A PROPOSAL TO IDENTIFY TRUSTWORTHY DATA IN SMART CITY APPLICATION

Neha Chauhan [1, a)]

[1] *Research Scholar, RK University, Rajkot, Gujarat, India*

[a)] *neha.chauhan@rku.ac.in*

Abstract: Era of Internet of things from past to give bargain numerous problems like security, authentication, privacy, confidentiality, additionally extraordinary assaults like tampering, jamming, sinkhole etc. Numerous issue is some way resolved using different IDS system (DEMO, SEVLTE) and other protocols like FIWARE, SMARTIE, and different scheme like RealAlert, Time based key generation etc. In this period a number of smart devices will increase rapidly and the use of smart devices also be increased to access the services from different things to made a city Smart, so it can be easy to manage by Internet of things (IoT).The Internet of things is transparently provide access to the different system, so that all the data is collected from different things. The main goal of these research is to provide trustworthy and correct data to sensor node. To identify trustworthy data for that we use the RSSI value, 6LoWPAN based on IEEE 802.15.4 and also check on – off attack so, utilizing our approach we use the Contiki OS and Cooja simulator to implement the trust evolution framework for smart city application.

Keyword: Trustworthy, IoT, Smart City, WSN, Security, RSSI

INTRODUCTION

Internet of Things (IoT) is a computing concept which provides interconnection between the uniquely identifiable devices. By integrating several technologies like actuators and sensor networks, identification and tracking technology, enhanced communication protocol and distributed intelligence of smart objects, IoT enables communication between the real time objects present around us. The effectiveness of IoT can be seen in both domestic (e.g. Assisted living, e-health, enhanced learning) and business (automation, intelligent transportation) fields.

While various issues are related to the implementation of IoT, Security of IoT have significant impact on the performance of IoT applications. Trust is an important aspect while talking about secure systems. A system can behave in untrustworthy manner even after having security and privacy implementation. Behavior based analysis of devices is required that can predict the device performance over the time. Trust management provides behavior based analysis of entities, using their past behavior, reputation in the network or recommendation. A trustworthy system is needed to prevent from unwanted activities conducted by malicious devices. My research work is to design a dynamic trust management system for IoT devices.

The IoT is an emerging area of interest for current developing networks. It has varied field of applications like industry, healthcare, transportation, smart city, etc. The IoT Connect both inanimate (nonliving) and living things by using sensors for data collection. A primary aim of the Internet of Things (IoT) is to deliver personalized or even autonomic services to individuals, building on a pervasive digital ecosystem that collects information from and offers control over devices that are embedded in our everyday lives. In future the number of smart objects are increase rapidly so all data must be passed in secure way via base station to smart things. As numerous problem arise like tempering, sinkhole, privacy issue, bad mouth attack, on-off behavior etc. when transfer the data in Internet of Things (IoT). So all these issues effects to the data and appropriate information cannot get through numerous objects and also generate the delay. To avoid these issues to must check the trustworthiness of data. Trust issue generate from malicious node, fault tolerant when sensing task done in wireless sensor networks.

State of Art

Internet of Things (IoT) is known as one of the key enabling technology for smart city application. In these paper author proposed policy based secure and trustworthy sensing for smart city application and these system is known as RealAlert. In these system to check the trustworthiness of data and IoT devices based on the report generated from collect the context of data based on policy rules. In RealAlert system evaluate the trustworthiness of IoT nodes and detect the malicious nodes [1].

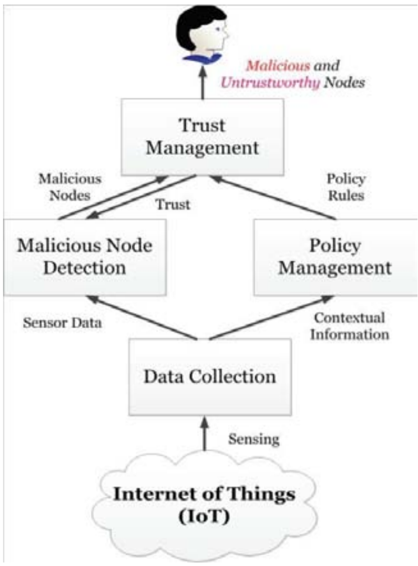


Fig 1 RealAlert Scheme [1]

Related Work

Policy-based Secure and Trustworthy Sensing for Internet of Things in Smart Cities [1]

This paper illustrate the trustworthiness of data as well as the sensor node and that system name as the RealAlert. In this paper, a policy-based secure and trustworthy sensing scheme is proposed for IoT called RealAlert. In the scheme, we identify the untrustworthy IoT nodes by evaluating its data reporting history. Moreover, policies are used to identify malicious nodes that have been compromised by attackers using contextual information. RealAlert is a holistic scheme, which is comprised of four components, i.e., data collection, policy management, malicious node detection, and trust management, aiming at properly evaluating the trustworthiness of the IoT nodes and detecting malicious ones in different contexts using policies.

State space model-based trust evaluation over wireless sensor networks: an iterative particle filter approach [2]

This paper authors proposed the state space modeling approach for evaluate a trust in wireless sensor networks. In these model each sensor node associate with a trust matric, which measure what kind of data transmitted from one node to another node and trusted by a server node. The performance of WSN depends on collaboration among distributed sensor nodes, while those nodes are often unattended with severe energy constraints and limited reliability. In such conditions, it is important to evaluate the trustworthiness of participating nodes since trust is the major driving force for collaboration and the trust value can be used as a decision making criteria for the end-user to take appropriate measures such as replacing detected faulty nodes.

Trustworthy service composition with secure data transmission in sensor networks [3]

This paper authors describe the service composition in sensor networks with secure way to transfer the data and over wireless sensor networks. Service composition provides us a promising way to cooperate various sensors to build more powerful IoT applications over sensor networks. However, the limited capability of sensor node poses great challenges not only to trustworthy service composition but also to secure data aggregation. In service-oriented sensor networks, the functionality provided by each sensor node is treated as a service and Services can be composed together dynamically and rapidly to develop novel and powerful applications. For a variety of candidate services, consumers can select qualified ones with respect to their specific functional and security requirements. In many cases the services might be malicious. They may not deliver its task with promised quality, or cause confidential data leakage to the public. Therefore, trust and security are the main concerns of service composition in sensor networks.

The Smart Citizen Factor in Trustworthy Smart City Crowdsensing [4]

The authors proposed the reputed based crowd sensing for smart city application. Smart city areas expect to enhance nature of life by merging ICT framework into physical and social foundation in urban conditions. The smart city foundation comprises of an application layer in which services are conveyed to citizen; a network layer in which users, information sources, and service provider's communication and in perception layer in which data acquisition and recruitment of sensing devices take place.

A survey of trust computation models for service management in internet of things systems [5]

In these paper authors survey on trust computation model for Internet of things for the purpose of service management. The open issue to solve is to devise an effective and efficient trust computation method for an IoT device acting as a service requester to dynamically assess the service trustworthiness of an- other IoT device acting as a service provider, taking into consideration of the service history. Trust computation done using quality of services (QoS) and social trust. In QoS trust refers to the belief that IoT devices is able to provide the quality service in response to a service request. To measure the QoS by packet delivery ratio. Social trust define from social relationship between owners of IoT devices and is measured by privacy, connectivity, intimacy. Propagation of trust done through to provide the evidence and trust propagation scheme that is 1. Distributed 2.

Centralized. In distributed manner the observation of IoT devices without any centralized entity and it is difficult to access the centralized entity. For making the distributed trust propagation each node in network maintain a data forwarding information table for hearing the activity of neighboring node but the disadvantage is if RSS field provide the wrong information to that data forwarding information table then wrong services provided by malicious nodes. In centralized trust propagation that require the centralized entity either a physical or virtual. Centralized trust propagation require more cost if the centralized entity is physical and may be require large amount of processing time. It is necessary to collect the evidence through the self-observation or feedback for the trust aggregation is required.

Trust Management Mechanism for Internet of Things [6]

Trust management has been used for providing the security service for the smart device. In these paper the authors illustrates the trust management architecture. In trust management architecture contain three layers: sensor layer, core layer and application layer. However, due to complex and heterogeneous architecture of IoT so the trust management issue cannot solved by cryptography. When provide the trust to data that time it is necessary consider how data passed through from sensor layer to core layer to application layer. In which one problem arise when to

assign the fuzzy logic by sensor node from sensor layer. In these trust procedure the trust management include when the service provide to service requester.

A Survey on Security and Privacy Issues in Internet-of-Things [7]

In these paper authors illustrates the architecture of authentication and access control mechanism for IoT, another segment describes the limitation of IoT devices and security issues in different layers. Limitation of IoT devices is the effect of environmental that time sensor networks or any sensing task is done so due thunderstorm or tsunami effect to provide the services to different things and also may contain the battery life problem due environmental effects.The final phase is the authentication request which is sent from the IoT device to the gateway. For the authentication scheme an approach is Datagram Transport Layer Security (DTLS) based on certificates with mutual authentication. The communication is done by introducing a new device called IoT Security Provider (IoTSSP), which is responsible for managing and analyzing the devices' certificates along with authentication and session establishment between the devices.

Security Access Protocols in IoT Capillary Networks [8]

Smart city services must be easily access by the IoT devices and that will used the huge amount of sensors, topologies of networks secure way to manage them. The capillary networks provide the short range extension network for show the IoT traffic. The author proposed the two types of IoT devices like IPbidirectional and IP-unidirectional devices. Capillary networks are seen as the fundamental enabling infrastructure(s) required for IoT, and more in general, for Internet of Everything, and then for the realistic development of the smart environment (SE) concept. It allows to collect traffic from any sensor device. In IoT scenarios, a number of technologies have been developed in order to achieve information privacy and security goals, such as the transport layer security, which could also improve confidentiality and integrity of the IoT, and the onion routing, which encrypts and mixes Internet traffic from different sources, and encrypts data into multiple layers, by using public keys on the transmission path. 6LoWPAN enables embedded nodes to use a restricted subset of IPv6 addresses, 6LoWPAN is a combination of IPv6 and IEEE 802.15.4.

Security in Internet of Things: issues, challenges, taxonomy, and architecture [9]

In these paper the authors illustrates DDOS, security challenges for different layers, RPL and various security issues in RPL and 6LoWPAN. The Routing Protocol for Low power and Lossy Networks (RPL) proposed for low power devices which will be an integral part of the IoT scenario lacks a proper security model. There are no special security measures proposed with RPL.

Modelling trust dynamics in the Internet of Things [10]

In these paper authors illustrate the trust management framework for IoT environments. In these framework there are mainly three main layer is: Services, Scenario, and Requirements. The scenario is the lower level of trust management framework and it’s include the context and Use cases. Context include the dynamicity of a trust model could be captured if we are able to determine the factors that influence trust in a given moment in time for a specific purpose. We advocate that trust models that are going to be defined for a given “thing” do not depend only on its behavior but also on what we call the Context or things around it.

PROPOSED FRAMEWORK FOR IDENTIFY TRUSTWORTHY DATA FOR SMART CITY APPLICATION

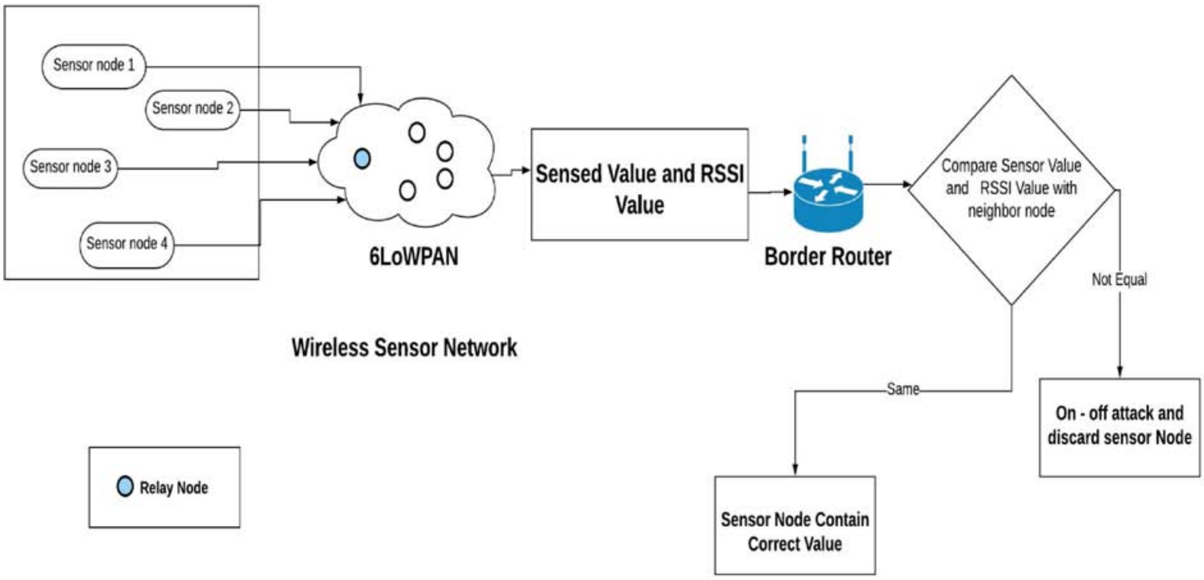

Sensor node 1
Sensor node 2
Sensor node 3
Sensor node 4
6LoWPAN
Sensed Value and RSSI Value
Border Router
Compare Sensor Value and RSSI Value with neighbor node
Not Equal
Same
On - off attack and discard sensor Node
Sensor Node Contain Correct Value
Wireless Sensor Network
Relay Node

Fig 2. Proposed architecture for Identify trustworthy data for Smart city application

All the component of proposed architecture described below:

- Sensor node: Sensor node contain sensed value. In these sensor used the sensor data of temperature sensor, humidity sensor and light sensor.
- 6LoWPAN: It is an IPV6 based local personal area network with limited processing power and IEEE 802.15.4 based networks.

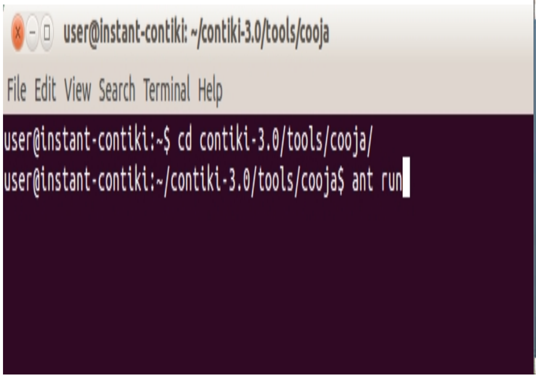
- Relay Node: When number of sensor node connect and that all node must in synchronous way to pass the sensed data that task done using Relay node.

In Proposed architecture to identify trustworthiness of sensor data for that 6LoWPAN, relay node and RSSI value used in above given smart city scenario framework. Relay node main task is to all the number of sensor node is connected them, so all the sensor node in synchronous way done the sensing task. Perhaps any of sensor node or malicious nodes come to wireless sensor network that time during sensing task must compare its sensor data and also checked it is connected with relay node or not. If it's new added sensor node is connected to relay node then its RSSI value and sensor data compare with its neighbor sensor node. If its value of newly added sensor node and its neighbor node sensed value, RSSI value same then in wireless sensor network no any malicious nodes available. When sensor node does not connect to relay node because its sensor data same with any sensor network sensor node but its location and its RSSI value is different, so wireless sensor network contain on – off attack. It is necessary to discard that particular node from sensor network. In these proposed scenario we used temperature sensor, Humidity sensor and light sensor. In on – off attack sometimes malicious node act good or bad. Using border router to route the information and sent to base station. Using 6LoWPAN the sensor node ipv6 address capture and store it to the route table. Because sensor has a low memory capacity and low processing power for that we used the 6LoWPAn based on IEEE 802.15.4 networks. We simulate our approach using Contiki OS and Cooja simulator.

IMPLEMENTATION AND ANALYSIS

Contiki is a wireless sensor network operating system and consists of the kernel, libraries, the program loader, and a set of processes. It is used in networked embedded systems and smart objects.

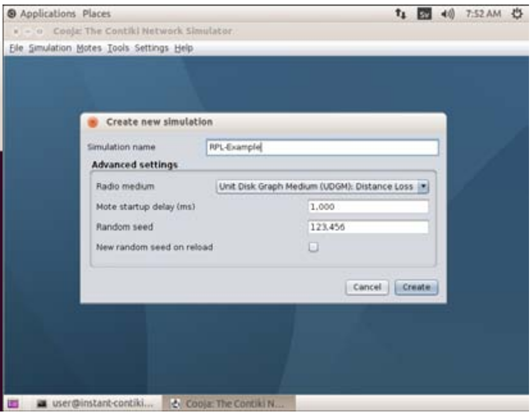
Starting Cooja
We can start the Cooja simulator using the following commands:
1. cd Contiki-3.0/tools/cooja
2. ant run



user@instant-contiki: ~/contiki-3.0/tools/cooja
File Edit View Search Terminal Help

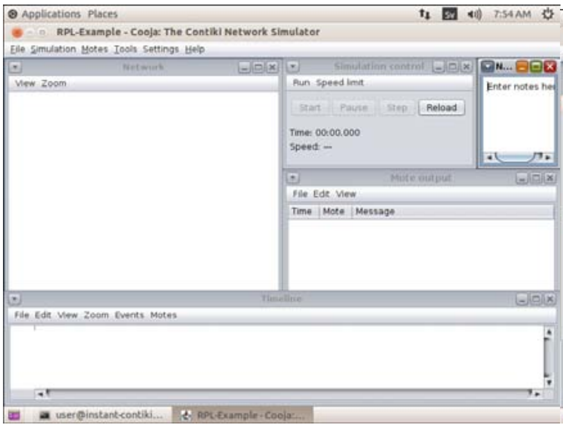
```
user@instant-contiki:~$ cd contiki-3.0/tools/cooja/
user@instant-contiki:~/contiki-3.0/tools/cooja$ ant run
```

Fig 3 Starting Cooja

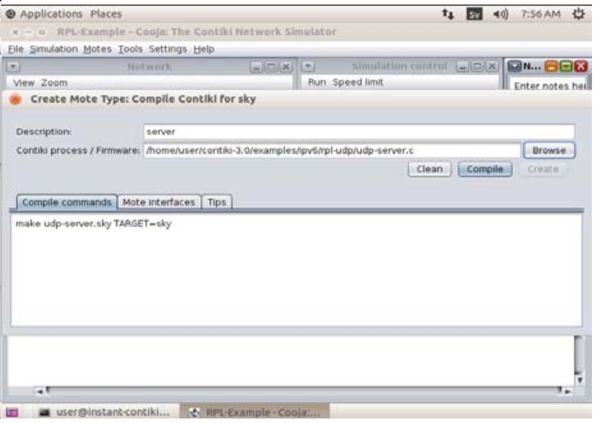


Simulation name: RPL-Example
Advanced settings
Radio medium: Unit Disk Graph Medium (UDGM): Distance Loss
Mote startup delay (ms): 1,000
Random seed: 123,456
New random seed on reload □

Fig. 4 Creating new simulatio



Time: 00:00.000
Speed: ---



Description: server
Contiki process / Firmware: /home/user/contiki-3.0/examples/ipv6/rpl-udp/udp-server.c

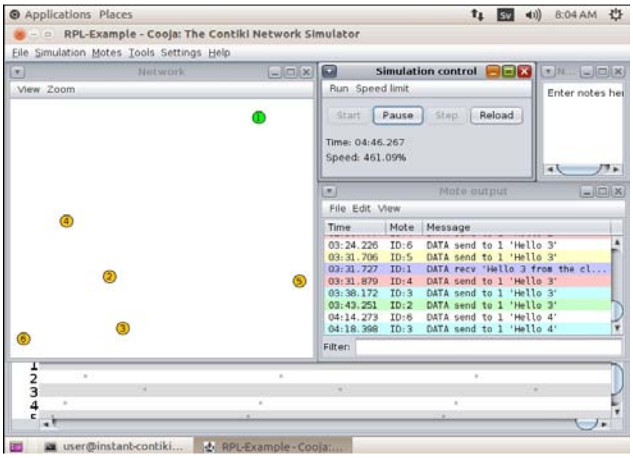
```
make udp-server.sky TARGET=sky
```

Fig. 5 Simulation interface

Fig 6 Create mote type interface

Setting Mote Types

Similarly, we may create the UDP Client mote by using the *udp-client.c* file. Once we do this, we will notice that a total of six randomly placed nodes will appear in the Network window. One possible random arrangement can be seen in Figure 7 . Amongst these, node 1 is the UDP Server and the rest are nodes which will execute the UDP Client code.



Time: 04:46.267
Speed: 461.09%

```
Time        Mote   Message
03:24.226   ID:6   DATA send to 1 'Hello 3'
03:31.706   ID:5   DATA send to 1 'Hello 3'
03:31.727   ID:1   DATA recv 'Hello 3 from the cl...
03:31.879   ID:4   DATA send to 1 'Hello 3'
03:38.172   ID:3   DATA send to 1 'Hello 3'
03:43.251   ID:2   DATA send to 1 'Hello 3'
04:14.273   ID:6   DATA send to 1 'Hello 4'
04:18.398   ID:3   DATA send to 1 'Hello 4'
```

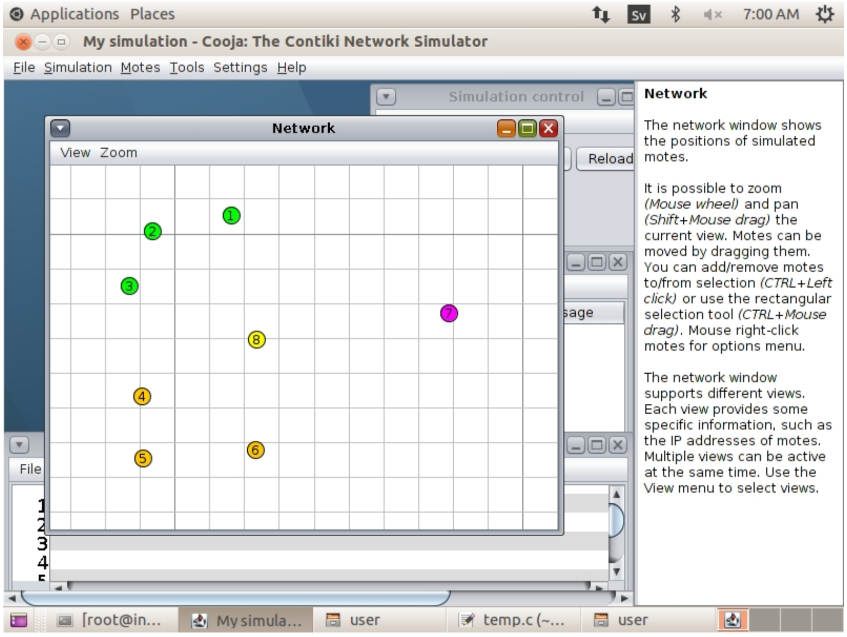
Fig. 7 Example Output

Proposed Work

The proposed algorithm shows the method of trustworthy data identify by RSSI value. To identify trustworthy data we check the RSSI value and also sensing value of sensor neighbor node as well as own node. If both have a same RSSI value and sensing value then sensor node is trustworthy. But some sensor node does not have same RSSI value but same sensing value i.e. temperature value, humidity etc. then that particular sensor node will be discarded.

```
Repeat
Sensor node: Sensor Value
for i in Read (Sensor node)
    Print "Sensor data"
End For
If RSSI value (Sensor node)! = RSSI value (neighbor node) and
    Sensor value (Sensor node) == Sensor value (neighbor node) then
    Print "On – off attack generate in Sensor network and node will discard"
Else
    Print "Right Node available in sensor network"
```

Wireless Sensor Network



Network

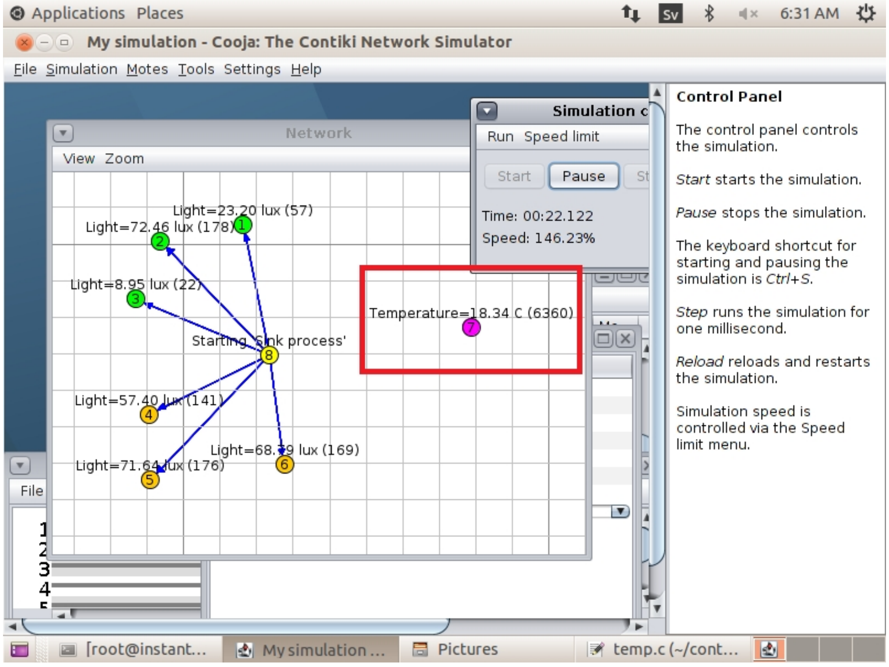
The network window shows the positions of simulated motes.

It is possible to zoom *(Mouse wheel)* and pan *(Shift+Mouse drag)* the current view. Motes can be moved by dragging them. You can add/remove motes to/from selection *(CTRL+Left click)* or use the rectangular selection tool *(CTRL+Mouse drag)*. Mouse right-click motes for options menu.

The network window supports different views. Each view provides some specific information, such as the IP addresses of motes. Multiple views can be active at the same time. Use the View menu to select views.

Fig 8 Wireless Sensor Network

To identify Trustworthy Data Using RSSI Value



Light=23.20 lux (57)

Light=72.46 lux (178)

Light=8.95 lux (22)

Starting 'Sink process'

Light=57.40 lux (141)

Light=68.79 lux (169)

Light=71.64 lux (176)

Temperature=18.34 C (6360)

Time: 00:22.122

Speed: 146.23%

Control Panel

The control panel controls the simulation.

Start starts the simulation.

Pause stops the simulation.

The keyboard shortcut for starting and pausing the simulation is *Ctrl+S*.

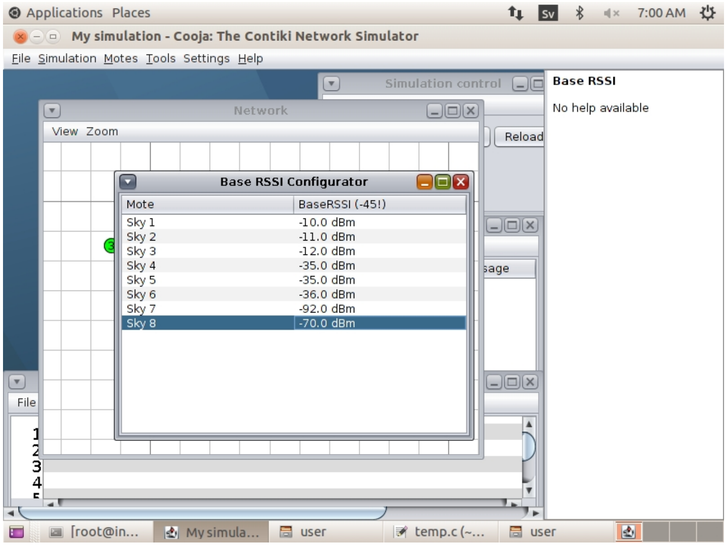
Step runs the simulation for one millisecond.

Reload reloads and restarts the simulation.

Simulation speed is controlled via the Speed limit menu.

Fig 9 Identify Trustworthy Node and Data

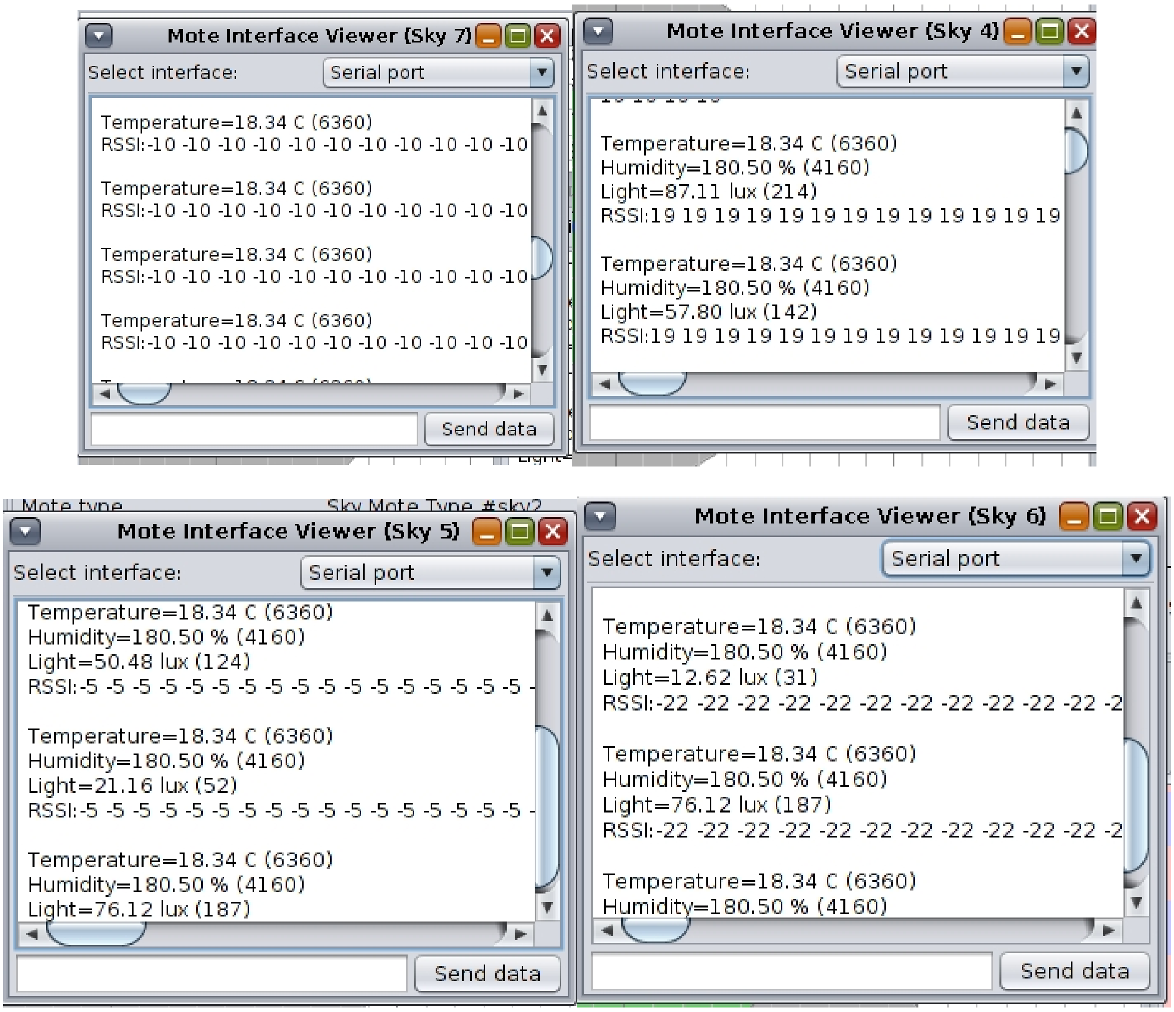
In Figure 9 red rectangle indicate the untrustworthy data and node because it is not connect to sensor node and behave like on-off attack. Because its temperature data is same but RSSI value is different.



Mote	BaseRSSI (-45!)
Sky 1	-10.0 dBm
Sky 2	-11.0 dBm
Sky 3	-12.0 dBm
Sky 4	-35.0 dBm
Sky 5	-35.0 dBm
Sky 6	-36.0 dBm
Sky 7	-92.0 dBm
Sky 8	-70.0 dBm

Fig 10 Base RSSI Value of Sensor Node

Sensor Data Value



```
Temperature=18.34 C (6360)
RSSI:-10 -10 -10 -10 -10 -10 -10 -10 -10 -10 -10

Temperature=18.34 C (6360)
RSSI:-10 -10 -10 -10 -10 -10 -10 -10 -10 -10 -10

Temperature=18.34 C (6360)
RSSI:-10 -10 -10 -10 -10 -10 -10 -10 -10 -10 -10

Temperature=18.34 C (6360)
RSSI:-10 -10 -10 -10 -10 -10 -10 -10 -10 -10 -10
```

```
Temperature=18.34 C (6360)
Humidity=180.50 % (4160)
Light=87.11 lux (214)
RSSI:19 19 19 19 19 19 19 19 19 19 19 19 19

Temperature=18.34 C (6360)
Humidity=180.50 % (4160)
Light=57.80 lux (142)
RSSI:19 19 19 19 19 19 19 19 19 19 19 19 19
```

```
Temperature=18.34 C (6360)
Humidity=180.50 % (4160)
Light=50.48 lux (124)
RSSI:-5 -5 -5 -5 -5 -5 -5 -5 -5 -5 -5 -5 -5 -5 -5 -5 -5 -

Temperature=18.34 C (6360)
Humidity=180.50 % (4160)
Light=21.16 lux (52)
RSSI:-5 -5 -5 -5 -5 -5 -5 -5 -5 -5 -5 -5 -5 -5 -5 -5 -5 -

Temperature=18.34 C (6360)
Humidity=180.50 % (4160)
Light=76.12 lux (187)
```

```
Temperature=18.34 C (6360)
Humidity=180.50 % (4160)
Light=12.62 lux (31)
RSSI:-22 -22 -22 -22 -22 -22 -22 -22 -22 -22 -22 -2

Temperature=18.34 C (6360)
Humidity=180.50 % (4160)
Light=76.12 lux (187)
RSSI:-22 -22 -22 -22 -22 -22 -22 -22 -22 -22 -22 -2

Temperature=18.34 C (6360)
Humidity=180.50 % (4160)
```

CONCLUSION AND FUTURE WORK

Every sensor has a limited memory and computing power so it is required store data in sensor node must be trustworthy, which make routing in devices more challenging. Using 6LoWPAN (IEEE 802.15.4), RSSI value we easily find trustworthy sensor data by comparing its RSSI value to its neighbor node available in network. As in our proposed algorithm, we have considered RSSI value of the particular signal as a parameter which indicates the strength of the received signal. This will help in the selection of the sensor node from which the incoming signal is having high RSSI value i.e. nearby node which leads to the best path to follow for the

Transmission of the packet. There are several other aspects that need to be explored as a future

work. Our next work is to measure value of the performance metrics for the existing algorithm and for the proposed work we measure on – off attack. Using RSSI value and 6LoWPAN IP based protocol we compare the sensor node RSSI value with near available sensor node and also compare sensor node sensed data. If sensor node have different RSSI value but same sensed data then in wireless sensor network contains on – off attack and that malicious behavior must be detect.

In these proposed system we create virtual sensor network but in future we work with real time data of sensor network so we find malicious activity and avoid the bad mouth attack, ballot stuffing attack from wireless sensor network. Then compare their scenario with result of simulation study.

REFERENCES

[1] W. Li, H. Song and F. Zeng, “Policy-based Secure and Trustworthy Sensing for Internet of Things in Smart Cities," in *IEEE Internet of Things Journal*, vol.5 (2), pp. 1-8, 2017.

[2] B. Liu, S. Cheng, “State space model-based trust evaluation over wireless sensor networks: an iterative particle filter approach,” in *The Journal of Engineering*, pp.1-9, Mar 2017.

[3] T. Zhang, J. Ma, N. Xi, X. Liu, Z. Liu, and J. Xiong, “Trustworthy service composition in service-oriented mobile social networks,” in 2014 IEEE International Conference on Web Services (ICWS), Alaska, USA, June 2014, pp. 684–687.

[4] M. Pouryazdan and B. Kantarci, “The Smart Citizen Factor in Trustworthy Smart City Crowdsensing,” in *IT Professional*, vol.18 (4), pp. 26-33, July/Aug 2016.

[5] J. Guo, I. Chen, J. J.P. Tsai, “A survey of trust computation models for service management in internet of things systems,” in *Computer Communications*, vol. 97, pp. 1-19, Jan 2016.

[6] L. Gu, J. Wang and B. Sun, “Trust management mechanism for Internet of Things,” in *China Communications*, vol.11(2), pp. 148-156, Feb 2014.

[7] Y. Yang, L. Wu, G. Yin, L. Li and H. Zhao, “A Survey on Security and Privacy Issues in Internet-of-Things,” in *IEEE Internet of Things Journal*, vol.4(5), pp. 1250-1258, Oct 2017.

[8] R. Giuliano, F. Mazzenga, A. Neri and A. M. Vegni, “Security Access Protocols in IoT Capillary Networks,” in *IEEE Internet of Things Journal*, vol. 4(3), pp. 645-657, Jun 2017.

[9] V. Adat, B. B. Gupta, “Security in Internet of Things: issues, challenges, taxonomy, and architecture,” in *Telecommunication System*, Vol.129, pp. 1-19, Jun 2017.

[10] C. F. Gago, F. Moyano, J. Lopez, “Modelling trust dynamics in the Internet of Things,” in *Information Sciences*, vol. 396, pp. 72-82, Feb 2017.