Intrusion Detection in Wireless Sensor Networks

Apoorrv Goya[1], Sonali Sharma[2], Upendra Tiwari[3], Kaushal Kishor[4]
Department of Information Technology
ABES Institute Of Technology

Abstract: Wireless Sensor Networks (WSN) are used in various application areas including tracking applications, health related applications, and military applications. Intrusion Detection in Wireless Sensor Network can be helpful in detecting an intruder in a battlefield. Intrusion Detection is defined as a mechanism which is used for detecting the unusual attackers. The methodology of Intrusion Detection protects the Wireless Sensor Network from inside as well as from outside attackers. The most important traits for any network are Security and Confidentiality. The network should be fully secured and the intruder should be detected before it harms the network. Our Simulation results show the advantages and uses of Multiple Sensor Heterogeneous Wireless Sensor Network.

Keywords: WSN, Intrusion Detection, COOJA simulator, Intrusion Detection System, Transmission Range.

Introduction:

A Wireless Sensor Network (WSN) is considered as a group of spatially deployed wireless sensors to monitor several changes of environmental conditions such as forest fire, air pollutant concentration, and object moving in a cooperative manner without relying on any underlying infrastructure support. Wireless Sensor Networks have low deployment cost and handling of it is also easy. Wireless Sensor Networks are applied over various fields of technology. Many network parameters such as sensing range, transmission range, and node density have to be prudently considered at the network design stage. To achieve this, it is perilous to capture the impacts of network parameters on network performance with respect to application specifications. Intrusion detection in a Wireless Sensor Network can be defined as a monitoring system for detecting the intruder that is attacking the network domain. Intrusion Detection identifies the authorized and unauthorized users and then perform the computation.

The intrusion detection application is concerned that how fast the intruder can be detected by the Wireless Sensor Network. If sensors are positioned with a high density so that the combination of all sensing ranges covers the entire network area, the intruder can be immediately detected as soon as it approaches the network area. However, such a high-density deployment program upsurges the network speculation and may be even exorbitant for a large area. However, it is not important to deploy so many sensors to cover the entire Wireless Sensor Network area in almost every application, as a network that has small and scattered void areas will also be able to detect a moving intruder within a certain intrusion distance.

In a Wireless Sensor Network, there are two ways to detect an intruder. The first way is Single-sensing detection in which the intruder can be successfully detected by a single sensor and the other way is Multiple-sensing detection in which the intruder can only be detected by multiple collaborating sensors. Sometimes, the sensed information provided by a single sensor might be insufficient for recognizing the intruder because individual sensors can only sense a portion of the intruder. Multiple Sensing Detection is more beneficial, useful and productive as compare to Single Sensing Detection as they will sense and recognize all the portions of the intruder and identifies the authentication.

Wireless Sensor Network has two network types which is based on capability of the sensors. First network type is Homogeneous Wireless Sensor Networks and the other network type is Heterogeneous Wireless Sensor Networks. Sensing range and Transmission range are the two factors on which the sensor capability is defined. In a heterogeneous Wireless Sensor Networks some sensors have a larger sensing range and more power to attain a longer transmission range. In this paper, we show that the detection probability for a given intrusion detection distance is mainly increased by the Heterogeneous Wireless Sensor Networks. All the important tasks are started by the high capability sensors in the Heterogeneous Wireless Sensor Networks.

Wireless Sensor Networks (WSN), sometimes known as Wireless Sensor and Actuator Networks (WSAN), are distributed autonomous sensors that monitors physical or environmental conditions, such as temperature, sound, pressure and to cooperatively pass their data through the network to a main location. Military applications such as battlefield surveillance encouraged the development of Wireless Sensor Networks. Many industrial and consumer applications, like industrial process monitoring and control, machine health monitoring uses the Wireless Sensor Networks. The Wireless Sensor Networks are built of several hundreds or even thousands nodes, where each node is connected to one or more sensors. Various parts of the sensor network nodes are as follows- a radio transceiver with an internal antenna to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and a battery. Sensor nodes have limitations of cost and size that results in limitations on resources such as energy, memory, computational speed and communications bandwidth. The topology varies from a simple star network to an advanced multi hop wireless mesh network in the Wireless Sensor Networks.

Existing System:

A Single sensor can easily detect the intruder by using single-sensing detection method. In wireless sensor network, all the work has been done in homogeneous single sensor as the different sensors can only sense a part of the intruder.

Proposed System:

Intrusion detection in heterogeneous Wireless Sensor Networks by describing intrusion detection with respect to the parameters of network.

Two Intrusion Detection models are:

(i) Single-sensing detection model.

(ii) Multiple-sensing detection model.

We are detecting the intruder in both single sensor and multiple sensor heterogeneous wireless sensor network by performing coding in JAVA and network diagrams in COOJA Simulator.

Modules in Wireless Sensor Network:

Module-1: Building Sensor Network.

In this module, all the network gets connected with each other. Each node in the network is connected to the neighboring node. Every node is autonomously arranged in network area. It is also arranged that each port number is authorized in a node. No port number is left unauthorized in a node.

Module-2: Creation of Packet.

In this module, we browse the source file and selects it. Selected data is sorted in different groups and the sorted data gets converted into fixed size of packets and the packet is then send from source to detector.

Module-3: Finding the authorized and unauthorized port.

The intrusion detection is defined as a mechanism for a Wireless Sensor Network to detect the existence of inappropriate or anomalous moving intruders. In this module, find whether the path is authorized or unauthorized. If path is authorized, the packet is send to valid destination. Otherwise the packet will be destroyed. Port number is the only method with the help of which we are going to decide whether the path is authorized or Unauthorized.

Module-4: Building Inter-Domain Packet Filters.

In this module, if any packet is received from unauthorized port number or from some other port number, then the packet will be filtered and destroyed. This filter only removes the unauthorized packets. All the authorized packets will always be send to its proper destination. All the packets are checked but only the invalid packets are filtered and removed.

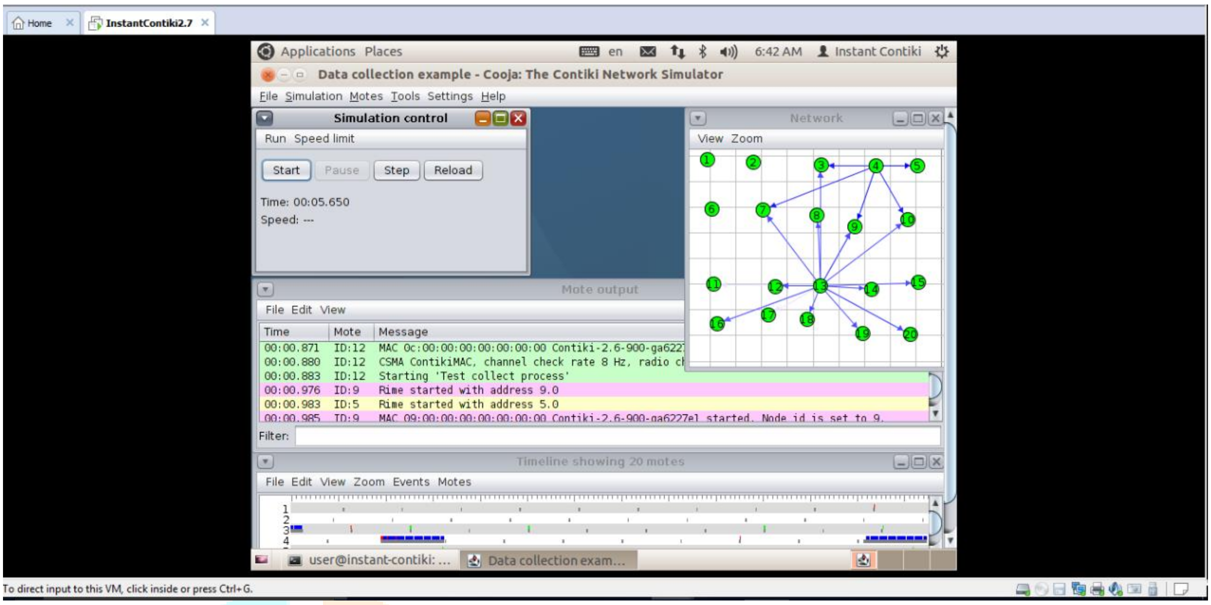
Module-5: Receiving the valid packet.

In this module, after filtering the invalid packets all the remaining valid packets will reach the destination.
All the invalid packets are filtered properly and no invalid packets should reach the destination.

Implementation:

For the implementation, we have used COOJA simulator so that we can show certain points with the help of this simulator that how actually nodes or motes make a group and work in a network by forming a group of nodes. It also shows the sensor map, network diagram, temperature of different nodes in the collect view, node information for all the nodes, transmission range for the different mote types, unicast receiver and sender. We have done the coding part in JAVA and all the data transmission work of project is shown with the help of JAVA coding. This COOJA simulator is usually a Operation System for Ubuntu so we are running it on the Virtual Machine (VM Ware). All the nodes travel in the form of the packets. The packets which are authorized means they have their port number, are only allowed to enter into the network. The packets which does not have their port number are unauthorized packets and hence they are discarded from entering into the network. The COOJA simulator work is shown as follows-

1. **Data Collection –**

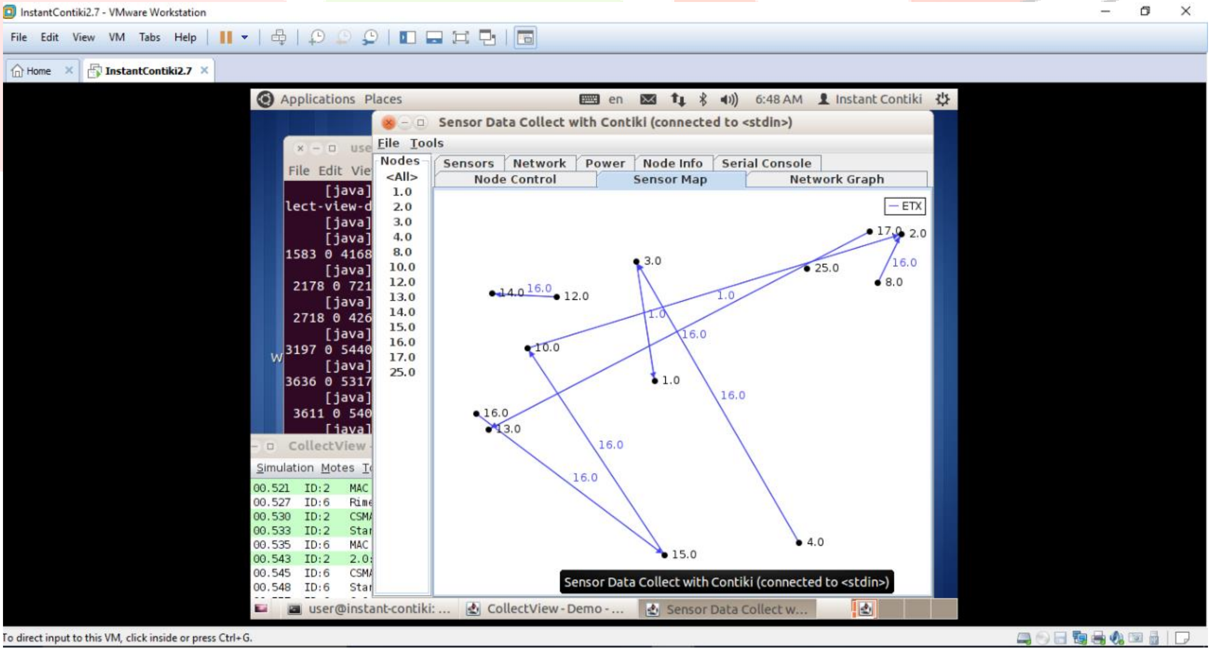


```
Time        Mote   Message
00:00.871   ID:12  MAC 0c:00:00:00:00:00:00:00 Contiki-2.6-900-ga622
00:00.880   ID:12  CSMA ContikiMAC, channel check rate 8 Hz, radio ch
00:00.883   ID:12  Starting 'Test collect process'
00:00.976   ID:9   Rime started with address 9.0
00:00.983   ID:5   Rime started with address 5.0
00:00.985   ID:9   MAC 09:00:00:00:00:00:00:00 Contiki-2.6-900-ga6227e1 started. Node id is set to 9.
```

Fig.1

Here we can show that how the various nodes and their data gets collected. This process is known as "Test Collect Process". There is a rime which gets started with different addresses. Every node is provided with its node id and MAC address. There are total 20 nodes in this diagram and a channel check rate of 8 Hz with radio channel 65491 is constant throughout the whole process.

2. **Sensor Map in Collect View –**


InstantContiki2.7 - VMware Workstation
File Edit View VM Tabs Help
Home
InstantContiki2.7
Applications Places
6:48 AM
Instant Contiki
Sensor Data Collect with Contiki (connected to <stdin>)
File Tools
Nodes
<All>
1.0
2.0
3.0
4.0
8.0
10.0
12.0
13.0
14.0
15.0
16.0
17.0
25.0
Sensors Network Power Node Info Serial Console
Node Control Sensor Map Network Graph
ETX
17.0
2.0
3.0
25.0
16.0
8.0
14.0
16.0
12.0
1.0
1.0
16.0
10.0
1.0
16.0
16.0
13.0
16.0
16.0
15.0
4.0
CollectView
Simulation Motes
user@instant-contiki: ...
CollectView - Demo - ...
Sensor Data Collect w...
To direct input to this VM, click inside or press Ctrl+G.

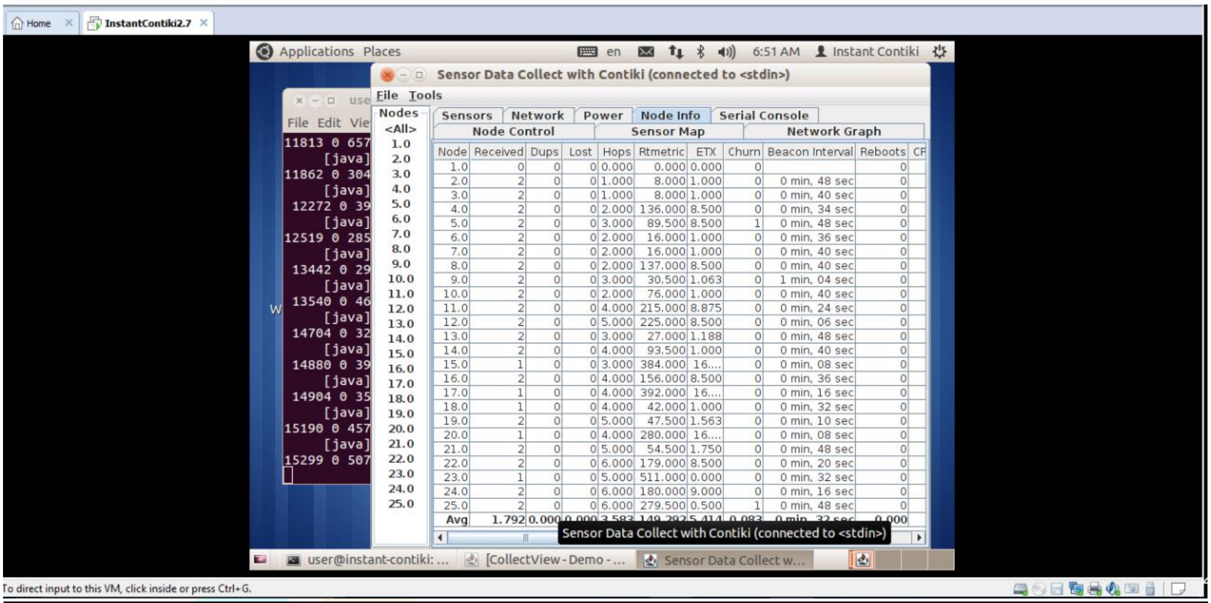
```
       [java]
lect-view-d
       [java]
       [java]
1583 0 4168
       [java]
 2178 0 721
       [java]
 2718 0 426
       [java]
3197 0 5440
       [java]
3636 0 5317
       [java]
 3611 0 540
       [java]
```

```
00.521  ID:2  MAC
00.527  ID:6  Rime
00.530  ID:2  CSMA
00.533  ID:2  Star
00.535  ID:6  MAC
00.543  ID:2  2.0:
00.545  ID:6  CSMA
00.548  ID:6  Star
```

Fig.2

In this process, there are 25 nodes. There is no order for the nodes. A node can be connected to other node in any order. As we can see node 16 and 1 has occur in almost every path. It is a map which senses all the nodes and analyses all the path between various nodes.

3. <u>Node Information in Collect View –</u>



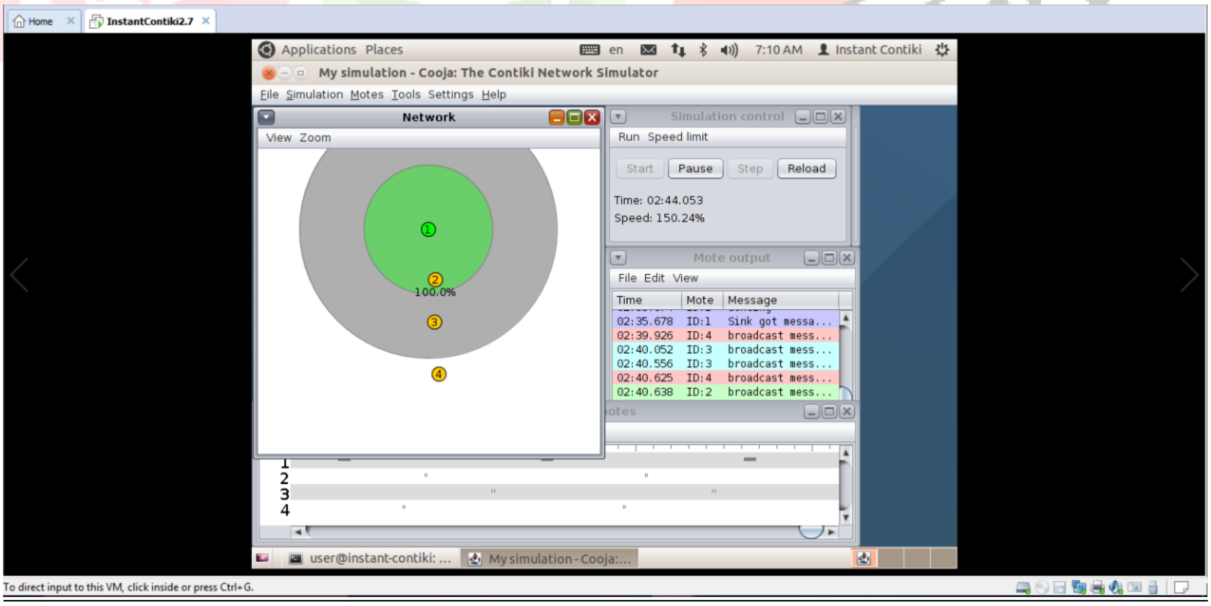
```
11813 0 657
      [java]
11862 0 304
      [java]
 12272 0 39
      [java]
12519 0 285
      [java]
 13442 0 29
      [java]
 13540 0 46
      [java]
 14704 0 32
      [java]
 14880 0 39
      [java]
 14904 0 35
      [java]
15190 0 457
      [java]
15299 0 507
```

Node	Received	Dups	Lost	Hops	Rtmetric	ETX	Churn	Beacon Interval	Reboots	CF
1.0	0	0	0	0.000	0.000	0.000	0		0	
2.0	2	0	0	1.000	8.000	1.000	0	0 min, 48 sec	0	
3.0	2	0	0	1.000	8.000	1.000	0	0 min, 40 sec	0	
4.0	2	0	0	2.000	136.000	8.500	0	0 min, 34 sec	0	
5.0	2	0	0	3.000	89.500	8.500	1	0 min, 48 sec	0	
6.0	2	0	0	2.000	16.000	1.000	0	0 min, 36 sec	0	
7.0	2	0	0	2.000	16.000	1.000	0	0 min, 40 sec	0	
8.0	2	0	0	2.000	137.000	8.500	0	0 min, 40 sec	0	
9.0	2	0	0	3.000	30.500	1.063	0	1 min, 04 sec	0	
10.0	2	0	0	2.000	76.000	1.000	0	0 min, 40 sec	0	
11.0	2	0	0	4.000	215.000	8.875	0	0 min, 24 sec	0	
12.0	2	0	0	5.000	225.000	8.500	0	0 min, 06 sec	0	
13.0	2	0	0	3.000	27.000	1.188	0	0 min, 48 sec	0	
14.0	2	0	0	4.000	93.500	1.000	0	0 min, 40 sec	0	
15.0	1	0	0	3.000	384.000	16....	0	0 min, 08 sec	0	
16.0	2	0	0	4.000	156.000	8.500	0	0 min, 36 sec	0	
17.0	1	0	0	4.000	392.000	16....	0	0 min, 16 sec	0	
18.0	1	0	0	4.000	42.000	1.000	0	0 min, 32 sec	0	
19.0	2	0	0	5.000	47.500	1.563	0	0 min, 10 sec	0	
20.0	1	0	0	4.000	280.000	16....	0	0 min, 08 sec	0	
21.0	2	0	0	5.000	54.500	1.750	0	0 min, 48 sec	0	
22.0	2	0	0	6.000	179.000	8.500	0	0 min, 20 sec	0	
23.0	1	0	0	5.000	511.000	0.000	0	0 min, 32 sec	0	
24.0	2	0	0	6.000	180.000	9.000	0	0 min, 16 sec	0	
25.0	2	0	0	6.000	279.500	0.500	1	0 min, 48 sec	0	
Avg	1.792	0.000	0.000	3.583	149.292	5.414	0.083	0 min, 32 sec	0.000	

Fig.3

In this process, we are provided with the information from node 1 to node 25. The information consists of- Received, Dups, Lost, Number of hops, Rtmetric, ETX, Chum, Beacon Interval and Reboots. In the last row, the average of each column has been calculated so that we can have an idea that how much average time for a particular type has been taken in the process. This process comes under the collect view.

4. <u>Transmission Range with 2 Different Mote Types –</u>


Home
InstantContiki2.7
Applications Places
en
7:10 AM
Instant Contiki
My simulation - Cooja: The Contiki Network Simulator
File Simulation Motes Tools Settings Help
Network
View Zoom
1
2
100.0%
3
4
Simulation control
Run Speed limit
Start
Pause
Step
Reload
Mote output
File Edit View
otes
1
2
3
4
user@instant-contiki: ...
My simulation - Cooja:...
To direct input to this VM, click inside or press Ctrl+G.

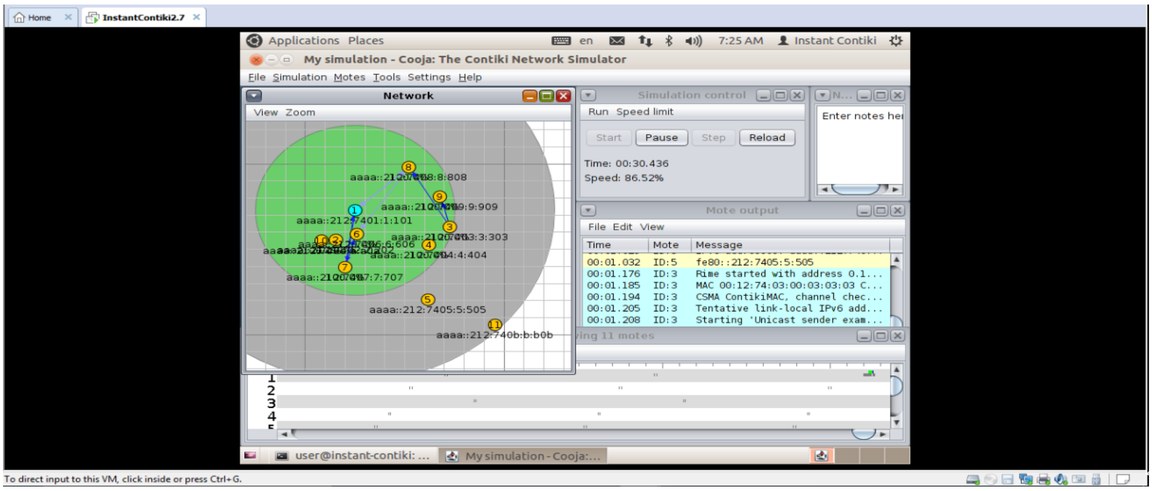
Time: 02:44.053
Speed: 150.24%

```
Time       Mote  Message
02:35.678  ID:1  Sink got messa...
02:39.926  ID:4  broadcast mess...
02:40.052  ID:3  broadcast mess...
02:40.556  ID:3  broadcast mess...
02:40.625  ID:4  broadcast mess...
02:40.638  ID:2  broadcast mess...
```

Fig.4

In this process, we took 2 different mote types so that we can differentiate among them and their transmission range can be specified. It is performed so we can check that if we are taking 4 modules or nodes then whether all the nodes lie in each other's range or not. Sometimes some nodes are out of the range of transmission. We need to adjust the transmission range for all the nodes so that every node during transmission should be in the range of each other. Node 1 which is marked in green color is of Sky mote type and the rest three nodes which are marked in yellow color are of MicaZ mote type.

5. **<u>Unicast Receiver and Sender –</u>**



Time: 00:30.436
Speed: 86.52%

```
Time        Mote   Message
00:01.032   ID:5   fe80::212:7405:5:505
00:01.176   ID:3   Rime started with address 0.1...
00:01.185   ID:3   MAC 00:12:74:03:00:03:03:03 C...
00:01.194   ID:3   CSMA ContikiMAC, channel chec...
00:01.205   ID:3   Tentative link-local IPv6 add...
00:01.208   ID:3   Starting 'Unicast sender exam...
```

Fig.5

In this process, we considered Sky motes but they are differentiated in terms of unicast receiver and unicast sender. As we can see in above figure, node ‘1’ is marked in blue color as it is the only receiver in this process and the rest nodes which are marked in yellow color are senders. IP address for all the senders are different and the receiver one by one receives all the nodes sent by the sender. The positions for all the nodes has also assigned and it is separated in 20m grid background.

We have performed all these points in the COOJA simulator and hence we obtain these results.

Problem Formulation:

Intrusion Detection in Wireless Sensor Network has certain limitations-

1.<u>Limited Storage Space and Memory</u> - A tiny sensor device has a small amount of memory and storage space for the code. To construct effective security techniques, it is necessary to limit the size of the security algorithm code.

2.<u>Power Limitation</u> - Once sensor nodes are installed in a sensor network, the energy must be conserved for extending the life of the individual sensor node and the entire sensor network.

3.<u>Security</u> - Maintaining security is very challenging in Wireless Sensor Network as it is not only being used in battlefield applications but also for scrutiny and building monitoring applications.

4.<u>Quality Of Service</u> - The Quality of Service in Wireless Sensor Network is difficult because the topology varies from a simple star network to an advanced multi hop wireless mesh network.

Objectives:

An **Intrusion detection system** (**IDS**) is a device that takes care of all the malicious activities and unauthorized access in a network.

1. **<u>Scalability</u> -** The network must preserve its stability. The number of communication messages exchanged will be more if we introduce more nodes into the network. So these nodes are combined into the existing network.

2. **<u>Fault Tolerance and Adaptability</u>** - Fault tolerance is the process that maintains sensor network functionalities without any disturbance due to failure of sensor node. The overall task of the sensor network is not affected by the failure of single node as in the sensor network every node has limited power of energy.

3. **<u>Power Consumption</u> -** Wireless sensor node is microelectronic device. All the nodes are equipped with a restricted number of power sources. Nodes are reliant on battery for their power.

4. **<u>Medium Access Control Communication</u>** – It is a major source of energy consumption in Wireless Sensor Network. Medium Access Control protocol directly control radio of nodes in network and it should avoid collisions from inquisitive node.

Applications:

Wireless Sensor Network has many applications. It collects the information which are related to human activities like health care, military scrutiny, highway traffic. It is also used for monitoring physical and environmental spectacles, such as ocean and wildlife, earthquakes, pollution, wild fire and water quality. Another application of Wireless Sensor Network is that it is used for monitoring industrial sites, such as building safety and manufacturing machinery performance. Security is considered as a vital issue for Wireless Sensor Network especially if the networks have confidential information.

Conclusion:

The main concern while designing a Wireless Sensor Network is always security. The medium has the broadcast nature therefore they are more disposed to security attacks. In this paper, we have proposed the implementation with the help of COOJA simulator and JAVA coding. It helps to improve the efficiency and it gives the information about every node present in the packet. It also shows network graph, sensor map, collect view and unicast receiver and sender for the nodes. The transmission between different mote types has also been done so that we can easily observe their ranges. As a result, it also improves the detection rate so that almost all the Intrusions can be detected easily. The discussed system is applicable to medium and large sized networks. It gives a inclusive range of flexibility in detection of Intrusions compared to the other existing systems as with COOJA simulator we have observed all the factors for each and every node. The energy efficiency and the system life time can be significantly improved.

References:

1. Idrees S. Kocher, Chee-Onn Chow, Hiroshi Ishii, and Tanveer A. Zia, “Threat Models and Security Issues in Wireless Sensor Networks”, International Journal of Computer Theory and Engineering, Vol. 5, No. 5, October 2013.

2. Mohd. Abdul Sattar, Mohd. Anas Ali, “Comparison of Various Intrusion Detection Systems in Wireless Sensor Network”, (IJARCCE) International Journal of Advanced Research in Computer and Communication Enginnering ISO 3297:2007 Certified Vol. 5, Issue 11, November 16.

3. Joseph Rish Simenthy, K. Vijayan, “Advanced Intrusion Detection System for Wireless Sensor Network” (IJAREEIE) International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 3, Special Issue 3, April 2014 p. 167-172.

4. G. Padmavathi and D. Shanmugapriya, “A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks”, International J. Computer Science, vol. 4, num. 1, pp. 1–9, 2009.

5. S. Ren, Q. Li, H. Wang, X. Chen, and X. Zhang, “Design and Analysis of Sensing Scheduling Algorithms under Partial Coverage for Object Detection in Sensor Networks,” IEEE Trans. Parallel and Distributed Systems, vol. 18, no. 3, pp. 334-350, Mar. 2007.

6. K.Q.Yan, S. C Wang, S. S Wang and C. W. Liu, “Hybrid Intrusion Detection System for Enhancing the Security of A Cluster-Based Wireless Sensor Networks”, Computer Science and Information Technology (ICCSIT), 3rd IEEE International Conference, 9-11 July 2010.

7. Pankaj Kumar Srivastava, Priyanka Rai, Upama Singh, “Intrusion Detection: An Energy Efficient Approach in Heterogeneous WSN”, International Journal of Scientific and Research Publications, Volume 2, Issue 11, November 2012 1 ISSN 2250-3153.

8. Nabil Ali Alrajeh, S. Khan, and Bilal Shams,” Intrusion Detection Systems in Wireless Sensor Networks: A Review” Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2013, Article ID 167575, 7 pages