Detection of A Black Hole Attack In RPL Using IDS

Project report submitted in fulfillment of the requirement for the degree of Bachelor of Technology

In

Computer Science and Engineering/Information Technology

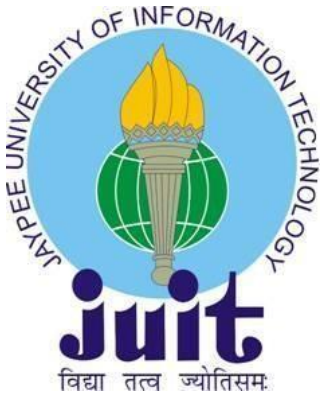
By

Ashish Sharma (123217)
Prakhar Gupta(121307)

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

We hereby declare that the work presented in this report entitled **"Detection Of A Black Hole Attack In RPL Using IDS"** in partial fulfillment 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 carried out over a period from July 2015 to May 2016 under the supervision of **Mr. Arvind Kumar** Assistant Professor, Department of Computer Science And Engineering. The matter embodied in the report has not been submitted for the award of any other degree or diploma.

(Student Signature) (Student Signature)
Ashish Sharma(123217) Prakhar Gupta(121307)

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

(Supervisor Signature)
Mr. Arvind Kumar
Assistant Professor
Department of Computer Science And Engineering
Dated:30/05/2016

`

ACKNOWLEGEMENT

We are grateful and indebted to Mr. Arvind Kumar, Assistant professor, Department of Computer Science And Engineering for his help and advice in completion of this project report. We express our deep sense of gratitude and appreciation to our guide for his constant supervision, inspiration and encouragement right from the beginning of this Seminar report. We also want to thank our parents and friends for their immense support and confidence upon us. We also would like to thank the computer lab staff for their constant technical support. We deem it a pleasant duty to place on record our sincere and heartfelt gratitude to our project guide for his long sightedness, wisdom and co-operation which helped us in tackling crucial aspects of the project in a very logical and practical way.

Ashish Sharma (123217)

Prakhar Gupta (121307)

Computer Science and Engineering

`

Table of Contents

`

`

`

List of Figures`

`

List of Tables

`

List of Abbreviations

1. IP----------Internet Protocol
2. IEEE----------Institute of Electrical and Electronics Engineers
3. LLN----------Low power and lossy network
4. RPL----------Routing Protocol for LLN
5. DIO----------DODAG Information Object
6. DAO----------Destination Advertisement Object
7. TCP----------Transmission Control Protocol
8. DODAG ----------Destination Oriented Directed Acyclic Graph
9. WSN----------Wireless Sensor Network
10. OF----------Objective Function

`

ABSTRACT

Internet of Things (IoT) has been a very trending research topic in the recent times, where physical objects interconnect as a result of conjunction of various existing technologies. IoT is rapidly developing, but there have been uncertainties about its security and privacy which can affect its sustainability. The network layer which is both wired or wireless is exposed to many kinds of attacks. Because of the openness of these wireless channels, communications can be easily monitored. This Project involves designing and implementing the security algorithms which can be of three types: Routing Security, Data Privacy and Authentication.

Authentication is the process of identifying users, computers, devices and machines in networks and restricting access to authorized people and non-manipulated devices. Processes of authentication typically rely on usernames and passwords, which are not particularly secure, but require frequent changing and do not work with unattended devices. Cryptographic mechanisms are a more stable way of securing communication over the Internet of Things. Particularly in embedded systems, where security demands are rising to protect against counterfeiting, firmware tampering and illegal access, strong cryptography is the only way to fulfill today's needs.

Routing Security is based on prevention against hackers who can easily access smart products wirelessly which can be devastating for some persons.

Data Privacy: - Data by one click can be deleted leading to breakdown of firm's most secured information about finance and other dealings. Hence keeping the data secure has to be the major functionality of smart products.

`

1. INTRODUCTION

1.1 The Internet-of-Things

1.1.1 About IoT

People say that the Internet has fundamentally changed society may be right, but at the same time, the greatest transformation actually still lies ahead of us. Several new technologies are now converging in a way that means the Internet is on the brink of a substantial expansion as objects large and small get connected and assume their own web identity. Following on from the Internet of computers, when our servers and personal computers were connected to a global network, and the Internet of mobile telephones, when it was the turn of telephones and other mobile units, the next phase of development is the Internet of things, when more or less anything will be connected and managed in the virtual world. This revolution will be the Net's largest enlargement ever and will have sweeping effects on every industry — and all of our everyday lives[1].Coming to its definition ,the Internet of Things is the network of physical objects or "things" embedded with electronics, software, sensors, and network connectivity, which enables these objects to collect and exchange data. The Internet of Things allows objects to be sensed and controlled remotely across existing network infrastructure, creating opportunities for more direct integration between the physical world and computer-based systems, and resulting in improved efficiency, accuracy and economic benefit. Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure. Smart connectivity with existing networks and context-aware computation using network resources is an indispensable part of IOT. With the growing presence of WiFi and 4G-LTE wireless Internet access, the evolution towards ubiquitous information and communication networks is already evident. However, for the Internet of Things vision to successfully emerge, the computing paradigm will need to go beyond traditional mobile computing scenarios that use smart phones and portables, and evolve into connecting everyday existing objects and embedding intelligence into our environment[1].

`

Fig.1.1.1 IOT Devices Interconnections

1.1.2 Growth of the IoT

An important inflection point occurred in 2008, when the number of things connected to the Internet surpassed the human population. The adoption rate of the IOT is trending to be at least five times faster than the adoption of electricity and telephony, shown in Figure 1. This equates to about six things for every person on earth [2]. An interesting trend contributing to the growth of the IOT is the shift from the consumer-based IPv4 Internet of tablets and laptops, that is, Information Technology (IT), to an Operational Technology (OT)-based IPv6 Internet of Machine-to-Machine interactions. This includes sensors, smart objects and clustered systems (for example, Smart Grid).

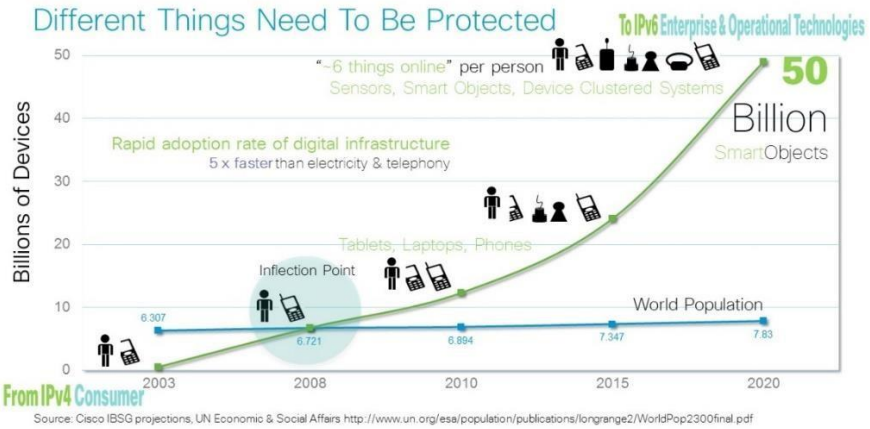


Figure 1.1.2 IOT Growth

`

1.1.3 Common Challenges

In many cases, a major disruption of the traditional model brings its own set of challenges. The following lists some security challenges and considerations in designing and building IOT devices or systems:

- Typically small, inexpensive devices with little to no physical security
- Computing platforms, constrained in memory and compute resources, may not support complex and evolving security algorithms.
- Designed to operate autonomously in the field with no backup connectivity if primary connection is lost
- Mostly installed prior to network availability which increases the overall on-boarding time
- Requires secure remote management during and after onboarding
- Scalability and management of billions of entities in the IOT ecosystem
- Management of Multi-Party Networks
- Physical Protection
- Tamper Detection techniques and design

1.2 Types of Topologies

1.2.1 Bus Topology

Bus topology is a network type in which every computer and network device is connected to single cable when it has exactly two endpoints, then it is called Linear Bus topology.

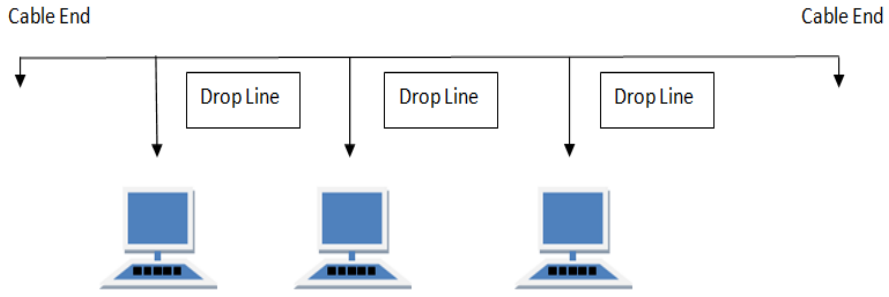


Figure 1.2.1 Bus Topology

`

Its basic features are:-

- It transmits data only in one direction.
- Every device is connected to a single cable

Its Advantages:-

- It is cost effective.
- Cable required is least compared to other network topology.
- It's used in small networks.
- It is easy to understand.
- Easy to expand joining two cables together.

Disadvantages of Bus Topology:-

- Cables fails then whole network fails.
- If network traffic is heavy or nodes are more the performance of the network decreases.
- Cable has a limited length.
- It is slower than the ring topology.

1.2.2 Ring Topology

It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbours for each device.

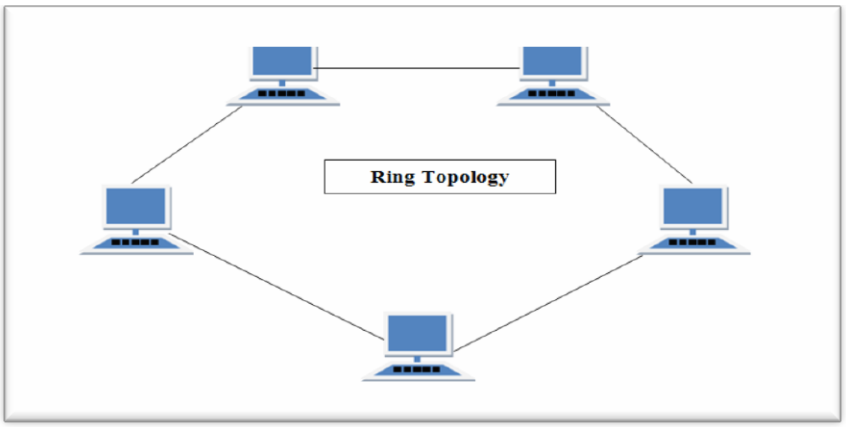


Figure 1.2.2 Ring Topology

`

Features of Ring Topology:-

- A number of repeaters are used for Ring topology with large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.
- The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called Dual Ring Topology.
- In Dual Ring Topology, two ring networks are formed, and data flow is in opposite direction in them. Also, if one ring fails, the second ring can act as a backup, to keep the network up.
- Data is transferred in a sequential manner that is bit by bit. Data transmitted, has to pass through each node of the network, till the destination node.

Advantages of Ring Topology:-

- Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
- Cheap to install and expand

Disadvantages of Ring Topology:-

- Troubleshooting is difficult in ring topology.
- Adding or deleting the computers disturbs the network activity.
- Failure of one computer disturbs the whole network.

`

1.2.3 Star Topology

In this type of topology all the computers are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node.

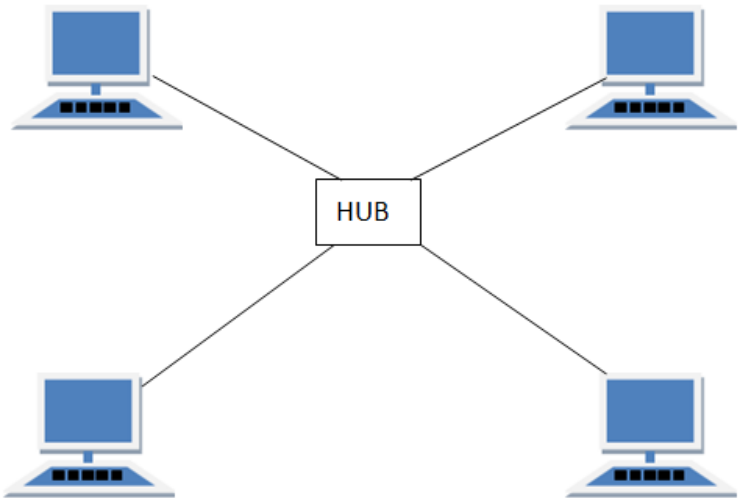


Figure 1.2.3 Star Topology

Features of Star Topology:-

- Every node has its own dedicated connection to the hub.
- Hub acts as a repeater for data flow.
- It can be used with twisted pair, Optical Fibre or coaxial cable.

Advantages of Star Topology:-

- Fast performance with few nodes and low network traffic.
- Hub can be upgraded easily.
- Easy to troubleshoot.
- Easy to setup and modify.
- Only that node is affected which has failed, rest of the nodes can work smoothly.

`

Disadvantages of Star Topology

- Cost of installation is high.
- Expensive to use.
- If the hub fails then the whole network is stopped because all the nodes depend on the hub.
- Performance is based on the hub that is it depends on its capacity

1.2.4 Mesh Topology

It is a point-to-point connection to other nodes or devices. All the network nodes are connected to each other. Mesh has `n(n-2)/2` physical channels to link `n` devices. There are two techniques to transmit data over the Mesh topology, they are:

- Routing
- Flooding

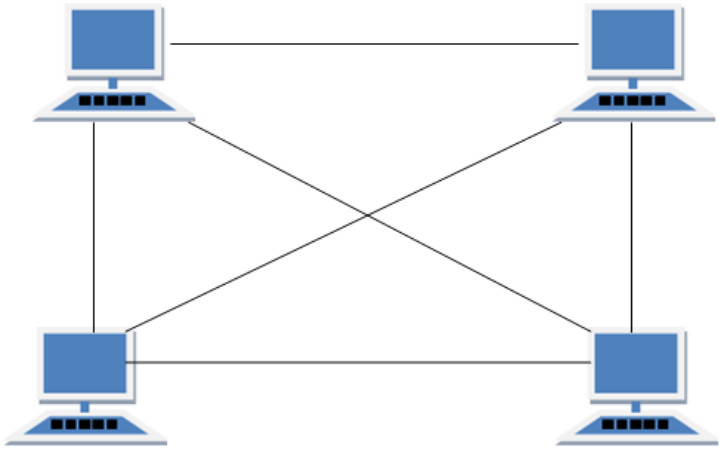


Figure 1.2.4 Mesh Topology

`

Routing:-

In routing, the nodes have a routing logic, as per the network requirements. Like routing logic to direct the data to reach the destination using the shortest distance. Or, routing logic which has information about the broken links, and it avoids those node etc. We can even have routing logic, to re-configure the failed nodes.

Flooding:-

In flooding, the same data is transmitted to all the network nodes, hence no routing logic is required. The network is robust, and then it's very unlikely to lose the data. But it leads to unwanted load over the network.

Types of Mesh Topology:-

- Partial Mesh Topology**:** In this topology some of the systems are connected in the same fashion as mesh topology but some devices are only connected to two or three devices.
- Full Mesh Topology**:** Each and every nodes or devices are connected to each other.

Features of Mesh Topology:-

- Fully connected.
- Robust.
- Not flexible.

Advantages of Mesh Topology:-

- Each connection can carry its own data load.
- It is robust.
- Fault is diagnosed easily.
- Provides security and privacy.

Disadvantages of Mesh Topology:-

- Installation and configuration is difficult.
- Cabling cost is more.
- Bulk wiring is required.

`

1.2.5 Tree Topology

It has a root node and all other nodes are connected to it forming a hierarchy. It is also called hierarchical topology. It should at least have three levels to the hierarchy.

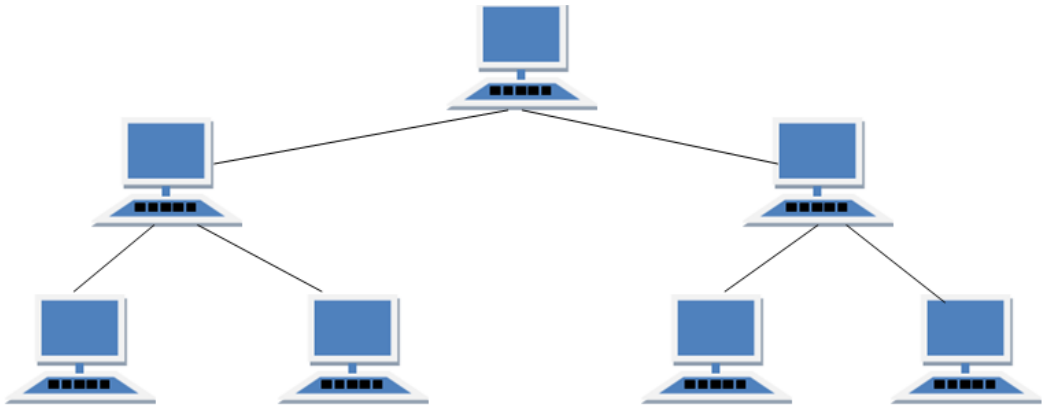


Figure 1.2.5 Tree Topology

Features of Tree Topology:-

- Ideal if workstations are located in groups.
- Used in Wide Area Network.

Advantages of Tree Topology:-

- Extension of bus and star topologies.
- Expansion of nodes is possible and easy.
- Easily managed and maintained.
- Error detection is easily done.

Disadvantages of Tree Topology:-

- Heavily cabled.
- Costly.
- If more nodes are added maintenance is difficult.

`

Note: - From All these network topologies we have considered tree topology in our project.

1.3 Problem Statement

Routing Protocols for Low power and Lossy networks cannot construct network proactively to exchange information where the conventional communication infrastructure do not exist. However, these Networks have vulnerability in data security due to their characteristics of network protocol. The Black Hole Attack is the major risks in these Networks as an attacker makes faulty route by responding fake network information to the information source, and intercepts data through faulty route they made. In this project, a Low power and lossy Network is to be constructed, and analyze the results from the simulation of the Black Hole Attack by using the cooja simulator.

1.4 Aims And Objectives

The overall aim is to analyze a Black Hole attack on a low power and lossy network in 6LoWPAN and design a detection system for the same.

1.5 Methodology

In our project we simulate a Black Hole Attack based on RPL on the Linux based simulator COOJA. Our prime methodology is to detect the malicious node which makes faulty route by responding fake network information to the information source, and intercepts data through that faulty route.

`

1.6 Organisation

In Chapter 1 we have discussed about IOT basics, the current growth in this field, the common challenges being faced by persons in implementing the IOT structure and finally the different types of network topologies.

In Chapter 2 we would be providing with the basic terminology about the different research paper read by us. We would be providing with facts and figures about different concepts we studied in those research papers.

In Chapter 3 we are going to provide a model of how the project is done on the basis of developments:-

• Analytical

• Experimental

• Statistical

In Chapter 4 we have given a proper analysis on Black Hole attack on basis of which we will be implementing and detecting the behavior of malicious node.

`

2. LITERATURE SURVEY

A literature review is a means to evaluate and interpret all available research relevant to a particular research question, or area. Its main aim is to present a fair evaluation of the research area of interest by conducting a rigorous and auditable methodology. The main purpose of our literature review is to find the relevant literature about Black Hole attack upon low power and lossy networks and their network protocols for the purpose of background study, summarize the existing work and identify the gap in the current research.

2.1 General Architecture Of IoT

Generally, IOT has four main key levels as shown in Fig. 2.1, which is described below[4]:

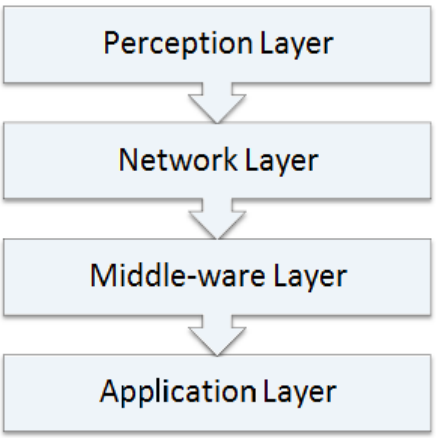


Fig. 2.1 Generic Architecture of IOT

2.1.1 Perception Layer

This layer consists of different kinds of data sensors like RFID, Barcodes or any other sensor network. The basic purpose of this layer is to identify the unique objects and deal with its collected data obtained from the real world with the help of its respective sensor(s).

`

2.1.2 Network Layer

The purpose of this layer is to transmit the gathered information obtained from the perception layer, to any particular information processing system through existing communication networks like Internet, Mobile Network or any other kind of reliable network[5].

2.1.3 Middle-ware Layer

This layer consists of information processing systems that take automated actions based on the results of processed data and links the system with the database which provides storage capabilities to the collected data. This layer is service-oriented which ensures same service type between the connected devices[6].

2.1.4 Application Layer

This layer realizes various practical applications of IOT based on the needs of users and different kinds of industries such as Smart Home, Smart Environment, Smart Transportation and Smart Hospital etc[7].

2.2 Analyzing the Security Concerns Of IOT

The major security goals of IOT are to ensure proper identity authentication mechanisms and provide confidentiality about the data etc. The Security triad or CIA triad, a distinguished model for the development of security mechanisms, implements the security by making use of the three areas which are Data confidentiality, integrity and availability as shown in the Fig. 2.2. A breach in any of these areas could cause serious issues to the system so they must be accounted for. The three areas are described below:

`

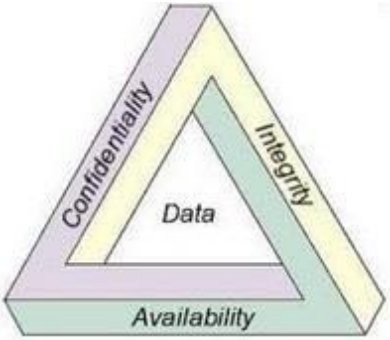


Fig.2.2.1 The CIA Triad

2.2.1 Data Confidentiality:-

Data confidentiality is identical to providing safeguard to user from the external attacks. It is the ability to provide safety to user about the privacy of the valued information by using different mechanisms such that its disclosure to the unauthorized party is prevented and can be accessed by the permitted users only. There are many security mechanisms to provide confidentiality of the data including, but not limited to, Data Encryption in which the data is converted into cipher text form which makes it difficult to access for the users having no proper authorizations, the Two-step verification, which provides authentication by two dependent components and allows the access only if both the components pass the authentication test and the most common Thumb Verification in which every person is uniquely identifiable. For the IOT based devices, it ensures that the sensor nodes of the sensor networks don't reveal their data to the other nodes, similarly the tags don't transmit their data to an unauthorized users.[8]

2.2.2 Data Integrity

During the transmission, data could be altered by the cyber attackers or could be affected by various other factors that are beyond human control including the crash of server or an electromagnetic anomaly. Data Integrity refers to the safeguard of useful information from the cybercriminals or the external interference during transmission and reception with some common tracking methods, so that the data cannot be faulted without the system catching the threat.[9] The methods to ensure the accuracy and originality of data includes methods like Checksum and Cyclic Redundancy Check (CRC) which are simple error detection

`

mechanisms for a portion of data. Moreover, continuous syncing of the data for backup purposes and the feature like Version control, which keeps a record of the file changes in a system to restore the file in case of various deletion of data can also ensure the integrity of data such that the data on IOT based devices is in its original form when accessed by the authorized users.

2.2.3 Data Availability

One of the major goals of IOT security is to make data availability to its users, whenever needed. Data Availability ensures the instant access of permitted party to their information resources not only in the normal conditions but also in disastrous conditions. Due to dependency of companies on it, it is necessary to provide firewalls to counterback the attacks on the services like Denial of- service (DoS) attack which can deny the availability of data to the user-end. Data Availability also ensure the prevention of bottleneck situations which prevent the flow of information. The Redundancy and Failover backup methods provide duplication of the system components in conditions of system failure or various system conflictions to ensure reliability and availability of data.

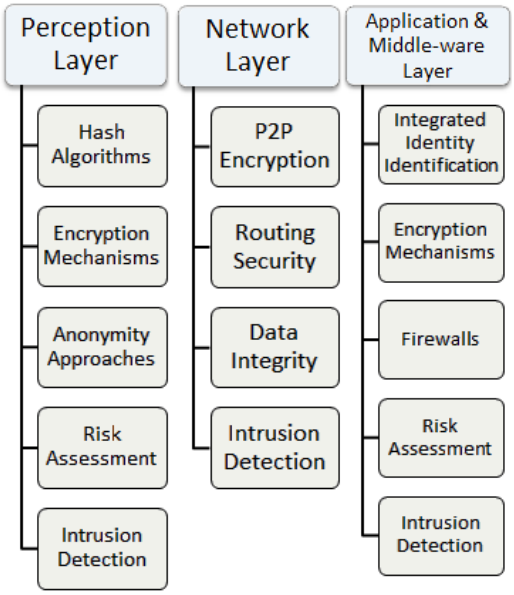


Fig.2.2.2 Security Architecture of IOT [10]

`

2.3 Routing protocols In Internet of Things

2.3.1 Overview of 6LoWPAN

The 6LoWPAN standard has been launched recently, but it already shows a good future. The first two 6LoWPAN specifications, RFC 4919 and RFC 4944, were released in 2007. The first one specifies requirements of 6LoWPANand goals while the other presents its functionalities and different formats. The working group has been improving other mechanisms of the standard like header compression, neighbour discovery, use cases and routing requirements. The improved 6LoWPAN standard has been emerging and attracts the interest of many research groups in this field so that the Zigbee , a research group that specializes in ad hoc and 802.15 network, announced that it would integrate IETF standards such as 6LoWPAN and RPL into its future specifications in 2009.[11]

2.3.1.1 Network Topology

The 6LoWPAN network contains many local LoWPANs, which are all connected to the Internet through a gateway, by IPv6. These devices are characterized by short radio range, low data rate, low power. The network deals with small packet size, low bandwidth and requires power saving for maintaining the life of nodes. 6LoWPAN supports both star and peer-to-peer topology; however, the topology can be changed frequently because of uncertain radio frequency, mobility or battery drain. Figure 2.3.1.1 shows the difference between the protocol stacks of 6LoWPAN and a typical IP network. In the typical model, IP is the only protocol used to connect different protocols from the data link and physical layer to multiple upper layer protocols. In 2008, another IETF working group, Routing over Low-power and Lossy Network (ROLL), was formed to establish a routing solution for such a network. This group proposed RPL (Routing protocol for Low-power and Lossy network), which was later considered the underlying routing protocol for 6LoWPAN. Improving the RPL operation is a

`

critical mission for the network to manage a huge number of nodes with resource constraint characteristic.[11]

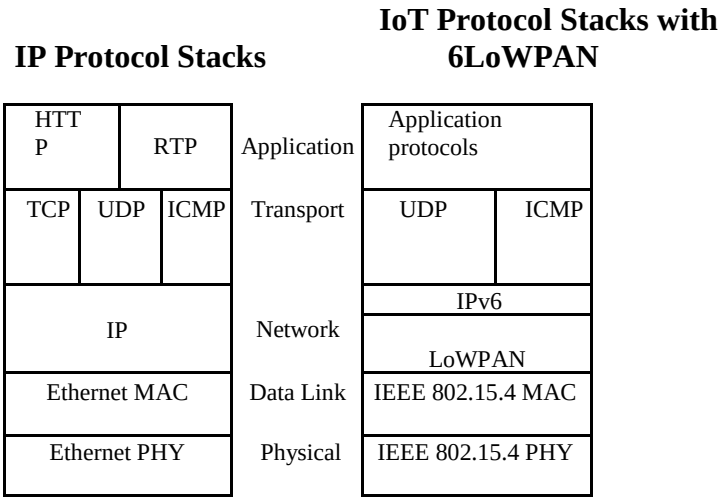


Figure 2.3.1.1 Comparison of 6LoWPAN and typical IP protocol stacks.[3]

2.3.2. Routing protocol for low-power and lossy network framework

2.3.2.1. RPL overview

The 6LoWPAN standard has been designed to operate in a network with large number of embedded sensor devices over low data-rate wireless links. Such criteria are specified in the routing requirements defined in RFC 5867 , 5826 , 5673 and 5548, with a core mandated list in which a candidate 6LoWPAN routing protocol must satisfy the following: (i) support different types of communication Unicast/any cast/multicast; (ii) adaptive routing with different network condition; (iii) constraint-based; (iv) support different traffic: multipoint-to-point (sensor nodes to sink manner), point-to-multipoint (sink broadcasts) and point-to-point traffic (sensor nodes communicate to each other); (v) scalability; (vi) configuration and management; (vii) node attribute; (viii) performance; and (iv) security. The ROLL working group extensively evaluated the existing routing protocols, such as OLSR (Optimized Link

`

State Routing Protocol), RIP (Routing Information Protocol), AODV (Ad hoc on demand Distance Vector Routing Protocol), etc. and concluded that none of them could satisfy the requirements. So the ROLL group proposed the RPL, which was specified according to all these requirements and later was considered an underlying protocol for these kind of networks. Besides that, looking at security problems of 6LoWPAN, routing is the weakest part because the nodes are easy to be compromised while they are travelling frequently in the routing networks, and contact with the new unauthenticated neighbors leads to many routing attacks. Therefore, it is much necessary to look at the RPL operation for further optimizing the 6LoWPAN security.[11]

2.3.2.2 RPL architecture and operations

RPL components consist of WSN nodes, which act as host routers for transmitting packets in WSN. 6LoWPAN nodes connect with Directed Acyclic Graph (DAG) topology to prevent any network loop. This DAG is then separated into multiple Destination Oriented DAG (DODAG), where the roots of these DODAG are normally local border router, which connect together and to the Internet through the backbone. The DODAG is considered a logical configuration on physical nodes, so a node can join multiple DODAGs to support routing optimization. Nodes in DODAG select and optimize the path using some node/link metrics and constraints, called DODAG instances such as node state, node energy, hop count, throughput, latency, link reliability, and link colour attribute. The node uses the objective functions to point out particular metrics chosen for optimizing route, represented by Objective Code Point (OCP). On the basis of objective functions and path cost toward the root, the Rank (or depth) of nodes is calculated to differentiate their relationship. At the building phase, the DODAG root starts broadcasting its DODAG Information Objective (DIO) message, which contains information about its rank, OCP and DAG-ID. All root neighbours have a direct path toward the root, so they set their rank to 1, add root address as their parent, update and continue broadcasting their own DIO. Once nodes in the network receive DIO, they form a set of parent nodes and select a preferred parent, which will be their default next hop towards the root. They then calculate their own rank based on the rank of their parent and cost path, and form their own DIO, which includes rank, OCP and DODAG-

`

ID, to broadcast again. By this broadcasting mechanism, the DIO is propagated throughout the network. Every node then knows the path to the root, and the DODAG topology is created.[3] When a node joins the network it can either wait for a DIO or send a DODAG Information Solicitation message (DIS) to ask others to send DIO if the waiting time is long. Once this node receives a DIO, it chooses its preferred parent and builds a Destination Advertisement Object (DAO) message, which contains its address and prefix parent. This DAO is advertised for other nodes to update their rooting table or optimise their parents if possible. On operation, if a link is broken somewhere, RPL provides two mechanisms to fix it. The first one, Global Repair, starts by DODAG root sending a new DAG sequence number to recalculate the whole topology. Once nodes receive new DIO messages, they can start parent selection and update the link cost again. If a local node suffers from a broken link and it does not want to wait a long time for Global Repair, it can use the Local Repair mechanism. This node first sends the poison message to all its children informing that they need to update their parent. It then sends a DIS message to get the new topology information like the first time it joins the network.[11]

2.4 Loopholes In 6LoWPAN Security

6LoWPAN is comprised of WSN and IPv6, therefore security threats from both have to be examined. There are also threats that aim at the adaptation layer of 6lowpan to attack the translation process of packets. The 6LoWPAN operation is represented by the performance of RPL; it is also necessary to analyze the threats towards this protocol.

2.4.1 Security threats in WSN

The security threats of WSN have been widely studied by the research community. The attacks can be divided by several schemes: outsider–insider adverse source, passive–active, compromising methods, host-based or network-based. From the protection threat's point of view, detection of the attacks from the outsider and insider requires different protection systems. The attackers outside of the network can start a passive attack such as unauthorized listening or active attack like denial-of-service (DoS), for example, jamming or power exhaustion. New malicious nodes can be created by several ways: attackers physically

`

capture the nodes and reprogram them, attackers can use software devices to breach the cryptographic keys or inject malicious code. One example is a Sybil attack, which uses the packet forging mechanism and leads to multiple types of other attacks like misdirection, exhaustion and unfairness. It will make the WSN unavailable, partitioned or resource exhausted. Another dangerous attack is the Sinkhole, which uses a packet dropping mechanism to attract traffic to a specific node. It generates selective forwarding, black hole attack and combines to partition the network. Besides that, when applying some IPv6 mechanisms like neighbour discovery and address auto-configuration in WSN, there are neighbour discovery threats as detailed in RFC 3756.[12]

2.4.2 Security threats from the internet side

End-users from the Internet can access information from the sensor field once 6LoWPAN is implemented. This increases the threats of authentication from users and sensor motes, sensor network availability and user accountability. The adversary can access the info illegally if no authenticated mechanism is applied to the network. When a communication channel between end-user and sensor network is established, the attacker can also eavesdrop on the sensitive info from the data stream, which breaks the network integrity. Besides that, the accountability of the users accessing the sensor network should be considered for detecting and recreating security incidents.[3]

2.4.3 Security threats from the routing protocol for low-power and lossy network

Current RPL threats directly interfere the routing operation by changing the route, making it longer or even changing the receiving address so that the time waiting for a packet goes to infinite. Threats on other layers that aim at resource consuming such as flooding and overwhelming, or destroying network traffic like jamming or congestion can also be considered indirect attacks to the routing part because they degrade the node operation. RPL is also vulnerable from passive eaves-dropping attacks and active tampering. Tampering active nodes, however, creates compromised nodes, which can cooperate to break the protocol operation rules and easily overcome the cryptography line. Besides that, RPL utilizes some specific rules for optimization of network operation; nevertheless, adversaries can exploit these to create different attacks. Potential attacks of these kinds are ranked, local repair and resource depletion attack.[11]

`

2.5 Security In 6LoWPAN

6LoWPAN needs to have a very strong security defense in place. However, security techniques from other networks cannot be straight away applied in this network because of many of its specific constraints. WSN is the network that has the nearest nature to 6LoWPAN therefore, WSN security mechanisms are preferred to be used in that network. This section examines the most prominent techniques that might be helpful in applying for 6LoWPAN.

2.5.1 Cryptography techniques

By encrypting messages before transmitting, the cryptography solutions aim at threefold protection: authentication — only the authenticated user, who has the right key, can decrypt and read the messages; integrity — message content should not be changed during transmission; and confidentiality — no one can understand the message without the key. The encryption methods for 6LoWPAN should be developed more to adapt to the prevailing constraints in 6LoWPAN devices such as low power and low computing ability. This is because unoptimised cryptography mechanisms will consume more resources and therefore, shorten network life time. Cryptography is also only helpful while protecting 6LoWPAN from the external attacks, but lacks the ability in detecting and eliminating internal attacks. There is a need for implementing IDS to monitor any malicious behavior of the network to prevent early security attacks to decrease its effects. IDS is an efficient way for discovering any attacker that bypasses the cryptography defense line, and ensuring a normal operation of the network.[11]

2.5.2 Intrusion detection system techniques

2.5.2.1. IDS Overview

The intrusion detection system is a well-known network security approach. The main idea behind it has been to collect the data from network and monitor any sign of attack that could raise an alarm and discover that resource. The development of technology has changed the

`

communication environment from wired or wireless or ad hoc to sensor network recently. IDS solutions have changed from data collection and analytical techniques to adapting the implemented environment. IDS applied in WSN should optimize the features and computational work for saving network resource. With regard to 6LoWPAN, the optimization ability of the IDS is more required because of the scalability in the network. The IDS approaches are divided by misuse, anomaly-based or specification-based type.

2.5.2.2 Application of IDS

6LoWPAN is still an on-going research area. Right now there are only a few security solutions proposed for the standard security. Cryptography solutions focus on choosing a fast, and secured encryption, and an effective key management method. Even when 6LoWPAN has an ideal cryptography defense, it still requires an IDS for dealing with network performance threats such as DoS and other resource attacks. The IDS will discover and stop most of the attacks that break cryptography line of defense to make changes on the network operations. However, till now no IDS solution has been proposed for 6LoWPAN security

`

3. SYSTEM DEVELOPMENT

3.1 Distance Vector Routing Protocol:-

It is one of the two major classes of intra domain routing protocols, the other major class being the link-state protocol. Distance-vector routing protocols use the Bellman–Ford algorithm, Ford–Fulkerson algorithm, or DUAL FSM (in the case of Systems' protocols) to calculate paths.

3.1.1 Working of DVRP

In distance vector routing, the least-cost route between any two nodes is the route with minimum distance. In this protocol, as the name implies, each node maintains a vector (table) of minimum distances to every node. The table at each node also guides the packets to the desired node by showing the next stop in the route (next-hop routing).

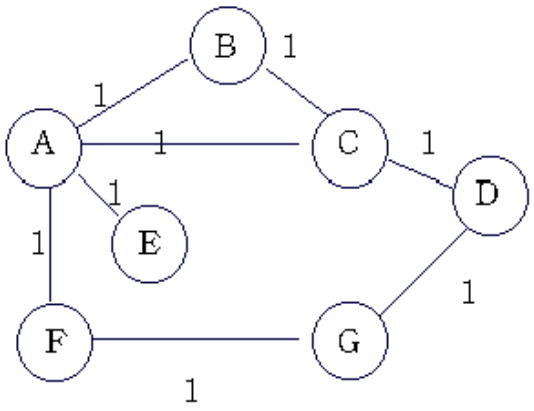


Fig.3.1.1 DVRP graph

`

Information Stored at Node	A	B	C	D	E	F	G
A	0	1	1	-	1	1	-
B	1	0	1	-	-	-	-
C	1	1	0	1	-	-	-
D	-	-	1	0	-	-	1
E	1	-	-	-	0	-	-
F	1	-	-	-	-	0	1
G	-	-	-	1	-	1	0

Table 3.1.1.1: '-'represents the node is not directly reachable

1. A sends its information to its neighbors B, C, E, and F.
2. Node B learns from A that node E can be reached at a cost of 1; B also knows it can reach A at a cost of 1, so it adds these to get the cost of reaching E by means of A. B records that it can reach E at a cost of 2 by going through A.
3. After every node has exchanged a few updates with its directly connected neighbors, all nodes will know the least-cost path to all the other nodes.
4. B knows that it was A, who said " I can reach E in one hop" and so B puts an entry in its table that says "To reach E, use the link to A.

Information Stored at Node	**Distance to Reach Node**						
	A	**B**	**C**	**D**	**E**	**F**	**G**
A	0	1	1	2	1	1	2
B	1	0	1	2	2	2	3
C	1	1	0	1	2	2	2
D	□	2	1	0	3	2	1
E	1	2	2	3	0	2	3
F	1	2	2	2	2	0	1
G	□	3	2	1	3	1	0

Table 3.1.1.2: Final distances stored at each node (Global View)

`

In practice, each node's forwarding table consists of a set of triples of the form:

(Destination, Cost, Next Hop).

For example, Table 3.1.1.3 shows the complete routing table maintained at node B for the network in figure 3.1.1.1

Destination	Cost	Next Hop
A	1	A
C	1	C
D	2	C
E	2	A
F	2	A
G	3	A

Table 3.1.1.3: Routing table maintained at node B

3.1.2 Problems with Distance Vector Routing:-

Routing Loops:-

A routing loop is a condition in which a packet is continuously transmitted within a series of routers without ever reaching its intended destination network. A routing loop can occur when two or more routers have inaccurate routing information to a destination network. The loop can be a result of:

- Incorrectly configured static routes
- Inconsistent routing tables not being updated because of slow convergence in a changing network

`

Count-to-Infinity Condition:-

Count to infinity is a condition that exists when inaccurate routing updates increase the metric value to "infinity" for a network that is no longer reachable. Remember that in Distance Vector RIP routing, the metric is hop count. When a router sends an update to a neighbor, it increments the hop count of each current route it knows about by 1.

3.2 Use of RPL Network

In a blackhole attack, a malicious node copies a destination node by sending an alternate route reply packet to a transmission node that initiates a routing discovery. By doing this, the malicious node can deprive the traffic from the source node. Simulations are done using Cooja Simulator that consists of the collection of all network protocols. To simulate Black Hole attacks, a new Black Hole protocol is added into the Cooja Simulator. The protocol is written using C language which involves the implementation of DODAG which comes under RPL networking. Having implemented the routing protocol which simulates the black hole, network performance is compared with and without black holes in the network. As expected, the throughput in the network was less considerably in the presence of a black hole. Afterwards, an IDS system is proposed towards detection of the malicious node.

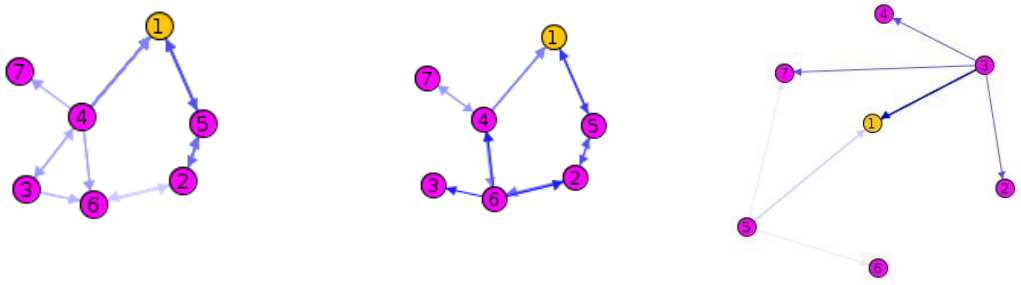


Figure 3.2 Different scenarios showing tree topology in Rpl network

`

3.3 RPL objective function & simulation using DGRM model in COOJA

3.3.1 Instant Contiki

Instant Contiki is an entire Contiki development environment in a single download. It is an Ubuntu Linux virtual machine that runs in VMWare player and has Contiki and all the development tools, compilers, and simulators used in Contiki development installed. Instant Contiki is so convenient that even hardcore Contiki developers use it.

3.3.2 The COOJA Simulator

COOJA is C language based simulator designed for simulating sensor networks running the Contiki sensor network operating system. The simulator is implemented in Java but allows sensor node software to be written in C. One of the differentiating features is that COOJA allows for simultaneous simulations at three different levels: Network Level, Operating System Level and Machine code instruction level. COOJA can also run Contiki programs either compiled natively on the host CPU or compiled for MSP430 emulator. In COOJA all the interactions with the simulated nodes are performed via plugins like Simulation Visualizer, Timeline, and Radio logger. It stores the simulation in an xml file with extension 'csc' (COOJA simulation configuration). This file contains information about the simulation environment, plugins, the nodes and its positions, random seed and radio medium etc. COOJA Simulator runs the Contiki applications whose files are placed in another directory and may also contain a “project-conf.h” file which provides the ability to change RPL parameters in one place.

3.3.3 Routing In RPL

In order to route the traffic upward, RPL only need the information in the DODAG. The DODAG tells who the preferred parent of the node is. So when a node wants to send a packet to the root , it simply sends the packet to its preferred parent in the tree, and the preferred

`

parent then sends the packet to his preferred parent and so on until the packet reaches the root. The rank is used to determine the relative position of a node in the DODAG and is used for loop avoidance as well. The rank is computed according to the OF. The rank is a 16bit monotonic scalar and is always higher than the rank of any of the parents. The RPL protocol populates DODAG with the parent information. The DODAG uses control packets called DODAG Information Object (DIO) and DODAG Information Solicitation (DIS) to convey the DODAG information. The formation of the DODAG is governed by the following rules.

1. The path metrics.
2. The Objective Function (OF)
3. The policies of the node.
4. Rules used for loop avoidance which is based on DODAG ranks.

`

3.3.4 Getting Started:-

3.3.4.1 Create new simulation

Click the File menu and click New Simulation.

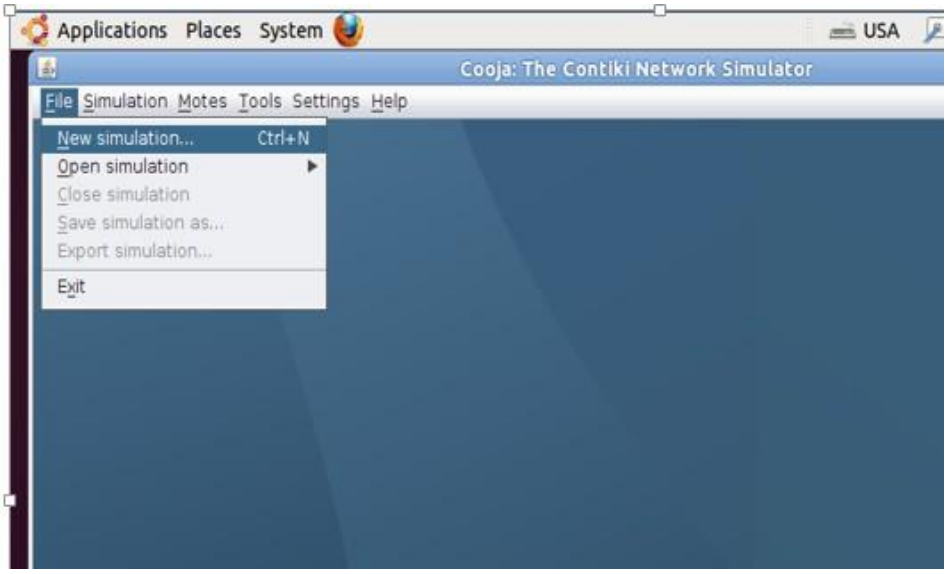


Fig. 3.3.4.1 New Simulation

`

3.3.4.2 Set simulation options

COOJA now opens up the Create new simulation dialog. In this dialog, we may choose to give our simulation a new name, but for this example, we'll just stick with My simulation. Click the Create button.

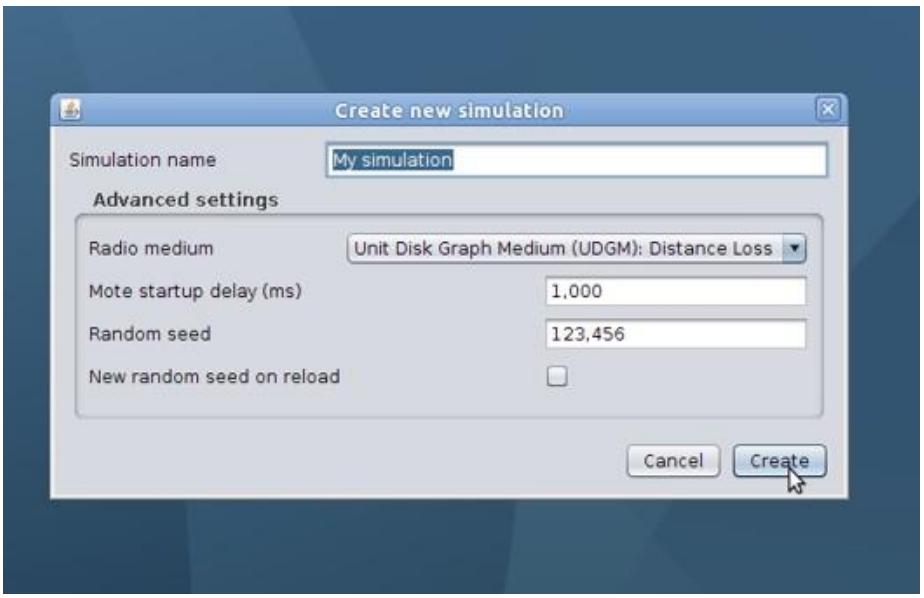


Fig. 3.3.4.2 Set Simulation Options

3.3.4.3 Simulation windows

COOJA brings up the new simulation. The Network window, at the top left of the screen, shows all the motes in the simulated network - it is empty now, since we have no motes in our simulation. The Timeline window, at the bottom of the screen, shows all communication events in the simulation over time - very handy for understanding what goes on in the network. . The Mote output window, on the right side of the screen, shows all serial port printouts from all the motes. The Notes window on the top right is where we can put notes for our simulation. And the Simulation Control window is where we start, pause, and reload our simulation.

`

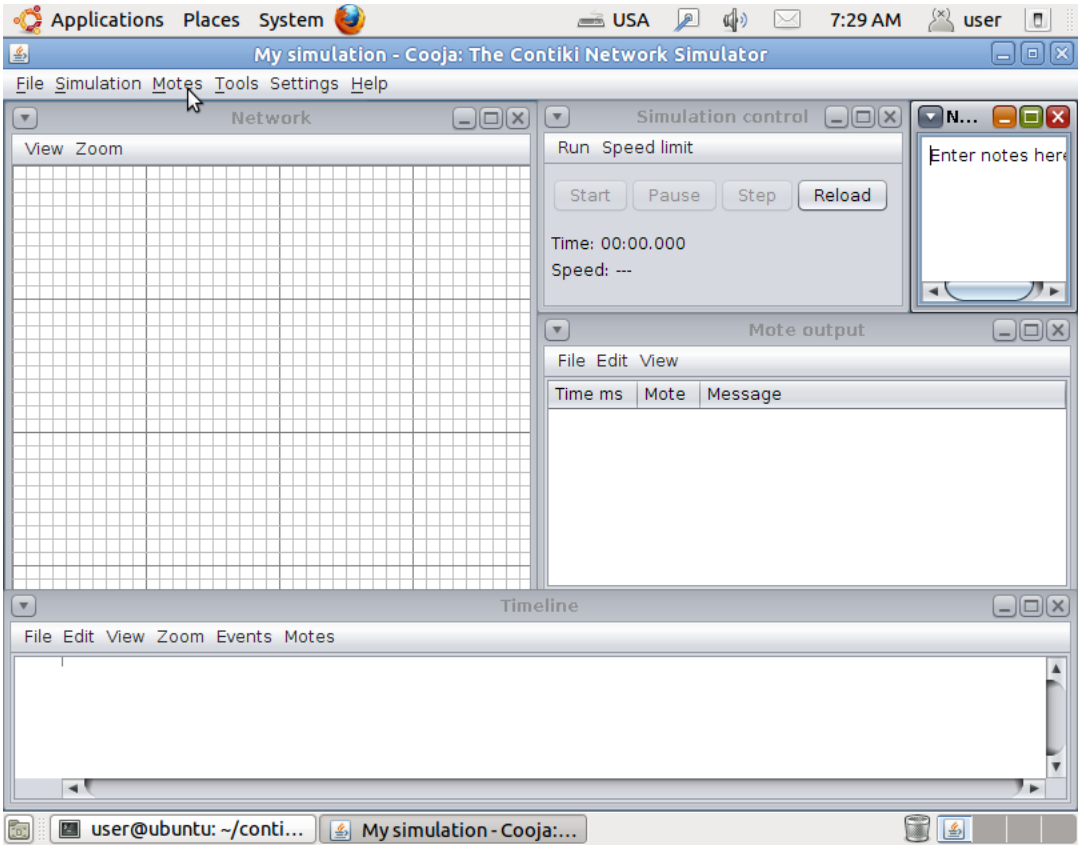


Fig.

3.3.4.3 Simulation Window

3.3.4.4 Add motes to the simulation

Add motes

Before we can simulate our network, we must add one or more motes. We do this via the **Motes** menu, where we click on Add Motes. Since this is the first mote we add, we must first create a mote type to add Click **Create new mote type** and select one of the available mote types. For this example, we click **Sky Mote** to create an emulated Tmote Sky mote type.

`

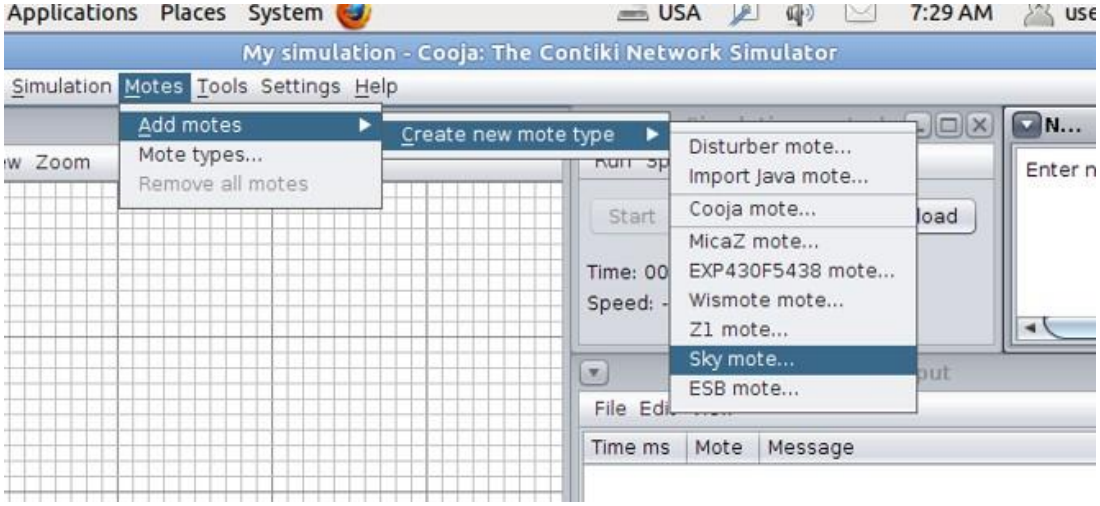


Fig. 3.3.4.4 Add Motes

3.3.4.5 Specify application C source file

Choose the file broadcast-example.c This file contains a simple Contiki application that randomly broadcasts a UDP packet to its neighbors. Click the Open button to choose the file.

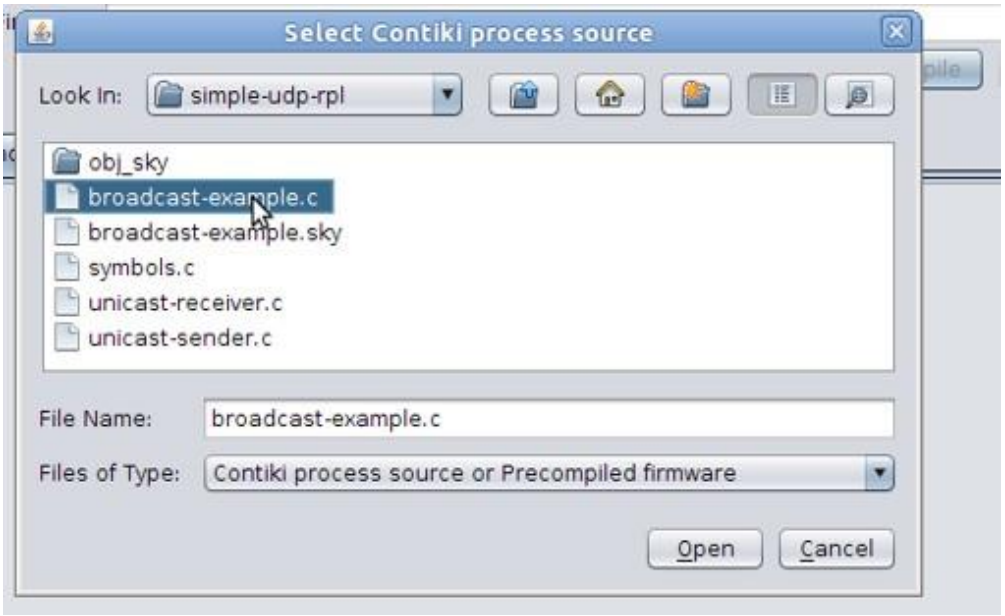


Fig. 3.3.4.5 Specify C File

`

3.3.4.6 Compile Contiki and the application

Now COOJA will verify that the selected Contiki application compiles for the platform that we have selected. Click the Compile button. This will take some time the first time around, expect it to take a minute at least. The compilation output will show up in the white panel at the bottom of the window.

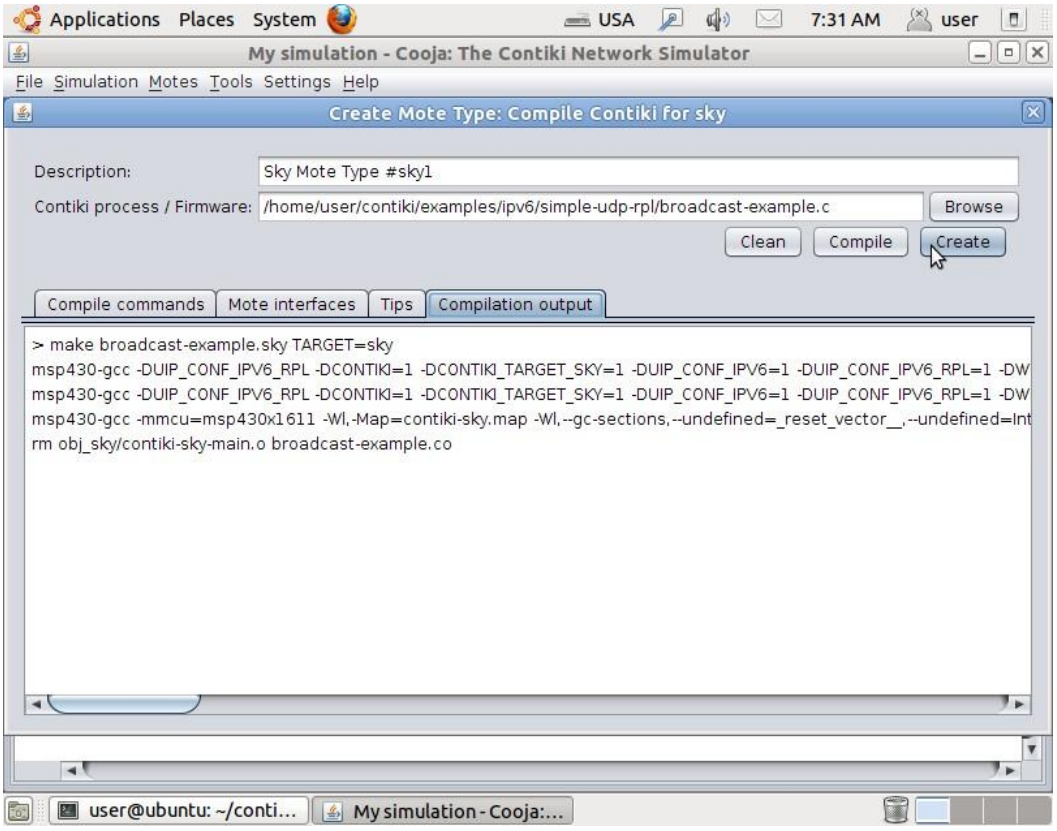


Fig. 3.3.4.6 Compile Contiki

3.3.4.7 Start the simulation

We can now see the 8 motes we added to the simulation in the Network window. Click the Start button to start the simulation.

`

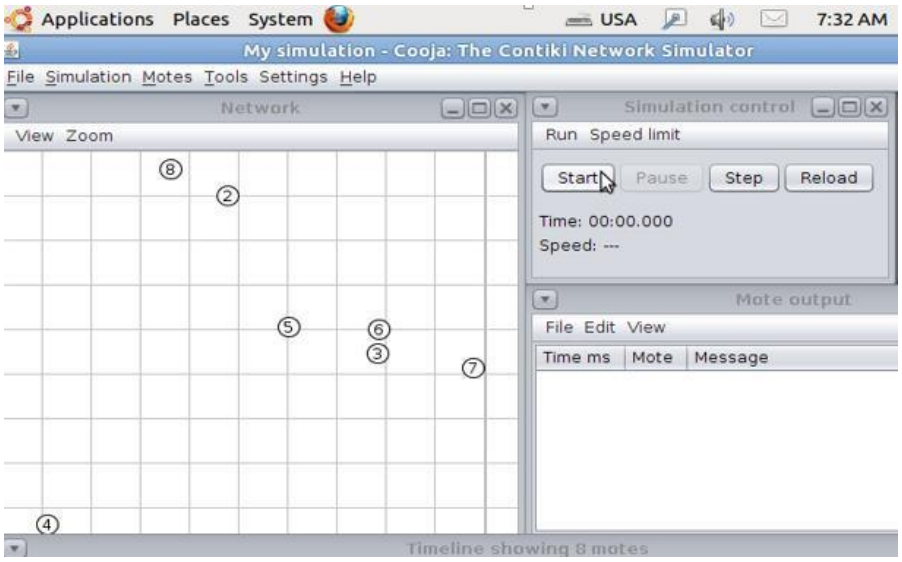


Fig. 3.3.4.7 Start Simulation

3.4 Implementation of black hole attack

3.4.1 Generation phase

We are using the cooja simulator to simulate the routing attack known as blackhole attack. Certain features of ContikiRPL have been exploited to simulate and monitor malicious behaviour in this work. ContikiRPL deals with every data packet differently. Each node processes and transmits data packets, which are generated by other node but routed through it differently 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 not forwarded completely by the malicious node. Malicious nodes continue to take part in the route formation by sending consistent DIO packets. This ensures nodes are live and continue to advertise themselves to the surrounding nodes. Malicious sensor nodes may or may not continue to send data packets generated by itself. Firstly we create a multihop network consisting of 4 nodes as being shown the figure 3.4.1. In this network we have taken one sink node that only collects the data, 2 normal sender nodes which send the random generated data and one malicious node that interferes with the routing of data through other

`

nodes and stops the data from forwarding through itself. As per the working of ContikiRPL routing protocol, various control messages are exchanged between sender nodes and sink nodes to form a topology. All signal messages are collected in the Log Listener plug-in of Cooja and further used for analysis.

1. Node 1 is the sink node.
2. Node 2 & 4 are sender nodes.
3. Node 3 is the malicious node

Figure 3.4.1 Nodes network

3.4.2 Detection Phase

In this phase we have developed a java program to detect the malicious behavior of the node through the matching of data send through it. Further explanation has been done in the next chapter.

`

4. PERFORMANCE ANALYSIS

In our work we have designed a code upon Black Hole attack based on rpl network in which a malicious node prevents transmission of message of neighbor node. Then we have proved via a java program that the messages are not passed through the malicious node. In the preliminary analysis we see that all nodes in a network are affected by the malicious activity. Since the simulation supports idealistic conditions; some nodes selected non malicious node as their next hop. Such sender nodes are initialized as non-affected nodes. Most of the data packets from non-affected sender nodes are expected to reach the sink node.

We have taken two scenarios that is in scenario 1 all the nodes are non-malicious and carry out a normal packet transfer while in scenario 2 one node of id-3 is placed as the malicious node in the network. On comparing the network graphs of the two scenarios i.e. Figure 4.1 and 4.2, it is seen that in the scenario 1 a multihop connected network is formed in which all the 7 sender nodes(id 2-8) transmit packets to the sink node (node id 1).

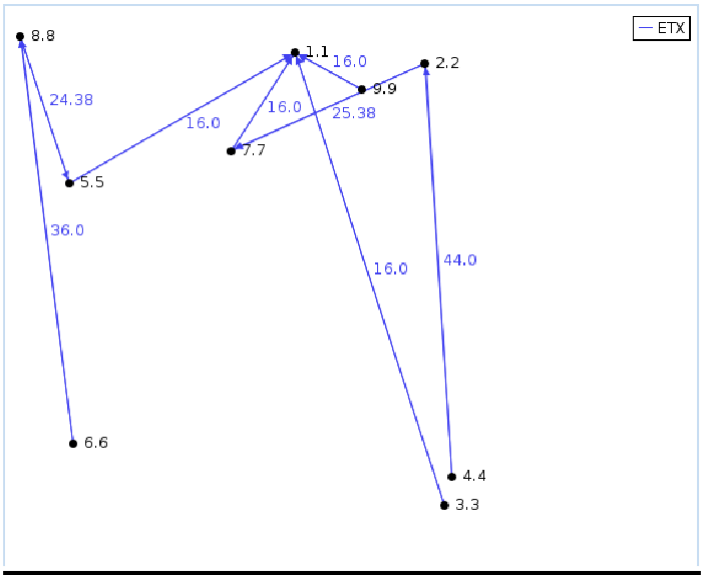


Fig. 4.1 Normal nodes network graph

In the other case, a multihop network is formed but it's not a connected graph as can be seen in fig 4.2. Here node 3 is the malicious one so its stops the data of node 2 from forwarding. Node 1 is taken as the sink node. Other nodes are sender nodes. So this gives a preliminary analysis of an insider attack that cannot be stopped using cryptographic measures. In order to provide a better security an IDS is required.

`

Further carrying out java based program analysis, figure 4.3shows the messages forwarded by the node 2 are not forwarded by the node 3 by means of matching the messages patterns generated in the cooja simulator which are saved through the log file plugin and hence the node 3 maybe malicious.

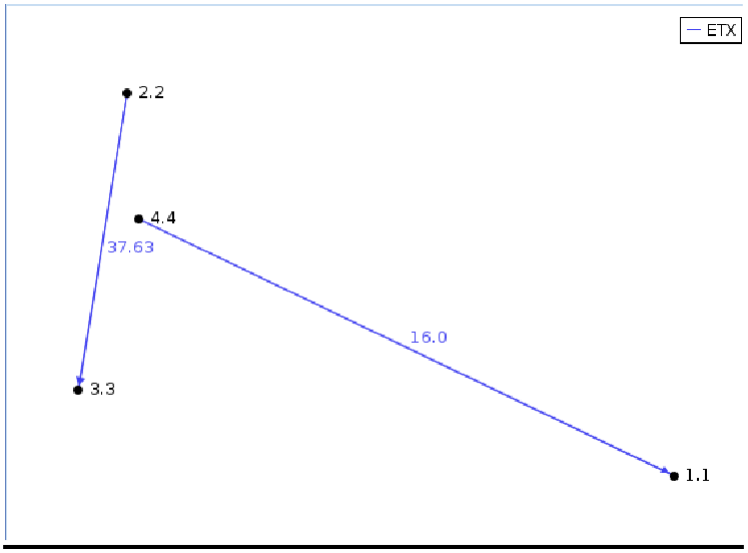


Fig 4.2 Malicious node network graph

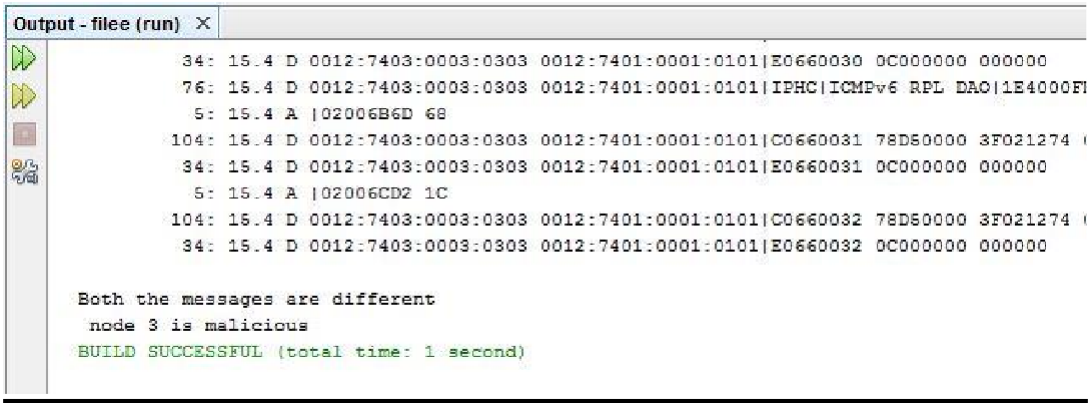


Figure 4.3 Output showing node 3 as malicious

`

5. CONCLUSIONS

5.1 Conclusions

Low power and Lossy networks are useful in the place where fixed communication infrastructure is not available. But it also has significant vulnerability to the security threats such as ‘Black Hole’ attack which maliciously reside in these networks to intercept data. With its nature broadcasting request and acknowledgement to the neighbor nodes, malicious nodes can be put into network, which always generate fake positive acknowledgement signal to the source to intercept packets, we call it ‘Black Hole Attack’. Our simulation showed how Black Hole Attack works on the Low power and lossy networks with further detection capability.

5.2 Future Scope

Study for understanding wireless network security in low power and lossy networks for attacks such as Warm hole, Gray hole and Black hole will be done in the near future, and also my research for preventing black hole attack will be done. Developing skills to use Cooja is also important for us to deal with these networks.

`

6. REFRENCES

[1] Vikrant Negi,"internet of things" seminar report ,2008,pp. 1-4.

[2] Cisco IBSG projections, economic & Social Affairs http://www.un.org/esa/population/publications/longrange2/WorldPop2300final.pdf. Pp. 2-4

[3] Anhtuan Le, Jonathan Loo, Aboubaker Lasebae, Mahdi Aiash and Yuan Luo," 6LoWPAN: a study on QoS security threats and countermeasures Using intrusion detection system approach", International Journal of Communication systems, 2012, pp. 1-20

[4] Hui Suo, Jiafu Wan, Caifeng Zou, Jianqi Liu, Security in the Internet of Things: A Review, in Computer Science and Electronics Engineering (ICCSEE), 2012, pp. 648-651

[5] Xue Yang, Zhihua Li, Zhenmin Geng, Haitao Zhang, A Multilayer Security Model for Internet of Things, in Communications in Computer and Information Science, 2012, Volume 312, pp 388-393

[6] Rafiullah Khan, Sarmad Ullah Khan, R. Zaheer, S. Khan, Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges, in 10th International Conference on Frontiers of Information Technology (FIT 2012), 2012, pp. 257-260

[7] Shi Yan-rong, Hou Tao, Internet of Things key technologies and architectures research in information processing in Proceedings of the 2nd International Conference on Computer Science and Electronics Engineering (ICCSEE), 2013

[8] Daniele Miorandi, Sabrina Sicari, Francesco De Pellegrini and Imrich Chlamtac, "Internet of Things: Vision, applications and research challenges," in Ad Hoc Networks, 2012, pp.1497-1516

[9] Luigi Atzori, Antonio Iera, Giacomo Morabito, "The Internet of Things: A Survey," in Computer Networks, pp. 2787-2805

`

[10] M.U. Farooq, Muhammad Waseem Anjum Khairi Sadia Mazhar, “A Critical Analysis on the Security Concerns of Internet of Things (IOT)”, International Journal of Computer Applications (0975 8887) Volume 111 - No. 7, February 2015,pp 2-10.

[11] Shelby Z, Bormann C. 6LoWPAN: The Wireless Embedded Internet. Wiley-Blackwell: West Sussex, United Kingdom, 2009.

[12] Roman R, Lopez J. Integrating wireless sensor networks and the Internet: a security analysis. Internet Research 2009

`

7. APPENDIX

7.1 Code Snippets:-

7.1.1 Sender1.c file

```
#include "contiki.h"
#include "net/uip.h"
#include "net/uip-ds6.h"
#include "net/uip-udp-packet.h"
#include "net/rpl/rpl.h"
#include "dev/serial-line.h"
#if CONTIKI_TARGET_Z1
#include "dev/uart0.h"
#else
#include "dev/uart1.h"
#endif
#include "collect-common.h"
#include "collect-view.h"

#include <stdio.h>
#include <string.h>

#define UDP_CLIENT_PORT 8775
#define UDP_SERVER_PORT 5688

#define DEBUG DEBUG_PRINT
#include "net/uip-debug.h"

static struct uip_udp_conn *client_conn;
static uip_ipaddr_t server_ipaddr;

/*---------------------------------------------------------------------------*/
PROCESS(udp_client_process, "UDP client process");
```

```
`
AUTOSTART_PROCESSES(&udp_client_process, &collect_common_process);
/*---------------------------------------------------------------------------*/
void
collect_common_set_sink(void)
{
  /* A udp client can never become sink */
}
/*---------------------------------------------------------------------------*/

void
collect_common_net_print(void)
{
}
/*---------------------------------------------------------------------------*/
static void
tcpip_handler(void)
{
  if(uip_newdata()) {
    /* Ignore incoming data */
  }
}
/*---------------------------------------------------------------------------*/
void
collect_common_send(void)
{
 }
/*---------------------------------------------------------------------------*/
void
collect_common_net_init(void)
{
#if CONTIKI_TARGET_Z1
  uart0_set_input(serial_line_input_byte);
```

```
`
#else
  uart1_set_input(serial_line_input_byte);
#endif
  serial_line_init();
}
/*---------------------------------------------------------------------------*/
static void
print_local_addresses(void)
{

}
/*---------------------------------------------------------------------------*/
static void
set_global_address(void)
{
  uip_ipaddr_t ipaddr;

  uip_ip6addr(&ipaddr, 0xaaaa, 0, 0, 0, 0, 0, 0, 0);
  uip_ds6_set_addr_iid(&ipaddr, &uip_lladdr);
  uip_ds6_addr_add(&ipaddr, 0, ADDR_AUTOCONF);

  /* set server address */
  uip_ip6addr(&server_ipaddr, 0xaaaa, 0, 0, 0, 0, 0, 0, 1);

}
/*---------------------------------------------------------------------------*/
PROCESS_THREAD(udp_client_process, ev, data)
{
  PROCESS_BEGIN();

  PROCESS_PAUSE();
```

```
`
  set_global_address();

  PRINTF("UDP client process started\n");

  print_local_addresses();

  /* new connection with remote host */
  client_conn = udp_new(NULL, UIP_HTONS(UDP_SERVER_PORT), NULL);
  udp_bind(client_conn, UIP_HTONS(UDP_CLIENT_PORT));

  PRINTF("Created a connection with the server ");
  PRINT6ADDR(&client_conn->ripaddr);
  PRINTF(" local/remote port %u/%u\n",
        UIP_HTONS(client_conn->lport), UIP_HTONS(client_conn->rport));

  while(1) {
    PROCESS_YIELD();
    if(ev == tcpip_event) {
      tcpip_handler();
    }
  }

  PROCESS_END();
}
/*---------------------------------------------------------------------------*/
```