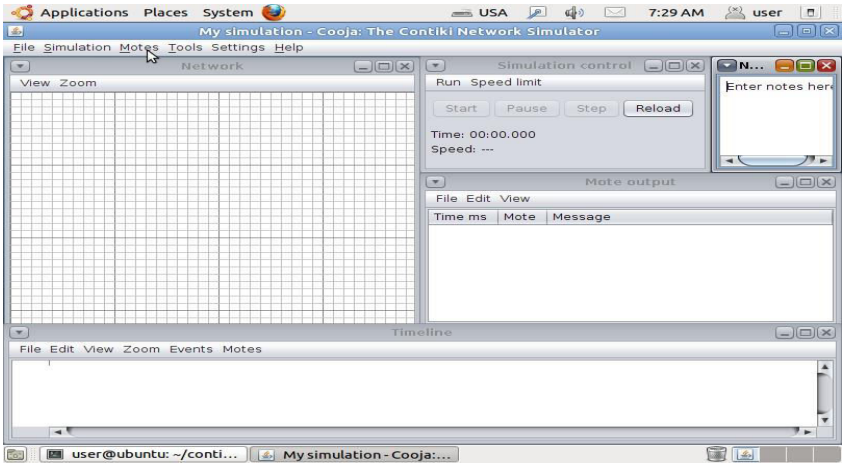
COOJA currently reveal the produce new simulation pop up window. during this dialog, we have a tendency to might favor to provide our simulation a brand new name, except for this instance, we'll simply follow My simulation.



8.

3.1.3 Simulation windows

COOJA now bring up the new simulation. The Network window, can see at the highest left of the window shows all nodes you implemented- it's empty currently, because we has not yet added any new sky mote. The Timeline window, contains all important details like communication rate , which node has packet now and all other important things- terribly handy for understanding what goes on within the network. . The stuff output winow is basically the interface window in cooja so all interface prinout of nodes. The Notes window on the highest right is wherever we will write notes in between of reading and simulation. and therefore the Simulation management window is wherever we tend to begin ,stop and reload our simulation.

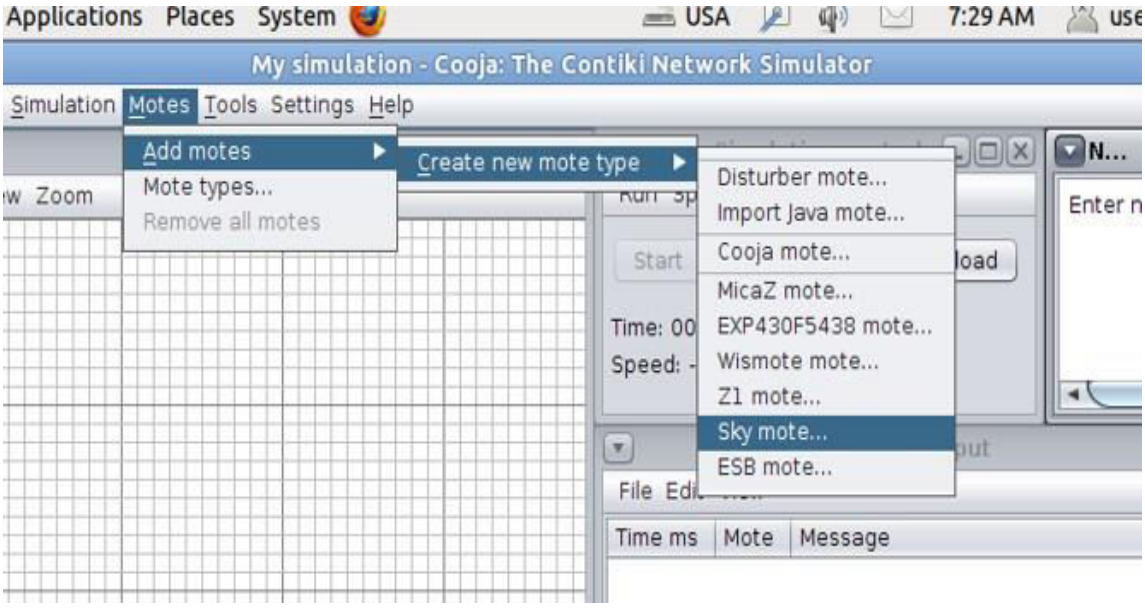


9.

3.1.4 Add motes to the simulation

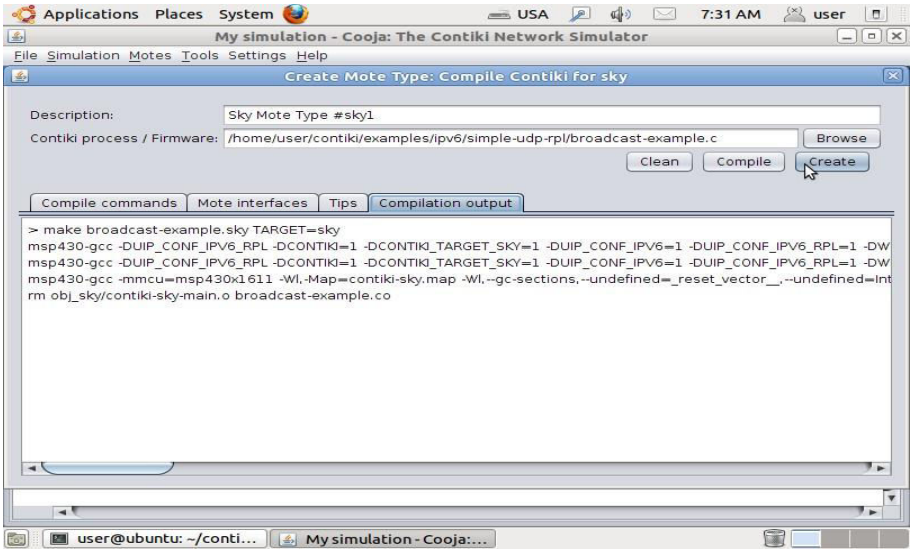
Add motes

Before we will make a new our network, we tend to should add one or additional motes. we tend to do that via the Motes menu, wherever we tend to click on Add Motes. Since this is often the primary stuff we tend to add, we tend to should 1st produce a stuff sort to feature Click produce new stuff sort and choose one in every of the obtainable stuff varieties. For this instance, we tend to click Sky mote to form associate emulated Sky MODE.



3.1.5 Compile Contiki and the application

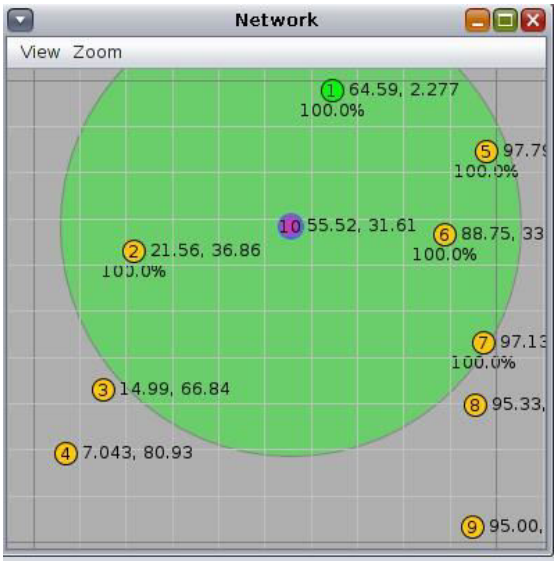
Now COOJA can test and compile that compile the application and compile on that platform we selected. Now Click at the Compile button. this may take some time as primary time require a second a minimum of. The compilation output can be seen within the white box at all-time low of the window.



10.

3.1.6 Start the simulation

After compilation of motes and placing those motes accordingly or randomly we can see a scenario in which there is a sink node 1 and 9 motes are senders , the view option used to enhance the view of simulation ,the simulation would be start after click on the start button.



3.2 Algorithms and code implementation (in cooja)

3.2.1 Implementation of WPS(Rank Attack)

As in COOJA simulation the Objective function is predefined and children chooses their preffered parent with objective to achieve best ETX first it calculates rank of each node :in the rpl the major way to calculate the rankis the base rank + increment depends on objective function , in this code if base rank -0 it means there is only one node in whole topology,base rank is rank given by its parent, and increment based on hops used by by the node to transfer the packets from node to sink.

```
if(baserank=0)
{if(p=NULL)
return INFINITERANK;
baserank=p->rank;
      }
increment=p!=NULL?
        p->dag->instance->minhopranking:DEFAULTTRACKINCREMENT;
        if((rplrank)(vaserank+increment)<baserank)
             {
Printf("RPL: 0F0 rank %d increase to rank with value of infinite due to wrapping\n",base rank);
return infiniterank;
}Return baserank+increment;
        }
```

This is the actual code to calculate rank of the nodes in topology.

But to choose the preffered parent after calculate rank there is another code function :

Code to choose best parent :

```
/* Both parent should be in same DAG
if(rank1<rank2 + mindifference && rank1>rank2 – mindifference)
{
 return dag->prefferedparent;
  }
  else
    if(rank1<rank2)
   {
    Return parent 1;}
   else
   { Return parent 2;
```

The above code compares two parent of that same DAG that which would be the best parent for the node given , it is default algo used by RPL the mechanism is as follow:

First it checks that both parent should be from same DAG and this code runs inloop gor every possible parent and the check its combination that fro which parent , is the best one.

It compare both the possible parent rank and then choose the parent which has minimum ranks+ minimum difference , here minimum difference is the minimum difference is the rank difference between two most preffered parent.

□ PSUEDO CODE FOR WPS (RANK ATTACK)

In the WPA when the malicious node attack it changes the objective function of the topologh graph , but here to represent the worst parent attack it chooses the worst parent instead choosing the best parent .

It changes the code of the function best parent as:

```
/* Both parent should be in same DAG
if(rank1>rank2 + mindifference && rank1<rank2 – mindifference)
{
return dag->prefferedparent;
}
else
  if(rank1>rank2)
{
Return parent 1;}
else
{ Return parent 2;
```

Here the mechanism is opposite to previous one as the sign are changed that now they prefer the parent which have the highest rank in the dag so it will be the worst way to form the topology of network through the RPL.it always return the parent which leads to the .worst path.

First from minimum difference from the parent rank it chooses those parent which have highest rank in network then from those worst nodes it then compare those two worst rank nodes and in result it will give the highest ranked node as the parent for the child, and if this function implement to any node results into worst parent attack.

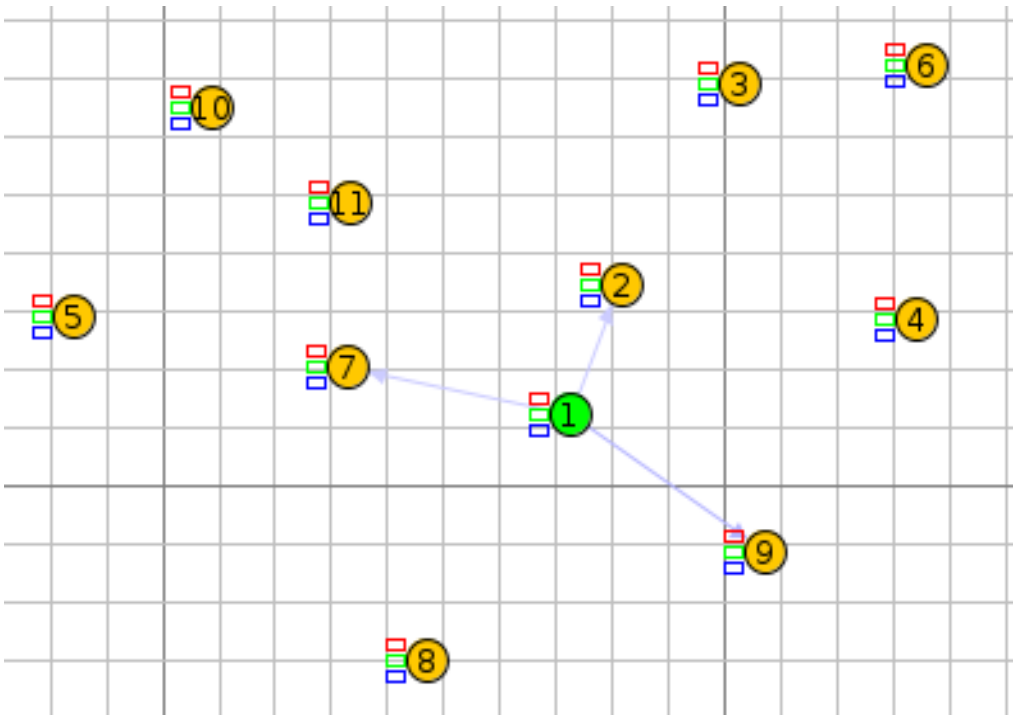
4.1 PERFORMANCE ANALYSIS

To perform the analysis part of the attack and without it ,we made a simulation code

Which shows nodes and their packet forwarding and their paths, parent used and distance between them,the following simulation is done on cooja simulation .

Here node 1 is sink or end Node while all other 10 nodes are source node from where the packets are generating.The arrow shows the connection and forwarding of packets. We first run the simulation without any attack ,then we stores its data about hop used , power consumption and path used then We run another simulation and see another data , the difference in power consumption, and

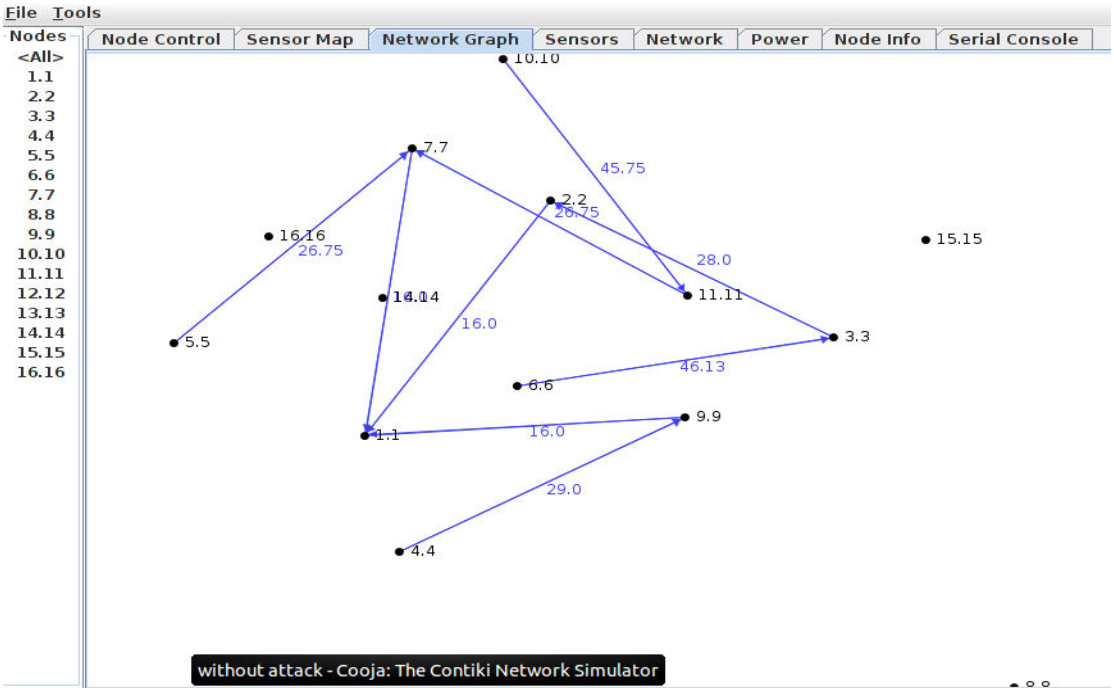
other factors.



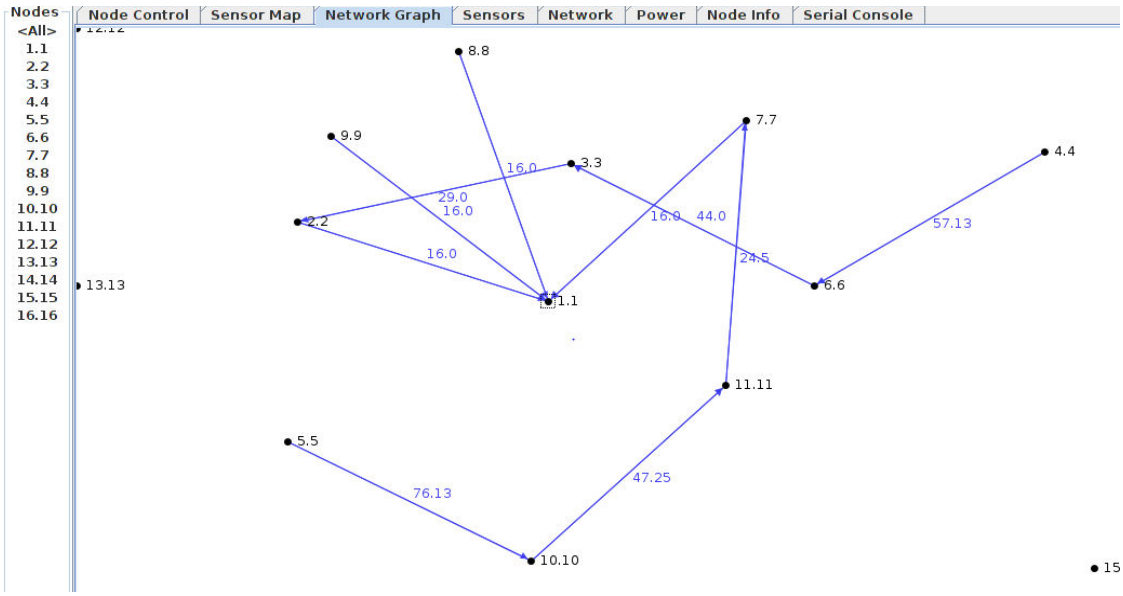
11.

First of all compares we see the network graph of nodes before the attack and changes after the attack:

BEFORE THE ATTACK:



AFTER THE ATTACK: 12.

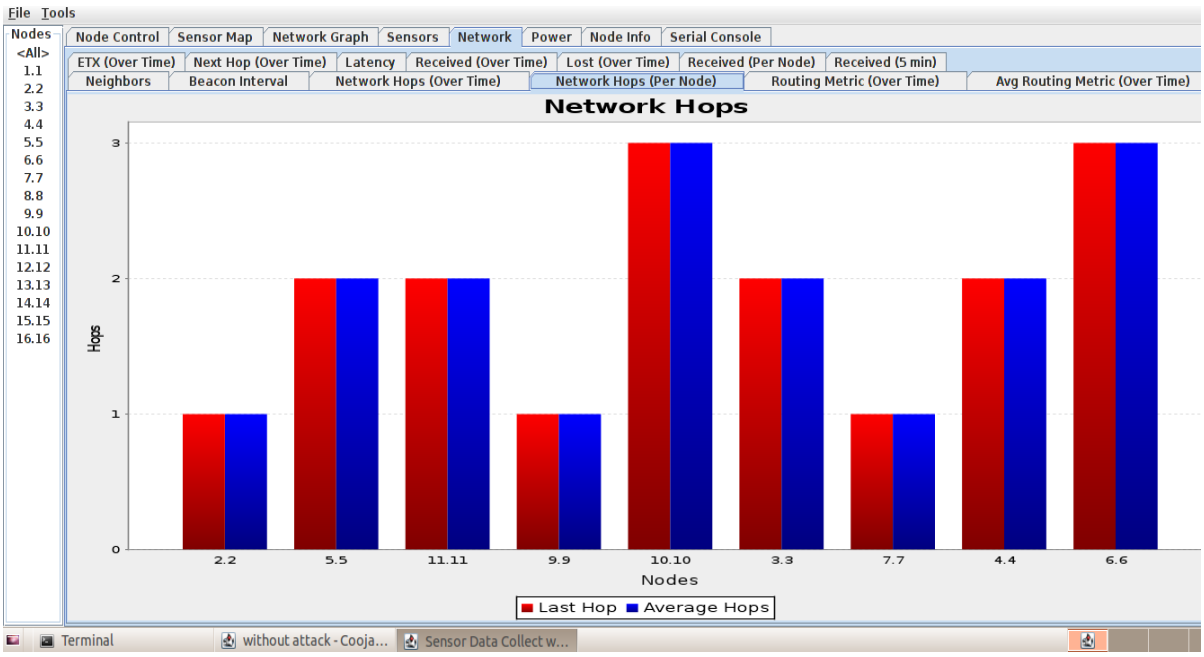


Here in the simulation the sink node is one(1) and the only changes after the attack are in topology path of node 4 and node 5, the numbers on arrow shows the ETX value ,as we can see fromnetwork graph before the attack the ETX VALUE for node 4 and 5 were 29 and 27.65 respectively. But

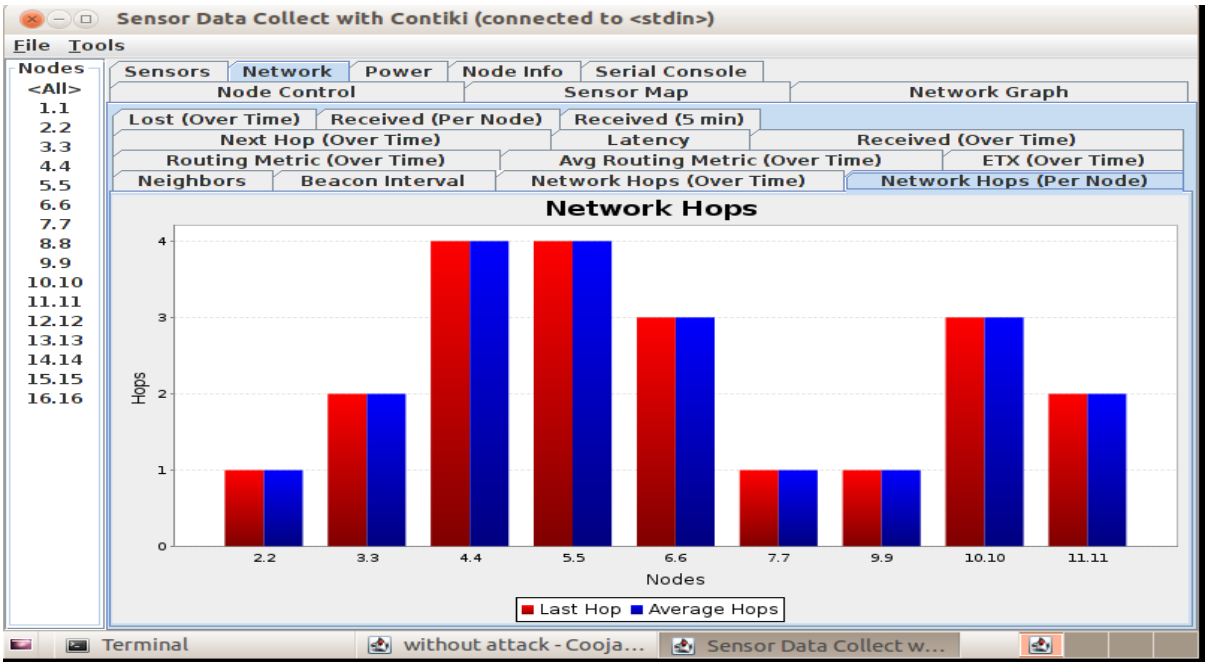
after the attack it increases to 57.13 and 76.13 respectively also their parents changes to worst parent (parent of node 4 change from9 to 6 and parent of node 5 changes from 7 to 10)

First we see the hops used by all nodes to transfer the data to sink nodes:

WHEN THERE IS NO ATTACK:



WHEN THERE IS WORST PARENT ATTACK ON SOME NODES:

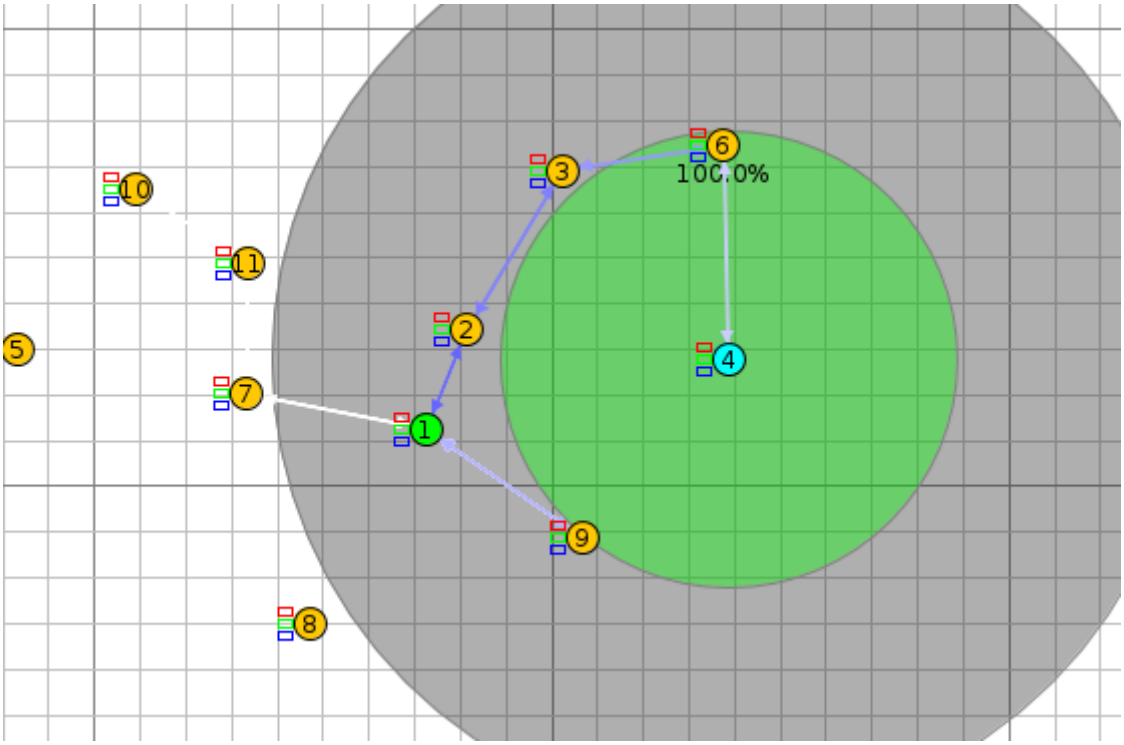


13.

If we analyse both the graphs then we can see many changes in hops used in it :
Like we can notice a great difference in the hop used of node 4 and node 5 , before attack the hops used by node for to reach destination were only 2, but after the attack happens the hops used by node 4 and 5 are increased to 4, that means the difference of 2 nodes , that concludes that after attack the path used by node 4 and node 5 to transfer packets changes after attack,

And that can only happened if they changes the preferred parent .

As we can see the simulation for nodes:

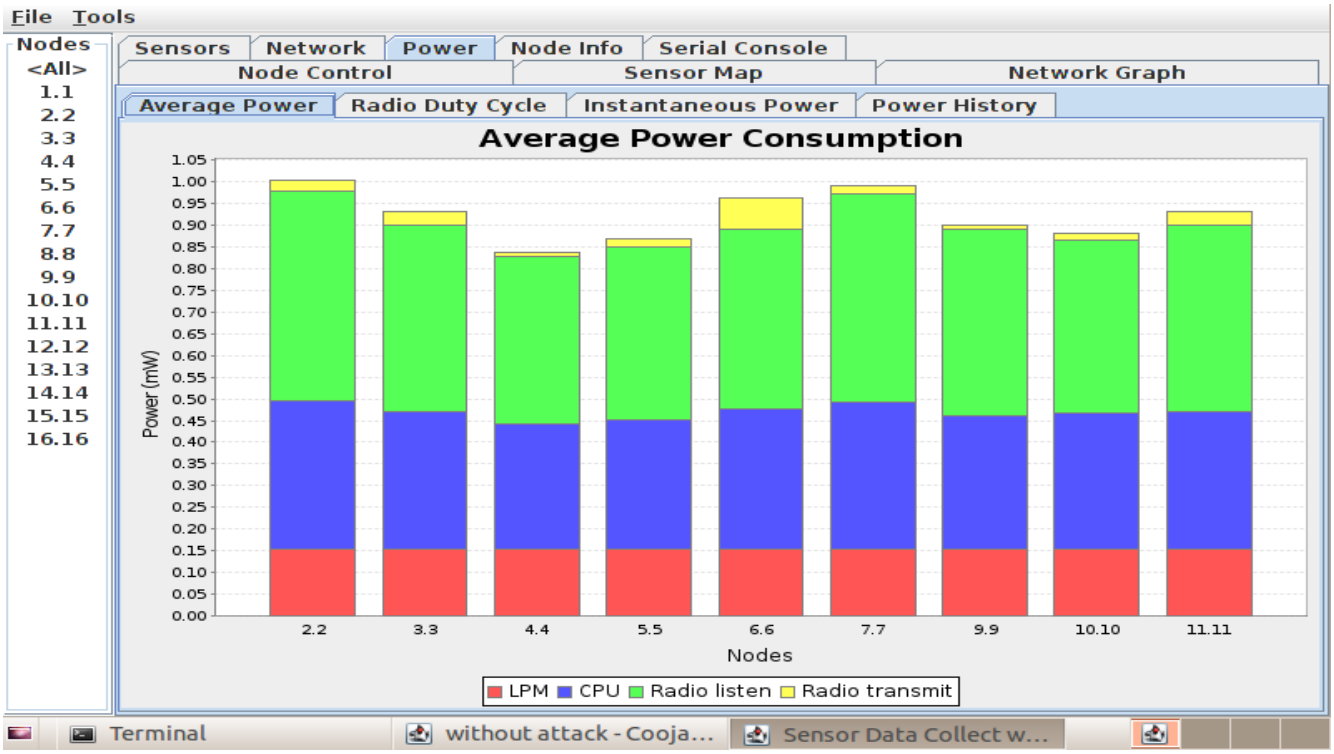


14.

The node 4 is using node 6 as her parent instead of node 9 which shold be the best parent but it uses node 6 as a worst parent that results it to use more hops to transfer data .

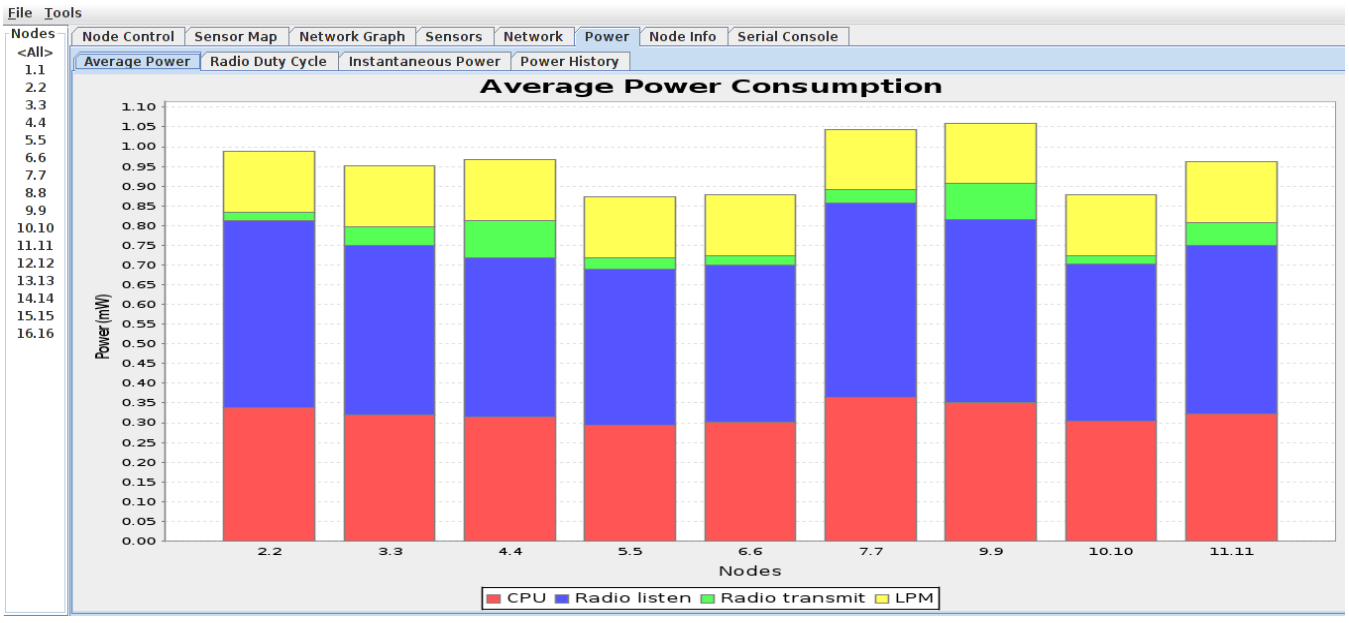
Now we look at the power avg. consumption by each node in transferring the data but keep it mind that the packet is just the “hello” word so there should be not much differenece in power consumption but tiny.

POWER CONSUMPTION BEFORE ATTACK BY NODES:



15.

POWER CONSUMPTION AFTER THE ATTACK HAPPENS:



16.

If we analyse both the cases then we can see that the power consumption difference is not too much , it is because of low traffic and low size of packets but still we can see difference at node 4 and node 5. and LPM increases on all the nodes that shows that " Line Per Minute " increases which means now more paths constructed as worst parent attack comes in action because due to attack it takes longest path to transfer the packets .

If we want see the whole

Nodes info then we have info before attack:

File Tools

Nodes

<All>
1.1
2.2
3.3
4.4
5.5
6.6
7.7
8.8
9.9
10.10
11.11
12.12
13.13
14.14
15.15
16.16

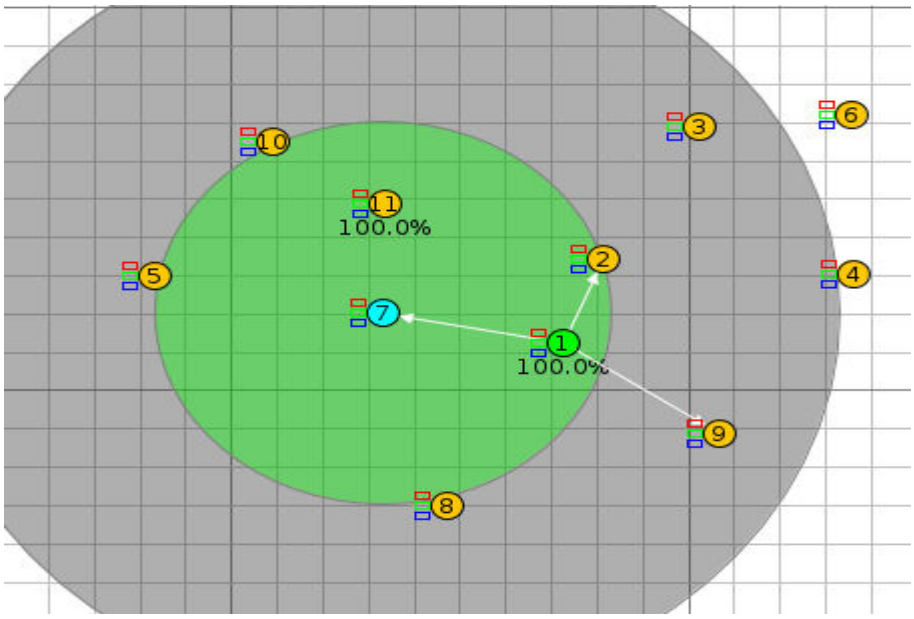
Sensors | Network | Power | Node Info | Serial Console

Node Control | Sensor Map | Network Graph

Node	Received	Dups	Lost	Hops	Rtmetric	ETX	Churn	Beacon Interval	Reboots	CPU Power	LPM Power	Liste
1.1	0	0	0	0.000	0.000	0.000	0		0	0.000	0.000	
2.2	10	0	0	1.000	384.000	16....	0	13 min, 58 sec	0	0.344	0.153	
3.3	1	0	0	2.000	515.000	24....	0	8 min, 44 sec	0	0.317	0.154	
4.4	8	0	0	4.000	940.125	44....	0	14 min, 11 sec	0	0.296	0.155	
5.5	9	0	0	4.000	926.222	44....	0	14 min, 33 sec	0	0.297	0.155	
6.6	8	0	0	3.000	657.500	32....	0	14 min, 11 sec	0	0.323	0.154	
7.7	1	0	0	1.000	384.000	16....	0	8 min, 44 sec	0	0.339	0.153	
8.8	0	0	0	0.000	0.000	0.000	0		0	0.000	0.000	
9.9	9	0	0	1.000	386.222	16....	0	15 min, 31 sec	0	0.315	0.154	
10.10	1	0	0	3.000	689.000	33....	0	8 min, 44 sec	0	0.314	0.154	
11.11	10	0	0	2.000	512.500	24....	0	14 min, 50 sec	0	0.323	0.154	
12.12	0	0	0	0.000	0.000	0.000	0		0	0.000	0.000	
13.13	0	0	0	0.000	0.000	0.000	0		0	0.000	0.000	
14.14	0	0	0	0.000	0.000	0.000	0		0	0.000	0.000	
15.15	0	0	0	0.000	0.000	0.000	0		0	0.000	0.000	
16.16	0	0	0	0.000	0.000	0.000	0		0	0.000	0.000	
Avg	**6.333**	**0.000**	**0.000**	**2.333**	**599.397**	**27....**	**0.000**	**12 min, 36 sec**	**0.000**	**0.319**	**0.154**	

17.

After the attack deployed on root 5 then it change its preffered parent from node 7 to node 10 which have which is worst parent :



18.

Also when the time increases and packets would forward under the attack then there are also analysis of rank attack after some time which shows the long term impact on end to end delay and deliveray ratio as follow shown in figure:

4.2 The main findings of these simulation results can be summarized as follows:

• If the WPA deployed on any node results in change in the packet forwarding route,which results in worst and longer route than it should be , as the parent of the child node changes to the worst parent

• The results of change the graph leads to use more hops to reach destination (or sink node) , so mechanism of more nodes will be used that results in more power consumption , that is opposite of the objective of the RPL as it should be designed for sensors and apparatuses to consume minimum power and transmit the data.

• Last but not least as we can see the long erm affect of this attack , as time passesthe delivery ratio decreases and end to end delay increases at increasing rate .

• Also the attack changes the topology of the network so we can’t track the packet path.

5. HANDLING WPA (RANK ATTACK) IN RPL

5.1 IDS

IDS may be atool or mechanism to sight attacks against a system or a network by analyzing the activity within network or within thesystem itself. Once associate degree attack is detectedthe rank or any other kind of attack IDS could log data concerning it rank attack /or report an alarm. generally, the detection mechanisms in associate IDS are either signature based mostly anomaly based. Signature are to detect the attacks which are pre defined by compare the pattern that matches from the attack which happened in the past. Signatures are from past and keep on the device and any signature matches an exact attack. generally signature primarily based techniquesare easier to use. They need, however, a signature of every attackattack and should store it .

No doubt that specific knowledge of every attack and cost to store it grow with numbers of attacks and different types of attack But this technique cannot detect new attacks like WORST PARENT ATTACK . Also this technique sometimes alarm false attack warning that creates blocking and mis conception by system so transmission problem would be there. These techniques are under development so that there acuuracy is not perfect and have loopholes in them , but our motive is to provide an algorithm to SVELTE that is helpful to find if there is an attack called worst parent attack and in which node it is present in graph so that it can be handled by IDS.

.

5.2 SVELTE

SVELTE: a light-weight nonetheless be intimate ective detects attacks in IoT. we have a tendency to conjointly compliment SVELTE with predistrivuted mini-firewall so as to filter malicious traffic before it reaches the resource unnatural nodes. we have a tendency to style. within the remainder of this section we have a tendency to gift our intrusion detection system.

Placement of SVELTE. the position of AN IDS is a crucial call that reflects the look of AN IDS and also the detection approaches. Keeping in sight the resource unnatural nature of the devices and also the IoT setup , we have a tendency to use a hybrid, centralized and distributed, approach and place IDS modules each within the 6BR and in unnatural nodes. SVELTE has 3 main centralized modules that we have a tendency to place within the 6BR. the primary module, referred to as 6LoWPAN plotter gathers data concerning the RPL network and reconstructs the network within the 6BR. The second module is that the intrusion detection part that analyzes the mapped information and detects intrusion a distributed mini-firewall, is intended to dump nodes by filtering unwanted traffic before it enters the resource unnatural network. The centralized modules have 2 corresponding light-weight modules in every unnatural node. the primary module provides mapping data to the 6BR therefore it will perform intrusion detection. The second module works with the centralized firewall. every unnatural node conjointly includes a third module to handle end-to-end packet loss.

5.3 ALGORITHM USED TO HANDLE THE WPA IN RPL

5.3.1 TO CHECK RANK INCONSISTENCY IN RPL

Checking the rank consistency, means that it alarms if the rank of the present node which we are checking is different from its neighbors or the head o

f cluster which should be in same DIO sequence. It could be find by checking that if the neighbors do not have the newest DIOmessage. There would be an alarm if any DIO message is reported by neighbour or head of cluster which is newer to the present node.

```
for each Neighbour in Member.Neighbour do
  if Member.DIO_seq < Neighbour.Member.DIO_seq then
    alarm fake DIO;
  else if Member.DIO_seq < Neighbour.Member.DIO_seq then
       Neighbour.fault = Neighbour.fault + 0.5 //penalised
   else if Member.DIO_seq = Neighbour.Member.DIO_seq then
       if Member.rank != Neighbour.Member.Rank then
         alarm fake DIO;
       end if
    end if
  end for
end for } }
```

5.3.2 TO CHECK THE RANK RULE IN RPL

This case is for worst parent attack (rank attack) this algorithm takes help of how many hops used by the node to transfer the packet to sink it compares the min hops used by tits neighbour and then gives result weather the attack is there or not.

```
for each Member in Cluster do
  if Member.rank + MinHopRankIncrease < Member.parent.rank then
      alarm rank attack;
  end if
  for each Neighbour in Member.Neighbour do {
      if Member.DAO.parent == 1 then
        if Member.rank – MinHopRankIncrease > Member.child.rank then
          alarm rank attack;
        end if
      end if
   end for
end for }
```

CONCLUSION

RPL is open to many kinds of attacks , one of these attack is WORST PARENT ATTACK in which child chooses its worst parent so that it chooses the worst or longest path opposite to its objective function. In this project we creates a simulation with the help of cooja simulator made changes to objective function of RPL implement code to show the worst parent attack and then analyze the affect of attacks on DODAG , how the change comes in the power consumption of the nodes in transmitting the packets ?, how there is difference in hops used to transmits packets ? and other losses done by this WORST PARENT ATTACK, after analyze the results we conclude that there are many worst losses that the RPL faces like more power consumption by IOT sensors and devices that record data, there is also end to end delay in long time cases and also dilevery ratio decreases as time of attack increases.

In answer of that we design an algorithm to check inconsistency in rank of node so that any changes in rank of nodes would be noticed and also another algorithm for check the rank or WP attack ,that on which node it is happening so that after detecting it SVELTE can detect the attack and can change the nodes objective function to the original as per need so that attack could be handled.

REFERENCES

[1] A Taxonomy of Attacks in RPL-based Internet of Things:Anthea Mayzaud, Remi Badonnel, and Isabelle Chrisment (Received June 23, 2015; revised and accepted July 30 & Aug. 12, 2015)

[2] The Impact of Rank Attack on Network Topology of Routing Protocol for LowPower and Lossy Network Anhtuan Le, Jonathan Loo, Aboubaker Lasebae, Alexey Vinel, Yue Chen, and Michael Chai(EEE SENSORS JOURNAL, VOL. 13, NO. 10, OCTOBER 2013)

[3] SVELTE: Real-time Intrusion Detection in the Internet of Things Shahid Razaa, Linus Wallgrena, Thiemo Voigta(Swedish Institute of Computer Science, Kista, Sweden Department of Information Technology, Uppsala University, Sweden ,June 14, 2013)

[4]A Specification-Based IDS for Detecting Attacks on RPL-Based Network Topology(Anhtuan Le , Jonathan Loo , Kok Keong Chai and Mahdi Aiash - 1 March 2016; Accepted: 5 May 2016; Published: 12 May 2016)

[5]A. Dvir, T. Holczer, and L. Buttyán, “VeRA—Version number and rank authentication in RPL,” in Proc. 8th IEEE Int. Conf. Mobile Adhoc Sensor Syst., Oct. 2011, pp. 709–714.

[6] Raza, S.; Wallgren, L.; Voigt, T. SVELTE: Real-time intrusion detection in the Internet of Things. Ad Hoc Netw. 2013, 11, 2661–2674

[7] Wallgren, L.; Raza, S.; Voigt, T. Routing attacks and countermeasures in the RPL-based Internet of Things. Int. J. Distrib. Sens. Netw. 2013, 2013, 794326.
