Analysis and Implementation for Secured Version Number and Rank Authentication (VeRA) in RPL (IoT)

Project Report submitted in partial fulfillment of the requirement for the degree of

Master of Technology

in

Computer Science & Engineering

under the Supervision of

DR. SHAILENDRA SHUKLA

By

PRIYANSHI SHARMA

Roll No. 152216

Jaypee University of Information Technology

Waknaghat, Solan – 173234, Himachal Pradesh

Certificate

This is to certify that project report entitled "**An Effectual Implementation for Secured Version Number and Rank Authentication in RPL(IoT)**", submitted by **Priyanshi Sharma** in partial fulfillment for the award of degree of Master of Technology in Computer Science & Engineering to Jaypee University of Information Technology, Waknaghat, Solan has been made under my supervision.

This report has not been submitted partially or fully to any other University or Institute for the award of this or any other degree or diploma.

Date:

Dr. Shailendra Shukla

Assistant Professor

Date: **Co-Supervisor's Name & Signature**

Designation

Acknowledgement

It is always said that God show the path in any challenge and any walk of life, so firstly my heartiest reverence to my Guru and God whose blessings have filled my life with wisdom, joy and prosperity.

I would like to express my immense gratitude and appreciate to my Supervisor **'Dr. Shailendra Shukla'** for his advice, support, guidance and inspiration throughout the course of my study. His enthusiasm and practical views on research have made a deep impression on me. I owe him my deepest gratitude for showing me the way to study and to conduct research.

I am thankful to **'Prof. S.P Ghrera'** Head of Department, Computer Science and Engineering, JUIT Waknaghat. I also express my sincere thanks to **'Dr. Pardeep Kumar'**, Assistant Professor in Computer Science and Engineering Department; for their inspiration, suggestions, moral support and guidance during the course of my study.

I would also like to thank all the staff of JUIT, Solan for their friendly behavior and assistance during my research study. Special thanks also due to my Friends for their assistance and expert advice.

Finally, without the support of my Family, their understanding and patience, it would have been impossible for me to finally complete my study.

Date:

Signature:

PRIYANSHI SHARMA

Table of Content

List of Figures

List of Tables

Abstract

In the current era of digital world as well as globalization, the interconnectivity is growing at very swift rate. Now days, we are surrounded with number of gadgets, mobile devices, smartphones, wireless nodes and many other objects which are digitally connected in real time. Internet of Things (IoT) is one of the prominent domains in wireless networking which enable the link between the real world objects. With the implementation of IoT, the physical objects in real world can be connected with each other to share the information and communicate in real time with higher degree of performance as well as security. IoT works on the development and integration of smart objects which can be controlled using remote network infrastructure. In this research work with the proposed security in the IoT networks, the scenario of dynamic key exchange between the motes shall be done in which the dynamic security key will be generated and authenticated for communication. In IoT security, it is necessary to devise and implement the protocols and algorithms by which the overall privacy and security in communication can be enforced to avoid any intrusion. As IoT can be used for military applications, it becomes mandatory to work on highly secured algorithms of key exchange with dynamic cryptography of security keys. The existing algorithm is devised with the integration of dynamic hybrid keys for secured communication to give the improved results on multiple parameters. In this simulation of IoT network, the scenario of dynamic key exchange between the motes is done in which the dynamic security key is being generated and authenticated for communication. In IoT security, it is necessary to devise and implement the protocols and algorithms by which the overall privacy and security in communication can be enforced to avoid any intrusion. As IoT can be used for military applications, it becomes mandatory to work on highly secured algorithms of key exchange with dynamic cryptography of security keys. The implementation is done using Cooja IoT Simulator to depict the scenarios. The implementation for IoT security is done on Cooja simulator so that the dynamic key exchange and security aspects can be presented.

Keywords: Contiki, Cooja Simulator, Internet of Things, IoT Security, RPL

CHAPTER 1

INTRODUCTION

1.1 Internet of Things

In the recent years, the machine to machine communication is in use and Internet of Things (IoT) [1] is becoming very famous. In the traffic system, the problem of congestion control is very common and it is classically handled by the global positioning systems by the drivers as well as traffic administrative authorities. But as the traffic density is increasing day by day, it is becoming difficult to handle and view all the possibilities in the prospective traffic area where the driver is willing to move. Moreover, the problem of security and integrity is also increasing rapidly as there are number of attacks in VANET [2] and GPS [3] systems being used by the crackers by sending the malicious code or fake packets. Ubiquitous computing is one of the recent technologies that is in the phase of implementation under Internet of Things (IoT).

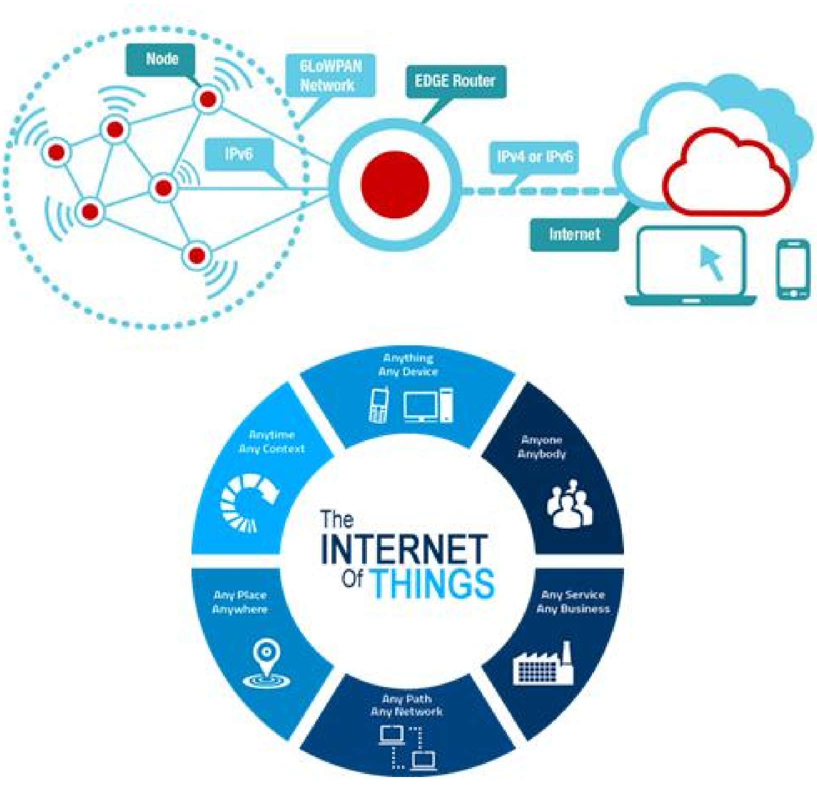


Figure 1.1: Internet of Things [1]

The term Internet of Things was first presented by Kevin Ashton in year 1999. The implementation of IoT is widespread now because of the availability of high performance wireless technologies. Radio Frequency Identification (RFID) tags and Sensors arebase in the implementation of IoT.The RFID tags can be embedded in real world devices and objects which can be monitored remotely using software based applications. The RFID readers can be used to locate, read and sense the RFID implanted objects. Very small micro sized transmitting and receiving chips are integrated with RFID which can communicate at distant point.

As per the reports from Forbes.com, the market of Internet of Things will reach around 267 billion dollars by year 2020. The analysis from Gartner underlines that around 8.4 billion objects with investment of 273 billion dollars will be interconnected with each other in current year 2017.

This figure of 8.4 billion objects is 31% more than the implementation figures of previous year 2016.

Some of the key applications of IoT are

- Smart Cities
- Smart Retail Points
- Smart Grid
- Smart Agriculture and Farming
- Internet of Vehicles (IoV)
- Connected Cars
- Connected Railways Infrastructure
- Wearable Devices
- Smart Home
- Smart Offices
- Software Defined Networking
- Smart Supply Chain
- Smart Healthcare and Smart Ambulances
- Industrial Internet
- Energy Management
- and many others

Following are some of the applications and real world implementations of Intelligent Transportation System throughout the globe

- Smart Traffic Control Lights with projection and display of varying speed limit
- Auto-Detection of Number Plate System disobeying the traffic signals and messages
- Speed Detection Cameras
- Collision Avoidance and Detection Systems
- Vehicle Notification Systems for Critical and Emergency Points

Figure 1.2 shows the technology trends in the Internet of Things, as with the technological advancement the Internet of Things is on the boom covering the whole.

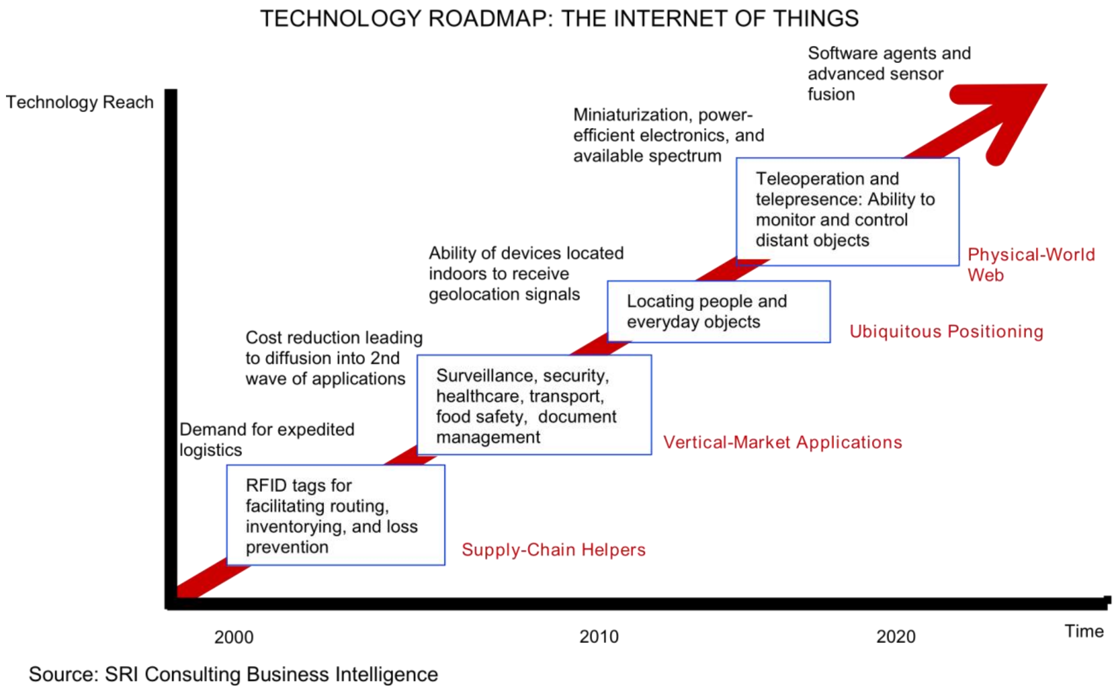


Figure 1.2 –Technology Trends in IoT [5]

Interconnectivity is the basic characteristic for IoT since the whole concept is built upon the idea of being able to interconnect everything (despite the traffic going through different networks).

Table 1.1 – Characteristics of IoT [6]

Characteristics	Description
Interconnectivity	Everything can be connected to the global information and communication infrastructure
Things-related services	Provides things-related services within the constraints of things, such as privacy and semantic consistency between physical and virtual thing.
Heterogeneity	Devices within IoT have different hardware and use different networks but they can still interact with other devices through different networks.
Dynamic changes	The state of a device can change dynamically, thus the number of devices can vary. (Device states: connected, disconnected, waking up, and sleeping)
Enormous scale	The number of devices operating and communicating will be larger than the number of devices in the current Internet. Most of this communication will be device to device instead of human to device.

1.2 Attacks on IoT based Virtual Infrastructure

Different types of attacks are used to control and damage the VANET at different layers. The vehicular nodes and associated infrastructure are key points and components in VANET. The attackers can damage and control the vehicular network by sending the malicious packets and signals and infrastructure can be virtually destroyed. Such attacks are in the high priority as these attacks affect the entire network [7]. A number of attacks are prevalent for controlling and damaging the vehicular networks.

Denial of service (DOS) Attack - Using DoS attack, the network availability is jammed by the attacker node or malicious packet. Fig. 1.2 shows the authentic and legitimate users are not able to access the network services. DoS is one of the prominent attack that works on the network layer of VANET.

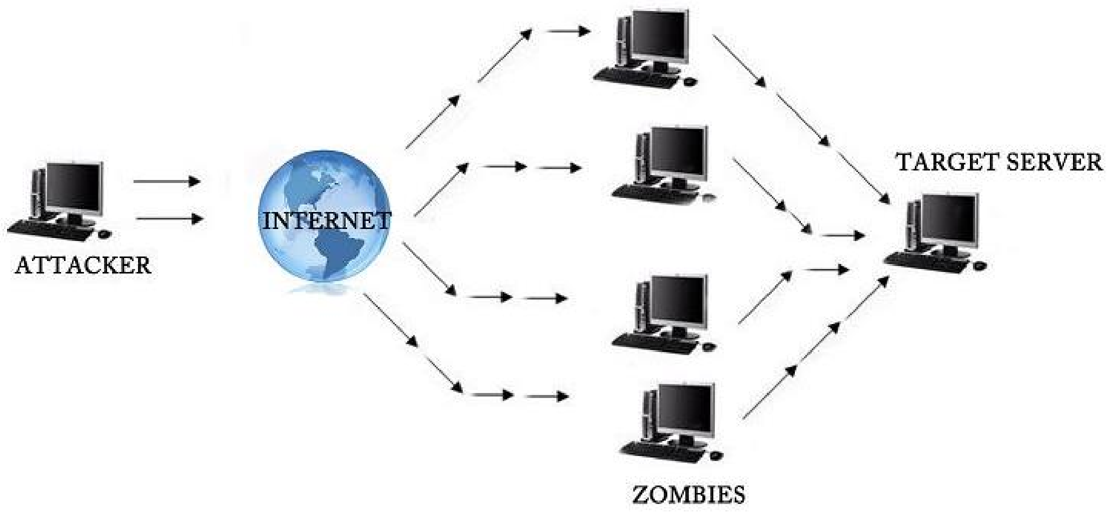


Figure 1.3 –Denial of Service Attack in Internet of Vehicles [8]

Distributed Denial of service (DDOS) Attack - DDOS attack is more dangerous in VANET as the mechanism involved is distributed in nature. In this attack, the malicious node or attacker perform the attack from multiple and different locations. Fig.1.3 shows the multidirectional jamming or blocking occurs in the network and authentic systems cannot communicate.

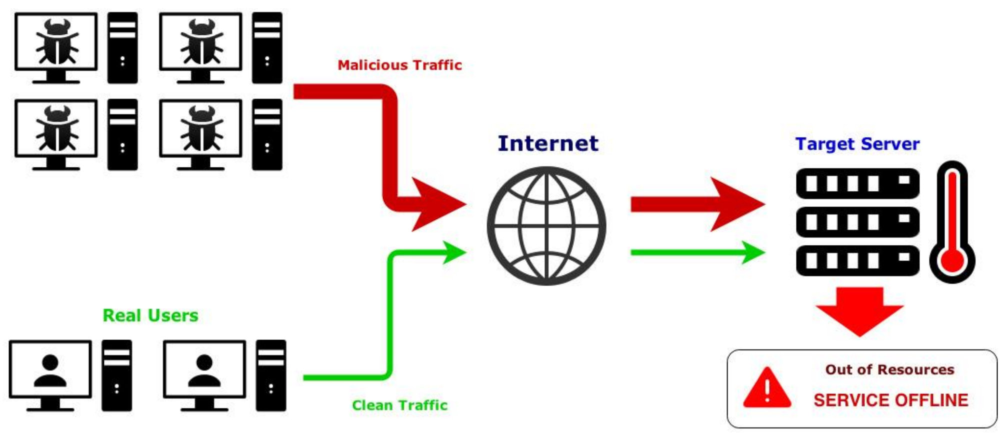


Figure 1.4 – Distributed Denial of Service Attack in Internet of Vehicles [8]

Sybil Attack-Sybil attack affects the network layer of vehicular network a lot. Using this attack, the manipulation of source identity takes place. The malicious node attempts to fabricate and manipulate the original identity and pretends to be a registered or original source node [9]. In Sybil attack, the attacker node creates assorted vehicles or nodes of same identity by replication and forces other nodes to leave or move fast from the road. Using resource testing these attacks can be detected which works on the assumption that vehicles have limited resources. This problem of Sybil attack can be addressed using public key cryptography where public keys are used to authenticate vehicles.

Node Imitation Attack - In this type of attack, the transmission of messages takes place by the imitated node of other identity[10]. In this way, the attacker can send the malicious or wrong messages to any node hiding or changing its own identity.

Application Level Attack - In this type of assault, the manipulation is done in the message received and then retransmitted to different nearby nodes or vehicles. This way, the network infrastructure and traffic can be damaged. For example, the message 'High Traffic Ahead' can be changed to 'Road Free Ahead, Move Fast' and then retransmitted to the nearby vehicles [11]. By this approach, the network congestion will be huge at the upcoming point or there can be situation of accident.

The modernization level of transport is currently an important aspect to take the measure of development. Progress in communication techniques and networking, together with vehicle location methods have become the key enablers of innovative transport systems. These three principal techniques for automatic location-sensing which are widely used for road transport of dangerous goods, logistics, armored car and other particular fields

- Triangulation
- Scene Analysis
- Proximity

The Internet of Things can logically be divided into a perception layer, a network layer, a service layer and an application layer. The perception layer senses, gathers information, and the network layer enables the connectivity between the different items making use of Internet technology, while the service layer offers services to the application or to the end user for further intelligent processing. Undoubtedly, this strong vision of Internet of Things could add new dimensions to Intelligent Transportation Systems and it will have a high impact on applications and services.

However, there are many challenges such as real-time traffic management, seamless connectivity, vehicle location prediction, security and privacy, interoperability, communications, associated with Internet of Things that needs to be addressed.

Next generation transportation systems based Internet of Things and sensors technologies:

- The intelligent transportation, connected vehicles and Internet of Things
- Intelligent vehicle monitoring system based on Internet of Things
- Distributed intelligent transportation system based Internet of Things architecture
- Internet of Things applications and services for real-time traffic management.
- Embedded systems and sensors for intelligent transportation systems.
- Wireless sensor devices in intelligent transportation systems.
- Vehicle location prediction based advanced sensor technologies.
- Peer-to-Peer data sharing for fleet management and safety purposes.
- Integrated transportation and sensors for location based services.

Wireless sensor networks are used to exchange information between an application platform and one or more sensor nodes. This exchange takes place in a wireless fashion. Figure describes the components of the wireless sensor networks are associated with each other.

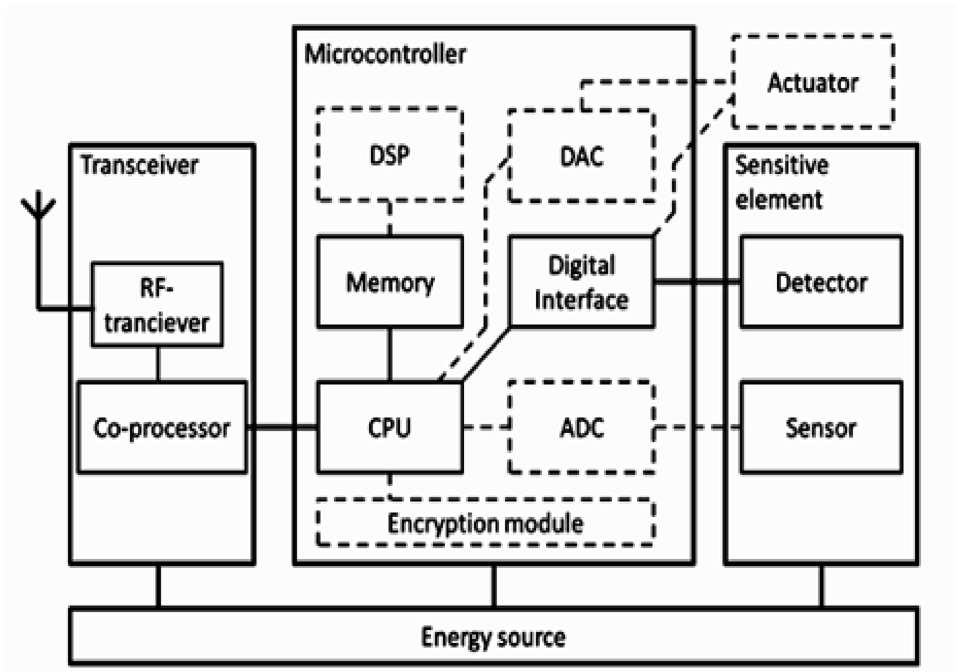


Figure 1.5 – Components of Sensor Node [2]

As shown in Figure 1.5 the IoT and related RFID is having number of applications in assorted domains.

There are number of specific purposes of sensors, such as measuring temperature, humidity, vibrations, motion, light, pressure and altitude. Companies will need to develop new applications to take advantage of all the big data that the sensors are generating. The lower costs and more advanced capabilities of RFID tags are starting to enable wider and more effective use. The cost of RFID, which has come down dramatically, is in more than just the tag itself. To determine the true cost per use you have to include the software applications and deployment costs. The combination of lowered costs for tags and improved capabilities means that their value proposition has changed, and represents an opportunity for enterprises to rethink RFID.

1.3 Ubiquitous Sensor Network

System characterizes the USN [12] as a theoretical system fabricated over existing physical systems which makes utilization of sensed information and gives learning administrations to anybody, anyplace and at whatever time and where the data is created by utilizing setting mindfulness.

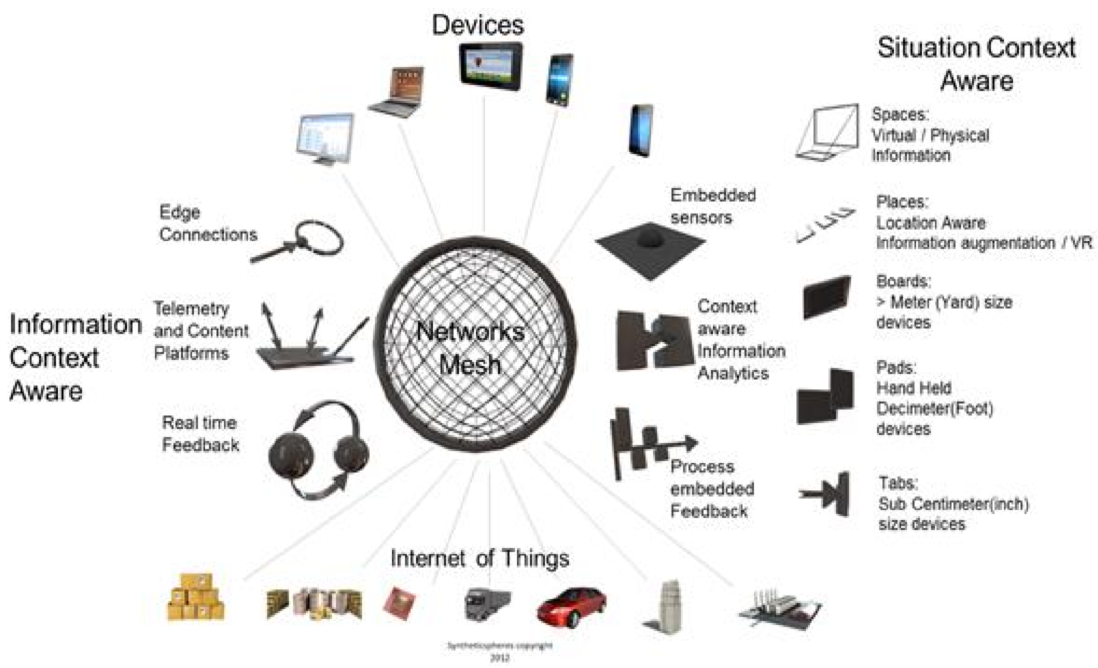


Figure 1.6 – Ubiquitous Systems [12]

In this definition "physical systems" implies different sorts of WSNs, as well as wired sensor systems and RFID [13,14].

1.4 Components of Sensor Used In IoT

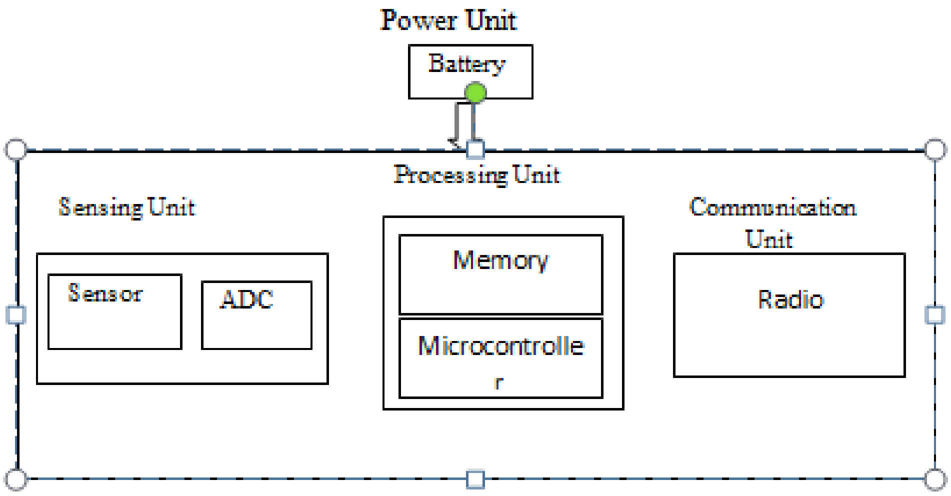


Figure 1.7- Components of Sensor used in IoT [13]

1.5 RPL (Routing Protocol over Low Power and Lossy Networks)

RPL alludes to the Routing Protocol in view of IPv6 that is implied and concocted towards Low-Power and Lossy Networks. It is taken accepted routing layered convention for the Internet of Things (IoT). From its consistency, RPL added to the advancement of correspondences in the realm of small, inserted, organizing gadgets, by giving, alongside different measures, gauge engineering for IoT. Routing issues are exceptionally trying for 6LoWPAN, given the low-power and lossy radio-interfaces, the battery provided hubs, the multi-bounce work topologies, and the successive topology changes because of portability. Fruitful arrangements ought to consider the particular application necessities, alongside IPv6 conduct and 6LoWPAN systems. A compelling arrangement was created by the IETF Routing Over Low power and Lossy (ROLL) systems working gathering. It has proposed the main IPv6 Routing Protocol for Low power and Lossy Networks (LLNs), RPL, in light of an inclination based approach.

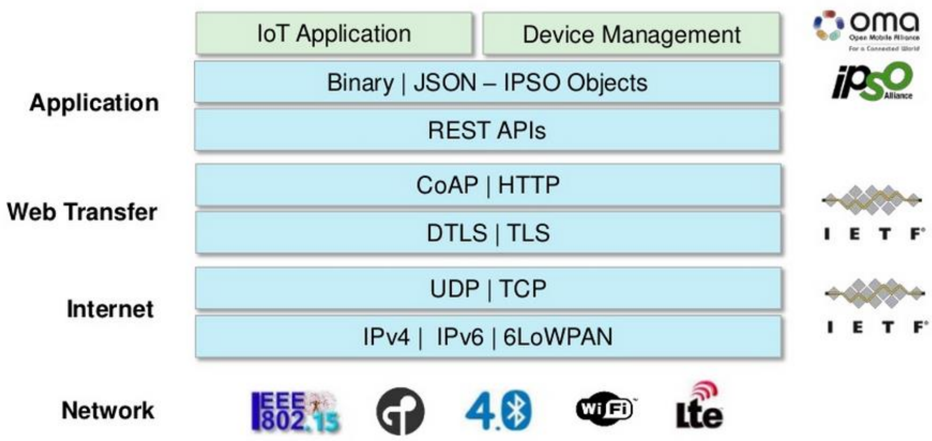


Figure 1.8 (a) : 6LowPAN Environment [15]

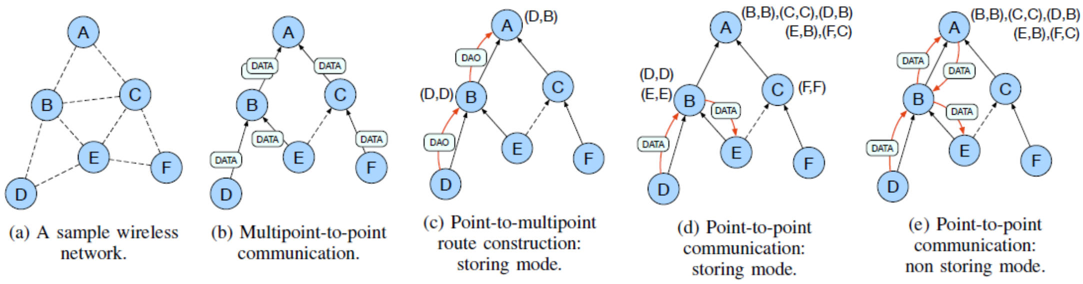


Figure 1.8 (b): Routing in RPL. Existing routes are shown next to the network nodes [15]

RPL can support a wide variety of different link layers, including ones that are constrained, potentially lossy, or typically utilized in conjunction with host or router devices with very limited resources, as in building/home automation, industrial environments, and urban applications. It is able to quickly build up network routes, to distribute routing knowledge among nodes, and to adapt the topology in a very efficient way. In the most typical setting entailed by RPL, the nodes of the network are connected through multi-hop paths to a small set of root devices, which are usually responsible for data collection and coordination duties. For each of them, a Destination Oriented Directed Acyclic Graph (DODAG) is created by accounting for link costs, node attributes/status information, and an Objective Function, which maps the optimization requirements of the target scenario. RPL can encompass different kinds of traffic and signaling information exchanged among nodes depends on the requirements of the considered data flows. In details, it supports: Multipoint-to-Point (MP2P), Point-to-Multipoint (P2MP), and Point-to-Point (P2P) traffic.

1.6 Tools and Technologies for IoT Programming

OpenIoT (URL: http://www.openiot.eu/) - It is free and open source platform to manage and program the sensors on cloud and Internet based environment. The concept of Sensing as a Service is finely adopted in OpenIoT.

Zetta (URL: http://www.zettajs.org/) - It is free and open source platform that is having base of Node.js. Zetta is used to create the IoT Servers which can control and run the worldwide distributed systems, sensors and computers including on-cloud.

DSA (URL: http://www.iot-dsa.org/) - Distributed services Architecture is one of the powerful IoT library under free and open source distribution. It makes the inter-objects communication very effective with higher degree of performance. DSA provides the toolkit for managing the IoT based applications, services as well as objects.

Node-RED (URL: http://nodered.org/) - Node-RED provides the programming interface and APIs for the Internet of Things. Using Node-RED, the flow based creation of remote IoT objects can be done with an easy web browser based flow editor. In the flow editor of Node-RED, the JavaScript code can be executed and remote objects can be programmed with easy as well powerful functionalities

IoTivity (URL: https://www.iotivity.org/) - IoTivity a powerful open source library which enable to inter-object connectivity with enormous speed and performance. It is written and programmed in C and C++. Most of the performance aware protocols like ANT+, Bluetooth low energy, Wi-Fi Direct, Zigbee, Z-Wave and others can be easy integrated with IoTivity.

Following is the list of other open source implementations for Internet of Things

Development Toolkits and Libraries

- Arduino
- Eclipse IoT Project
- Kinoma
- M2MLabs Mainspring
- Node-RED

- ThingBox

Automation for Home and Offices

- Eclipse SmartHome
- Home Gateway Initiative (HGI)
- Ninja Blocks
- openHAB
- PrivateEyePi
- RaZberry
- The Thing System

Middleware

- IoTSyS
- Kaa
- OpenIoT
- OpenRemote

Operating Systems

- AllJoyn
- Brillo
- Contiki
- FreeRTOS
- Raspbian
- RIOT
- Spark
- TinyOS

IoT Integration Tools and Horizontal Platforms

- Canopy
- Chimera IoT
- DeviceHive
- IoT Toolkit
- M2MLabs Mainspring

- Mango
- Nimbits
- Open Source Internet of Things (OSIoT)
- OpenRemote
- Pico Labs
- prpl Foundation
- RabbitMQ
- SiteWhere
- SiteWhere
- ThingSpeak
- webinos
- Yaler

Protocols

- Advanced Message Queuing Protocol (AMQP)
- Constrained Application Protocol (CoAP)
- Extensible Messaging and Presence Protocol (XMPP)
- OASIS Message Queuing Telemetry Transport (MQTT)
- Very Simple Control Protocol (VSCP)

Implementations for Engineering

- Open Garden
- Open Source Robotics Foundation
- OpenWSN

CHAPTER 2
LITERATURE SURVEY

A number of researchers and practitioners have worked on the analysis of remote sensor technology and IoT but there is huge scope for the improvement in cases where data transmission & integrity is necessary due to huge requirements of confidentiality & integrity.

2.1 Extracts of the Literature Evaluated

Table 2.1 – Effective Evaluation of Literature Analyzed

Authors	Work	Advantages	Disadvantages
Atzori [1], (2003)	Deep evaluation of IoT and the assorted applications in multi perspectives. Enormous aspects of data transmission and security is addressed	Multi-factor authentication and performance aspects are investigated on assorted parameters	Complexity and cost is the key issue
An L. [2], (2003)	Security and Integrity aspects are incorporated with the cryptology in the algorithmic approaches. Devised new approach for security and overall effectiveness	Devised new approach for the security in IoT and including vehicular networks which is effectual in multiple scenarios	Cost Factors higher
Ben et. al [3], (2004)	IoT and its applications in medical domain is addressed with the real time experimental results.	Overall performance and multiple scenarios for the analysis of medical	Effectiveness in the security to more than 5% is escalated

		examinations and monitoring using IoT	
David [4], (2004)	Devised and implemented the TinySec, the first fully-implemented link layer security architecture for wireless sensor networks	Novel and effective approach for security and integrity is devised and integrated in IoT based environment	Overall turnaround time
Jayasudha [5], (2012)	Dissect the target environment and impart data to the base station for further resolution, The data aggregation using this algorithm will reduce energy consumption and there is a significant trade-off between communication and computation cost	A novel and effectual with the energy parameter network is considered and integrated	Evaluation on cost and complexity not implemented
Jun [6], (2011)	Exploration of wireless technologies with the communication links modeled as independent on/off channels for the escalation model of IoT.	The usage of wireless RFID and multiple channels considered for performance aware IoT	Deep review is done and proposed the efficiency using soft computing
Kopetz [7], (2007)	Incorporation and integration of RFID for the implementation of IoT in assorted	Integration of remote frequency based devices integrated with	Complexity is a key aspect

	scenarios	multiple dimensions to have better control and effective communication	
Wenliang [8], (2010)	Proposed and implemented security in wireless sensor networks with the use of encrypt messages sent among sensor nodes. Keys for encryption purposes must he agreed upon by communicating nodes	Higher security is achieved	Higher complexity in specific cases
Roberto [9], (2006)	The performance of the Direct Protocol is analytically characterized while, for the Co-operative Protocol, the work provide both analytical evaluations and extensive simulations	Performance aware network is proposed with the higher level of security and less complexity	More complexity can be there in specific cases of multilayered approaches
Wenliang [10], (2010)	Provides a framework in which to study the security of key pre distribution schemes, propose a new key pre distribution scheme which substantially improves the resilience of the network	Novel and effectual approach using predistribution scheme is used that is better and performance aware	Complexity and cost is the key issue

	compared to previous schemes, and give an in-depth analysis of the scheme in terms of network resilience and associated overhead.		
Biswas, K. et. al. [39], (2006)	Preserve the basic security features such as confidentiality and integrity as well as to protect from replay attack in presence of mote class attacker.	Basic security and integrity to achieve higher performance	Execution Time and Complexity
Bussi, K. et. al. [40], (2006)	A light-weight, one-way, cryptographic hash algorithm is suggested with a target to produce a hash-digest with fixed and relatively small length for such an energy-starved wireless network. The primary focus is making the algorithm light-weight so that upon using it in application of network like WSN, the nodes can successfully run the algorithm with low energy.	Lightweight and cost effective protocol	Compatibility for multiple networks
Carl Endorf et. al. [41], (2010)	Presents an ultra-lightweight first-order side-channel resistant crypto of KLEIN, which is a new family of lightweight block cipher	Ultra-lightweight first-order side-channel resistant crypto of KLEIN	Assorted network compliance

	that has advantages in both of software and hardware performances		
Chen, C.L. et. al. [42], (2009)	Underlines the secure information aggregation using homomorphic encryption in wireless sensor networks allows data to be aggregated without having to decrypt the packets. While data aggregation provides a means to reduce network traffic, homomorphic encryption increases the size of the packets and this could negatively affect system performance		Execution Time and Complexity
Cochavy et. al. [43], (2006)	Propose a lightweight hash, Neeva-hash satisfying the very basic idea of lightweight cryptography. Neeva-hash is based on sponge mode of iteration with software friendly permutation which provides great efficiency and required security in RFID technology. The proposed hash can be used for many application based purposes.	Devise new approach for security and integrity	Adaptability
Dimitris M. et. al. [44], (2013)	Addresses that W.S.N demands are lightweight security schemes due to	Implementation of lightweight and secured protocol	Execution Time and Complexity

	the fact that the nodes in the networks are resource constrained. In order to provide secure data transmission in wireless sensor networks, cryptographic algorithms has to be incorporated		
Donna A. et al. [45], (2015)	Considers two different applications: hop by hop transmission of data from cluster nodes to the base station and the direct access to cluster nodes data by mobile users via mobile devices. Due to the hardware limitations of WSNs, some low-cost operations such as symmetric cryptographic algorithms and hash functions are used to implement a dynamic key management	Devise new approach or mobile as well as wireless networks to achieve higher degree of accuracy and security	
Ghosal, A. et. al. [46], (2016)	In this work, various authentication protocols such as key management protocols, lightweight authentication protocols, and broadcast authentication protocols are compared and analyzed for all secure transmission applications.	Implementation of assorted factors in the authentication protocols	Performance
Kiruthika, B.	The authors have also	Implementation of	Cost factor and

et. al. [47], (2004)	performed a number of statistical tests and cryptanalytic attacks to evaluate the security strength of the algorithm and found the cipher provably secure.	statistical tests and machine intelligence	execution time
Naveena [48], (2015)	In this survey, the authors enhance the role of elliptical curve cryptography in wireless ad-hoc networks.	ECC Approach is used for wireless network security	
Mallikarjunaswamy [49], (2004)	To avoid the energy consumption over a cryptographic operations are design of Message Authentication protocol for Lifetime enhancement In wireless sensor networks called MALLI, which uses a famous structure of hash algorithm 2AMD-160. To demonstrate that, the execution time and the security achieved by the proposed method are more effective than the traditional approaches.	Energy optimization and security are achieved	
Tejeshwari [50], (2008)	In this paper, the authors propose a secured ACP for Wireless networks. This protocol is based on Elliptic Curve Discrete	Use of new approach for encryption and security	

	Log Problem (ECDLP) and double trapdoor chameleon hash function which secures the WSN from malicious attacks such as node masquerading attack, replay attack, man-in-the-middle attack, and forgery attacks. Proposed ACP has a special feature known as session key security. Also, the proposed ACP is more efficient as it requires only one modular multiplication during the initialization phase.		
Amit[51], (2011)	VeRA-Version no. & Rank Authentication in RPL	It checks that version number is modified by root node or malicious node.	Complexity and overhead

2.2 Analysis of Research Papers and Articles

Atzori et. al. [1] addressed the Internet of Things. Principle empowering component of this promising standard is the coordination of a few advancements and interchanges arrangements. Recognizable proof and following advances, wired and remote sensor and actuator systems, improved correspondence conventions (imparted to the Next Generation Internet), and appropriated insight for keen articles are only the most significant. As one can undoubtedly envision, any genuine commitment to the development of the Internet of Things must essentially be the aftereffect of synergetic exercises directed in diverse fields of learning, for example, information transfers, informatics, gadgets and sociology. In such an intricate situation, this review is coordinated to the individuals who need to approach this unpredictable train and add to its improvement. Diverse dreams of this Internet of Things standard are accounted for and empowering advancements audited. What rises is that still real issues should be confronted by the exploration group.

An L. [2] proposed the Public key cryptography (PKC) in IoT as the enabling technology underlying many security services and protocols in traditional networks such as the Internet. “In the context of wireless sensor networks, elliptic curve cryptography (ECC), one of the most efficient types of PKC, is being investigated to provide PKC support in sensor network applications so that the existing PKC-based solutions can be exploited. This paper presents the design, implementation, and evaluation of TinyECC, a configurable library for ECC operations in wireless sensor networks.

Ben et. al. [3] proposed a new range of applications such as large area monitoring including environmental monitoring, wildlife exploration, and real time patient medical data which is collected by using wireless sensors. The purpose of this paper is to present the initial effort in building a flexible strategy to achieve secure data transmission in medical wireless sensor networks.

David [4] introduced TinySec, the first fully-implemented link layer security architecture for wireless sensor networks. In the design, the authors leverage recent lessons learned from design vulnerabilities in security protocols for other wireless networks such as 802.11b and GSM.

Jayasudha [5] proposed the wireless sensor networks unceasingly scrutinize the target environment and impart data to the base station for further resolution. Since it is a resource constraints environment, network lifetime pursues on the battery backup. Hence in this paper, clustering based localized prediction scheme is proposed by exploiting spatial and temporal correlation to have accurate data aggregation and energy efficient network.

Jun [6] explored topological properties of WSNs employing the q-composite scheme in the case of $q = 1$ with unreliable communication links modeled as independent on/off channels. However, it is challenging to derive results for general q under such on/off channel model. In this paper, the authors resolve such challenge and investigate topological properties related to node degree in WSNs operating under the q-composite scheme and the on/off channel model.

Kopetz [7] associated the physical things to the Internet makes it conceivable to get to remote sensor information and to control the physical world from a separation.

Wenliang [8] achieved the security in wireless sensor networks with the use of encrypt messages sent among sensor nodes. Keys for encryption purposes must he agreed upon by communicating nodes. Due to resource constraints, achieving such key agreement in wireless sensor networks is nontrivial.

Roberto [9] built the first Direct Protocol, a second Co-operative Protocol. The Co-operative Protocol is adaptive: its security properties can be dynamically changed during the life-time of the WSN. Both protocols also guarantee implicit and probabilistic mutual authentication without any additional overhead and without the presence of a base station.

Wenliang [10] achieved the security in wireless sensor networks, it is important to be able to encrypt and authenticate messages sent between sensor nodes. Before doing so, keys for performing encryption and authentication must be agreed upon by the communicating parties. Due to resource constraints, however, achieving key agreement in wireless sensor networks is nontrivial.

Biswas, K.et. al. [39] aims to preserve the basic security features such as confidentiality and integrity as well as to protect from replay attack in presence of mote class attacker.

Bussi, K. et. al. [40] cryptographic hash calculation is proposed with an objective to deliver a hash-process with settled and moderately little length for such vitality starved remote system.

Carl Endorf et. al. [41] presents an ultra-lightweight first-order side-channel resistant crypto of KLEIN, which is a new family of lightweight block cipher that has advantages in both of software and hardware performances.

Chen, C.L. et. al. [42] underlines the secure information aggregation using homomorphic encryption in wireless networks allows data to be aggregated without having to decrypt the packets.

Cochavy et. al. [43] proposes a lightweight hash, Neeva-hash satisfying the very basic idea of lightweight cryptography. Neeva-hash is based on sponge mode of iteration with software friendly permutation which provides great efficiency and required security in RFID technology. The proposed hash can be used for many application based purposes.

Dimitris M. et. al. [44] addresses that the wireless networks requests for lightweight security conspires because of the way that the hubs in the systems are asset obliged. With a specific end goal to give secure information transmission in remote sensor systems, cryptographic calculations must be consolidated.

Donna A. et. al. [45] considers two different applications: hop by hop transmission of data from cluster nodes to the base station and the direct access to cluster nodes data by mobile users via mobile devices.

Ghosal, A. et. al.[46] in this work, various authentication protocols such as key management protocols, lightweight authentication protocols, and broadcast authentication protocols are compared and analyzed for all secure transmission applications.

Kiruthika, B. et. al. [47] addresses the limitations of security and integrity, this paper proposes a lightweight block cipher based on chaotic map and genetic operations. This sequence is used in XOR, mutation and crossover operations in order to encrypt the data blocks.

Mallikarjunaswamy [48] - To avoid the energy consumption over a cryptographic operations are design of Message Authentication protocol for Lifetime enhancement In wireless sensor networks called MALLI, which uses a famous structure of hash algorithm 2AMD-160. To demonstrate that, the execution time and the security achieved by the proposed method are more effective than the traditional approaches.

Tejeshwari [49] - In this paper, the authors propose a secured ACP for Wireless networks. This protocol is based on Elliptic Curve Discrete Log Problem (ECDLP) and double trapdoor chameleon hash function which secures the WSN from malicious attacks such as node masquerading attack, replay attack, man-in-the-middle attack, and forgery attacks. Proposed ACP has a special feature known as session key security.

CHAPTER 3

PROBLEM DESCRIPTION

3.1 Problem Formulation

Security and integrity is the main issue in IoT based network environment in which machine to machine communication is required. The proposed approach is making use of dynamic hybrid cryptography in the keys generation and authentication. The hybrid dynamic clustering based approach is security and performance aware as the data transmission is integrated without hindrance. The existing approach is fully secured and cannot be cracked by the interceptions. If there is any interception, the acknowledgement packet will be transmitted and intruding attempt can be identified. The key is generated with each simulation attempt at the time of data packet initialization so that the interceptions can be avoided with the analysis of historical patterns.

3.2 Need of the Issues Identified

Now days, the Internet of Things is widely used and integrated in almost all the domains whether it is related to smart vehicles, smart traffic control, airways, smart cities, smart ambulances, military applications and others. It becomes very necessary to work out the security aspects of IoT with the secured routing of packets so that the intrusion cannot take place and all the transmission can be fully secured.

CHAPTER 4
ANALYSIS OF EXISTING SOLUTION

4.1 Advantages of the Existing Approach

- Higher level of performance and integrity because of the dynamic location sensing
- Dynamic topology so that the consistency can be checked and evaluated
- The weights and related properties can be set on the real time dynamic network
- Integration of dynamic clustering approaches so that the key can be more secured
- The existing approach is effective in terms of higher integrity, security and performance
- Implementation of existing approach based on the dynamic clustering can be used for any type of network
- The existing aspects are effective and giving better results which are the key components of dynamic security on multiple parameters

This problem can arise in RPL when there is inconsistency in the topology. Inconsistency arises due to the congestion, loss of packets or any node failure.

4.2 Security Analysis of RPL

This issue can ascend in RPL when there is peculiarity in the topology. Irregularity ascends in perspective of the blockage, loss of packets or any node disappointment. Precisely when oddities are seen, the RPL nodes ought to trigger repair instruments.

"These structures contribute besides to the topology upkeep when node and affiliation disappointments happen. The nearby repair portion incorporates into finding a decision way to deal with course the packets when the favored parent is not accessible. The node picks another parent in its parent list. It is additionally conceivable to course packets by strategies for a family node e.g. node with a near rank. This decision way may not be the most overhauled one. The range repair instrument is attainable and empowers the system to join again inside a sensible time. Precisely when the near to repair systems flop accordingly of different irregularities, the DODAG root can start a general repair by growing the variety number of the DODAG outline. The RPL system is then totally changed which impacts every one of the nodes of the topology. The RPL custom encourages instruments to evade circles, see irregularities and repair DODAGs. Number to-constancy considers happen when a parent makes its rank view and picks its tyke as another parent and the tyke do moreover since it can't re-join to another node et cetera. By then, the rank estimation of both parent and tyke does not stop to increment. To keep this, the RPL custom constrains the most over the top rank respect permitted inside the chart. DODAG floats show up when a node does not regard the rank property which construes that the DODAG is no longer non-cyclic. To keep this, a leaving node must hazardous substance its sub-DODAG by propelling an unending rank. The leaving node has in like way the likelihood to utilize a segregating fragment, which includes in surrounding a go-among DODAG and rejoining the fundamental DODAG later. The RPL convention can in like way see oddities utilizing information way support system."

4.3 RPL (Routing Protocol for Low-Power and Lossy Networks)

- IPv6 Based Protocol for IoT
- Primarily for 6LowPAN
- Dynamic creation of DODAG
- Unidirectional as well as Bi-Directional
- Multiple instances occurrence and maintanance
- Localized behavior for higher optimization

Following is the scenario of DODAG in which the versions and ranks are maintained in IoT LowPAN environment.

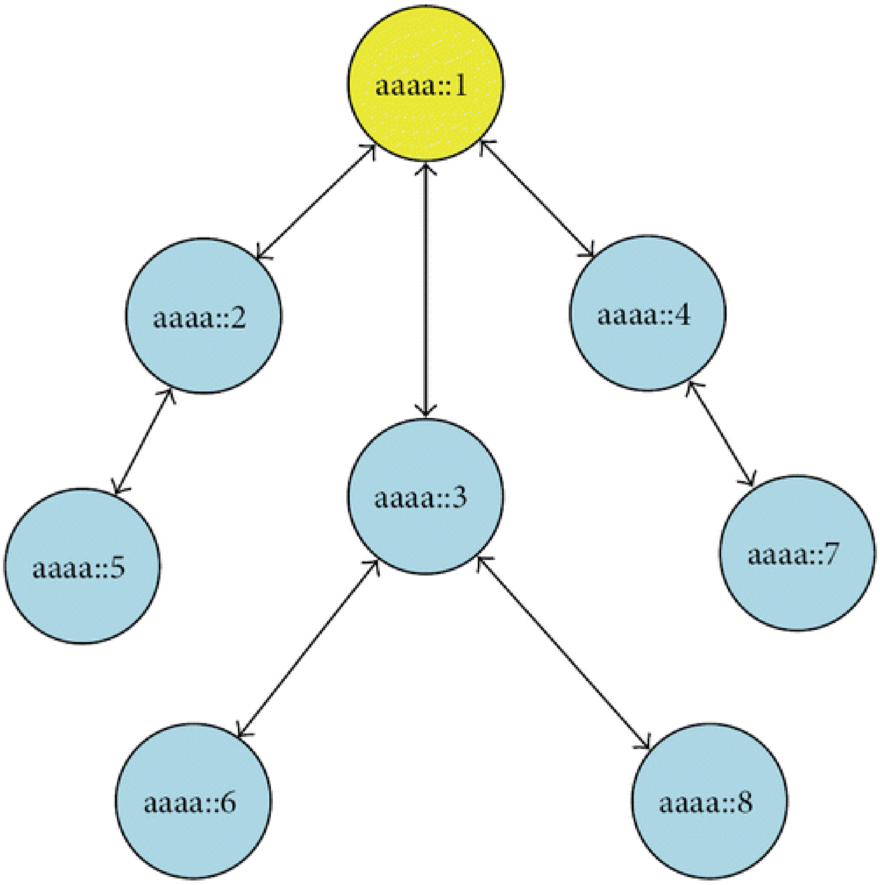


Figure 4.1: RPL DODAG where each node has a unique IPv6 address [52]

RPL enables each node in the framework to pick if packets are to be sent upwards to their family or downwards to their adolescents. "Routinely, concerning the condition in ContikiRPL that we use to show strikes in this paper, the base troublesome way a node can pick the acquaintance of a packet is with know each one of its relatives which picks the course towards leaf nodes and consider up heading as the default course of a packet. In RPL securing mode, in-structure controlling tables are used to separate packets heading upwards and the packets heading downwards in the framework.

4.4 Self-Healing in RPL

RPL has worldwide and interfacing repair parts that can come enthusiastically if there is a controlling topology bewilderment, an association baffled longing, or a node dissatisfaction. On a node (parent) or an affiliation dissatisfaction a zone repair instrument tries to pick another parent or way. In case there are all the more close frustrated desires, RPL plays out a fundamental general repair where the whole DODAG is imitated. The RPL custom uses the conspiracy layer metric as a parameter in the check of a default course. The way is thought to be wonderful if interface layer attestations are gotten on it.

RPL in like way uses a stream check to direct peculiarities in the RPL DODAG. Right when a RPL framework is solid, the stream clock break is wide. In any, unending supply of irregularities, the stream clock is reset, and more DIO messages are sent (by the nodes) in the degree of nodes that are subjected to groupings from the standard. The running with events are considered as varieties from the standard in the RPL When arranging circles are seen, When a node joins a DODAG and When a node moves inside a structure and changes rank.

4.5 Attacks against RPL

Extended Rank Attacks - The extended rank strike contains in purposely building up the rank estimation of a RPL node with a particular exceptional focus to pass on buoys in the network. Loops are shaped when its new kept up parent was in its before sub-DODAG and just if the aggressor does not use drift keeping up a key separation from structures.

Gathering Number Attacks - The gathering number is a key field of each DIO message. It is augmented unaltered down the DODAG outline and is reached out by the root only, each time a repairing of the DODAG is enter which is in like way called general repair. A more dealt with deference exhibits that the node has not moved to the new DODAG plot and can't be used as a parent node. An attacker can change the game plan number by misguidedly growing this field of DIO messages when it pushes them to its neighbors. Such a strike causes a silly changing of the whole DODAG compose. This strike can make many circles and as a results loss of information packets. In like way the section insignificant changing's of the chart increment generally control message overhead draining node resources and hindering the structure.” There is a security framework called VeRa (staying for Version Number and Rank Authentication) that keeps oversaw nodes from duplicating the root and from sending a senseless extended Version Number.

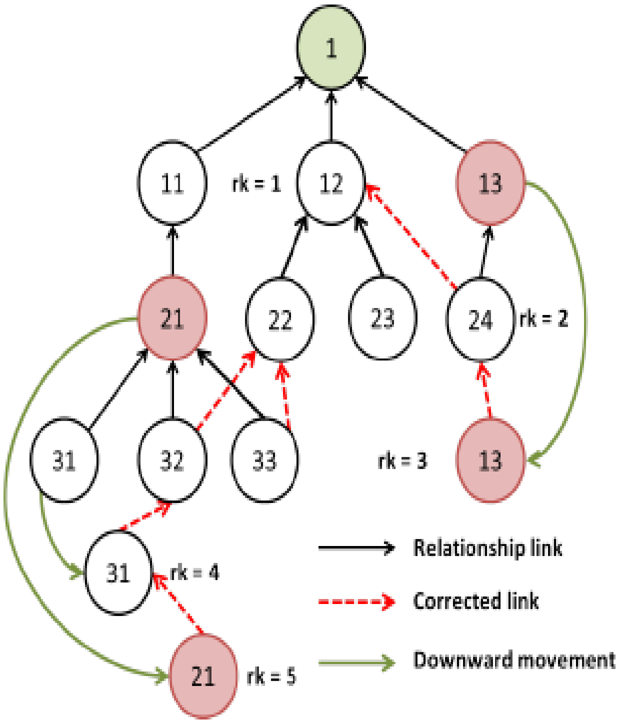


Figure 4.2: Rank increased attack in a RPL network [53]

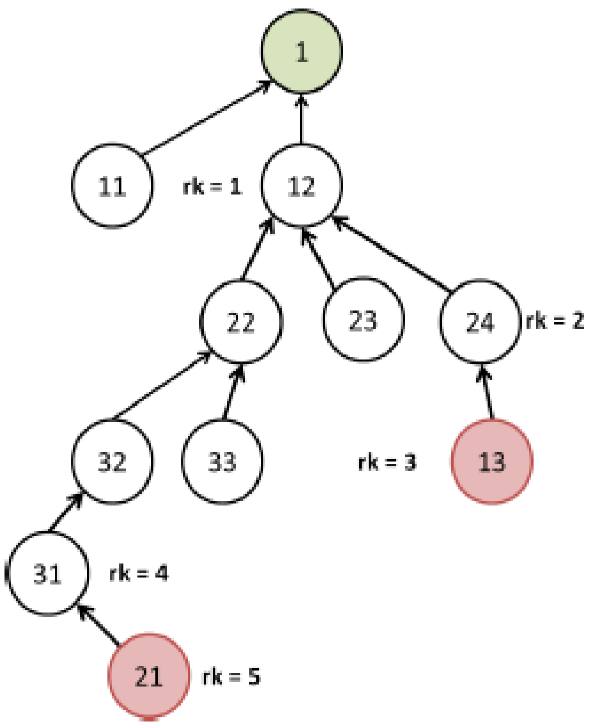


Figure 4.3: Rank increased attack in a RPL network [53]

4.6 Analysis of Existing Solution

There are two main attacks against RPL

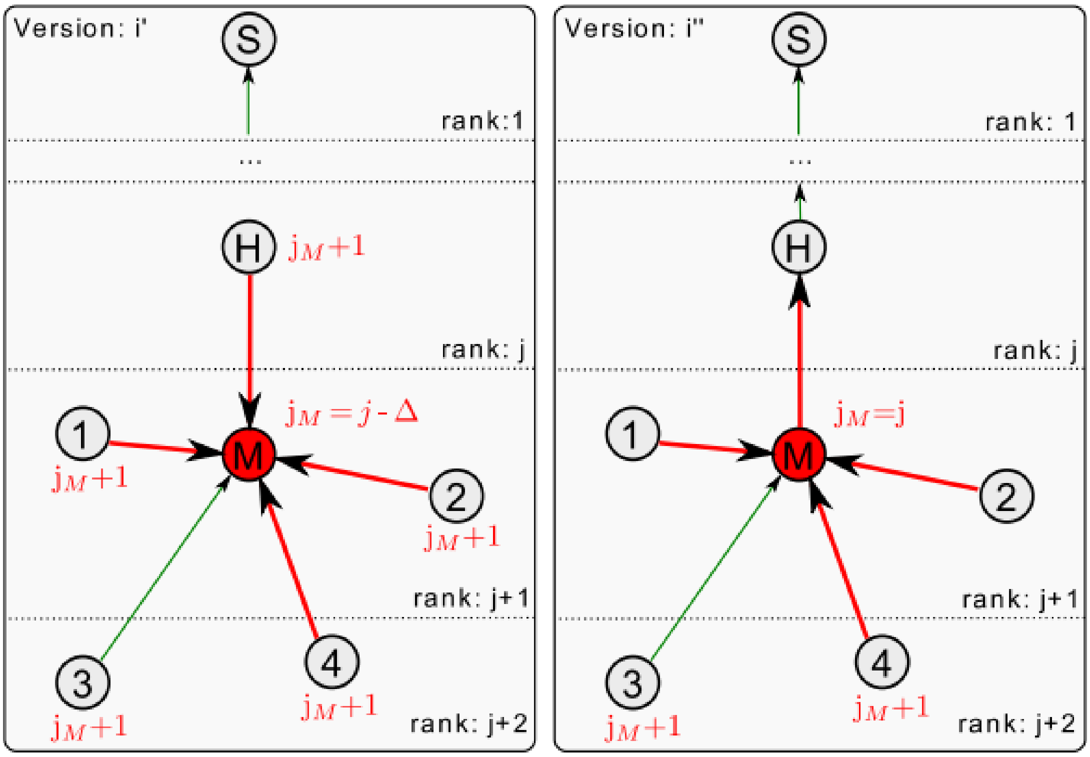
- Dynamic topology based authentication

- Maintaining and logging the original sender and receiver
- Dynamic hash key for higher degree of security and integrity
- Dynamic identification of malicious key and nodes so that further assaults can be avoided.

VeRA (Version Number and Rank Authentication) The Version Number and Rank Authentication (VeRA) security scheme proposed for RPL prevents: 1) Misbehaving nodes from impersonating a DODAG root and sending a DIO message with an illegitimate increased Version Number. 2) Misbehaving nodes from publishing an illegitimate decreased rank. It also prevents Version Number and Rank using one-way hash chain with a fixed length.

The building blocks of this scheme are-

1) Hash - MD5, SHA and others
2) MAC - Keyed-Hashing for Message Authentication (HMAC).
3) Digital Signature - ECC, RSA, DSA.



(a) Topology after a rank spoofing (b) Topology after a replay attack

Figure 4.4: Rank Spoofing and Replay Attacks [54]

The node M disseminates the rank jM falsely decreased by Δ, and thereby incorrectly attracts nodes 1, 2, 4, and the parent node H, which creates a sinkhole. (b) Visualizes a replay of the parent rank, only attracting nodes 1, 2, and 4 with intact upstream to H.

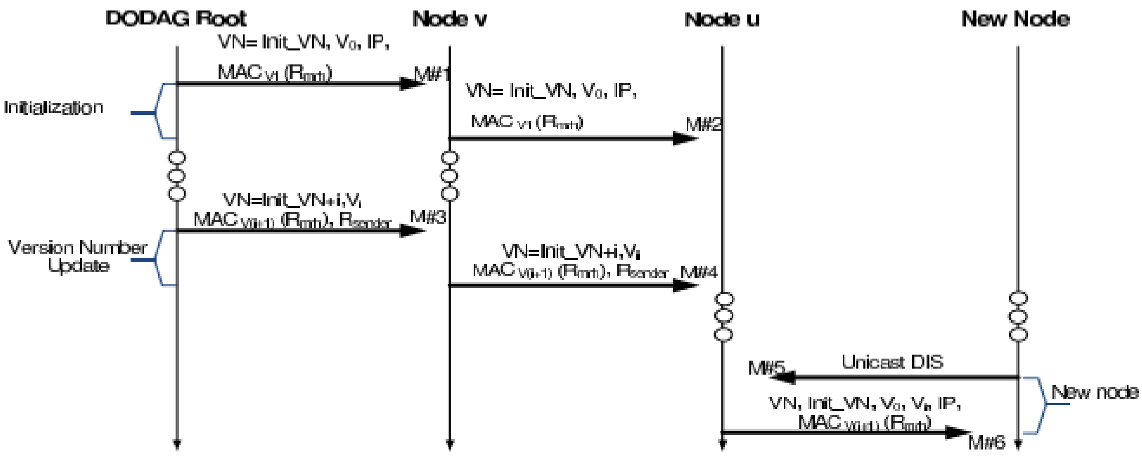


Figure 4.5: Sequence Diagram of the Security Scheme [54]

Table 4.1: Notations integrated with VeRA [54]

SYMBOL	DEFINITION
i	Index for Version Hash Chain $(0, \ldots, n)$
j	Index for Rank Hash Chain $(0, \ldots, l)$
l	Last Index of Rank Hash Element $(= 2^{16} - 1)$
n	Last Index of Version Hash Element
V_i	i-th Element of Version Hash Chain
$R_{i,j}$	j-th Element of Rank Hash Chain for i-th Version
r	Random Seed for Version Hash Chain
x_i	Random Seed for Rank Hash Chain at Version i
VN_i	Numeric Version Number at Version i
c_i	i-th Element of Encryption Chain

4.7 Cryptographic and Secured Encryption Based Perspectives in Assorted Scenarios

Security objectives can be implemented by applying cryptographic tools such as encryption or message authentication schemes. This section gives an overview of the cryptographic tools that are used in the work.

One-Way Hash Functions

A one-way hash function maps a (large) input set of elements with variable length into a (small) co-domain of elements with fixed length. The one way property allows to efficiently computing the hash value of an element, while the reverse calculation from a hash value to the original element is computationally hard. Hash functions play an important role in cryptography like for authentication schemes and integrity checks. Hash functions can also be applied recursively to their output to create a hash chain. A random number x is used as seed for a hash function h(_). The output of h(x) is hashed again, so that the second output is denoted by h(h(x)) or h2(x). If this is done i-times, the end of the hash chain results in hi(x). If any element of the chain is known, it is possible to compute any further element up to the end of the chain by performing the required number of hash operations. However, it is infeasible to create any prior element due to the one-way property of the hash function. Such a hash chain is useful to prove the ownership of secret information without revealing the secret. An example application for password authentication is given by Lamport : A client and a server communicate over an insecure channel. The client creates a hash chain using its password as seed hi(password) and securely provides the server with the end of the hash chain. Each time the client wishes to authenticate itself to the server, it sends the i - 1th hash chain element to the server.

The server hashes the element one more time and checks if h(hi1(password)) = hi(password). If both hash chain elements match, the server accepts the authentication. Next time the client sends an authentication, it sends the i - 2nd element, so that the server performs two more hash operations and so on. An adversary that replays a recorded hash element is detected since the element has already been used.

Message Authentication Codes

Hash functions are also applied within other cryptographic constructs such as the creation of a message authentication code (MAC). A MAC is used to authenticate the originator of a message and to check its integrity. MACs are based on a shared secret key and are thus created by symmetric protocols. The sender uses the secret key to create a MAC of a message and transmits both messages and MAC to the receiver. The receiver also creates the MAC of the message and compares its own computation to the MAC it received. If both match, the receiver has verified that the message has been created by a key holder and that it has not been modified. The CBC-MAC (cipher block chaining MAC) [13] and HMAC (keyed-hash MAC) [14] are examples to create such MACs. HMAC appends a shared secret to the message and hashes the concatenation with a cryptographic hash function. Hence, only a secret holder creates a valid MAC. The message is split into n blocks of equal size. An initial block contains control Wags, a nonce and the length of the message to support variable size messages. This block is encrypted by a block cipher, like AES, applying a secret key. The resulting cipher is XORed with the second block which denotes the first block of the actual message. The XOR conjunction is encrypted and then XORed with the next block, and so on. The last block denotes the MAC which may be truncated to the desired length.

Symmetric Authenticated Encryption

The CBC-MAC is applied within the CCM mode of operation which denotes a symmetric authenticated encryption scheme and is further considered in this work. CCM stands for Counter with CBC-MAC which uses a block cipher both for encryption in counter mode and the creation of a CBC-MAC. The CBC-MAC provides authenticity and integrity, while the encryption ensures the confidentiality of the message content. For encryption the plaintext is divided into blocks of equal size. To each plaintext block a unique key stream is applied by creating the XOR conjunction. To create such distinct key streams, a CCM nonce consisting of a random part and a counter is encrypted using a secret key. For each plaintext the counter can simply be incremented to provide a unique key stream. Authentication is achieved by the creation of a CBC-MAC of the plaintext message using the same secret key. To protect against collision attacks, the MAC is encrypted together with the plaintext message. Furthermore, CCM provides additional authenticated data for the authentication of unencrypted information such as routing headers. For this purpose, an additional MAC of this unencrypted information is created but not encrypted. CCM requires each nonce to be used only once with a given encryption key, so that key streams are not reused . If used twice or more, an attacker simply reveals the XOR conjunction of two plain texts P1 and P2 by combining two cipher texts that were created with the same key stream Ki:

(Ki _ P1) _ (Ki _ P2) = (P1 _ P2)

He may be able to extract both P1 and P2 and thus receives the applied key stream:

(Ki _ P1) _ P1 = Ki = encKs(_i)

where Ki is the secret key stream, Ks is the secret key and _i is the applied nonce. Each further message using this nonce-key pair is easily decrypted.

Public-key cryptography:

In contrast to symmetric approaches in which each party holds the same key, a public-key scheme is based on asymmetric keys. Hereby, different keys for en-decryption are used rather than a single secret key . The receiver therefore creates a key pair. One key is private and kept secret by the owner. The other is made publicly available and thus called public key. The public key is used for encryption and the private key for decryption, so that anyone can encrypt a message, but only the holder of the private key is able to decrypt the message. The asymmetric scheme relevant for this work is RSA which can be used for encryption and for the creation of digital signatures for authentication. To create a digital signature using RSA, each sender signs its messages before transmission. Signing with RSA is done by computing the hash value of the entire message and signing it by encryption with the private key. Hence, the cipher denotes the signature which is appended to the message. A node that receives a signed message first verifies the signature. This is done by computing the hash value of the entire message and decrypting the signature using the public key of the sender thus revealing the hash value. If both hash values match, the message has not been altered but was created by the owner of the private key.

CHAPTER 5
METHODOLOGY

5.1 Tools and Technologies Used

- Ubuntu Linux Operating System
- VMWare Workstation
- Contiki Operating System
- Cooja IoT Network Simulator
- C Programming Language

5.2 Implementation Strategy

Algorithm

- *Initialization of IoT Scenario and a DODAG RootElement generates a random number r and calculates a hash chain, named as VeraVersionNumber hash chain, of size n + 1: V_n, V_{n-1}, V_1, V_0 where $V_n = h(r)$, $V_i = h(Vi+1)$, with the random number*
- *For each element Vi of the VeraVersionNumber hash chain the DODAG RootElement generates a new random number xi and calculates a new hash chain, named as MyRank hash chain, of size l + 11 : $R_{i,0}$, $R_{i,1}$, $R_{i,l-1}$, $R_{i,l}$ where Ri,0 = h(xi), $R_{i,j}$ = h(Ri,j−1), with the new random number*
- *Then the DODAG RootElement reveals the RootElement of the VeraVersionNumber hash chain V0, computes MACV1 (R_{mrh}) a message authentication code (MAC) value over the Max MyRank hash (mrh) value $R_{mrh} = R_{1,l}$ of the next element V_1 with the next VeraVersionNumber hash chain element (V_1) as the key*
- *Using a digital signature {V_0, MACV1 (Rmrh}sign the DODAG RootElement binds these values to a particular DODAG and DODAGID*
- *Finally, the DODAG RootElement multicasts a DIO message with V_0, MACV1 (R_{mrh}), the initial value Init of the VeraVersionNumber, and the signature (M#1; the DODAG RootElement can resend the signed DIO message until the first VeraVersionNumber update occurs*
- *Upon receiving the signed DIO message, each intermediate*
- *node verifies the authentication data and in case of success saves the signature, the RootElement V0 of the VeraVersionNumber hash chain, the MAC value, and the initial value InitV N of the VeraVersionNumber*

- *When the trickle timer expires, it multicasts to all neighbors the DIO message (M#2)*
- *Upon VeraVersionNumber update, the DODAG RootElement sends a DIO message (M#3) with the following parameters: next VeraVersionNumber value V N as described, next VeraVersionNumber hash chain element Vi , $MACV_{i+1}$ (R_{mrh}) a message authentication code (MAC) value over the Max MyRank hash value R_{mrh} = R_{i+1},l with the next VeraVersionNumber hash chain element Vi+1 as the key, and a MyRank element value Rsender = h $MyRank_{RootElement}$ (xi), where $MyRank_{RootElement}$ is the new MyRank value2 of the DODAG root*
- *Upon receiving a DIO message with a new VeraVersionNumber or new MyRank value, an intermediate node can easily verify the message because, if the VeraVersionNumber is increased by the DODAG root, h i (Vi) must be equal to V0*
- *Upon success, the intermediate node saves the current VeraVersionNumber value (only if the VeraVersionNumber increased)*
- *Moreover, using the revealed key Vi , the MAC value from the previous update MACVi (R_{mrh} = $R_{i,l}$), and the MyRank element R_{sender}, the intermediate node can verify whether the MyRank value of its parent is monotonically increasing as follows:*
- *It generates Rcheck = h l−MyRanksender (Rsender), where MyRanksender is the MyRank value of the parent*
    - *It checks if MACi = MACVi (Rmrh), from the previous update, is equal to MACcheck = MACVi (Rcheck)*
    - *If so, intermediate node v can conclude that the MyRank is monotonically increasing and: – It calculates its MyRank value regarding its Objective Function, MyRankv*
        - *It calculates δ = MyRankv − MyRanksender, the difference between the node MyRank value and its parent MyRank value*
- *Node v has the parent MyRank from the DIO message*
        - *It calculates R_{sender}= h δ (R_{sender})*
        - *When the trickle timer expires, it multicasts to all neighbors the DIO message (M#4) according to the new Rsender value*
- *If an attacker wants to increase the VeraVersionNumber (or decrease the MyRank), then it has to compute a pre-image of the last revealed hash chain element of the VeraVersionNumber chain (or compute a pre-image of the last R_{sender})*
- *However, computing the next element Vi+1 or previous R_{i-1} knowing V_i or R_i is hard when x, r is not known and h is a cryptographic one-way hash function*
- *In the case when a new node wants to join the DODAG, any DODAG node receiving a unicast DIS message (M#5) from the new node must reply with a DIO message (M#6) containing the*

current VeraVersionNumber value, the initial VeraVersionNumber value, the RootElement of the VeraVersionNumber hash chain (V0), the current VeraVersionNumber hash chain element (Vi), saved signature (IP), and the last MAC value.

How VeRA is affected when rank changes or udated?

Version Number and Rank Authentication (VeRA) is multiway approach towards the security and integrity in the Internet of Things (IoT). Assorted assaults are implemented with rank chain tampering aspects. In case of any update of rank, VeRA makes use of higher level of cryptography hash functions and credentials by which these values can be validated and the overall network communication can be made secure. The implementation of versioning control and ranking integrates higher security degree enabled cryptography hash approaches so that the verification from all the parent nodes can be done. VeRA keeps track of the publishing in association with the DODAG tree by which the parent nodes and the authenticated communications can be verified for upcoming transmissions. The multilayered approach for version and rank authentication is one of the effectual mechanism by which the overall communication in assorted nodes can be authenticated at multiple layers. It is effectual and performance aware in case of low power and lossy networks which are traditionally used in wireless networks as well as IoT. The perspectives related to routing are taken care and associated with Routing Protocol for Low power and Lossy Networks (RPL) but the integrity and secured communication in the nodes is controlled by VeRA. Using the approach to maintain each and every layer of nodes during transmission and conversation between the motes, the rank allocation and escalation of security can be done.

CONTIKI-COOJA

Contiki (http://www.contiki-os.org) is one of the widely used operating system for IoT programming using different types of sensors and RFIDs. It is free and open source operating system under BSD license with the base code of programming language C. Contiki can be used for the communication between low powered RFID chips in wireless networks with higher degree of performance and security.

The programming on Contiki is done using Cooja Network Simulator in which the base libraries of RFID chips and sensors are available in C. To program, control and monitor the remote IoT devices, the back-end C programs and related header files can be customized and recompiled to get the desired results. Contiki works on IPv4 as well as IPv6 networking with the integration of lightweight protocols so that low power chips and radio frequency chips can be connected without performance issues.

URL for Downloading Instant Contiki :
http://sourceforge.net/projects/contiki/files/Instant%20Contiki/

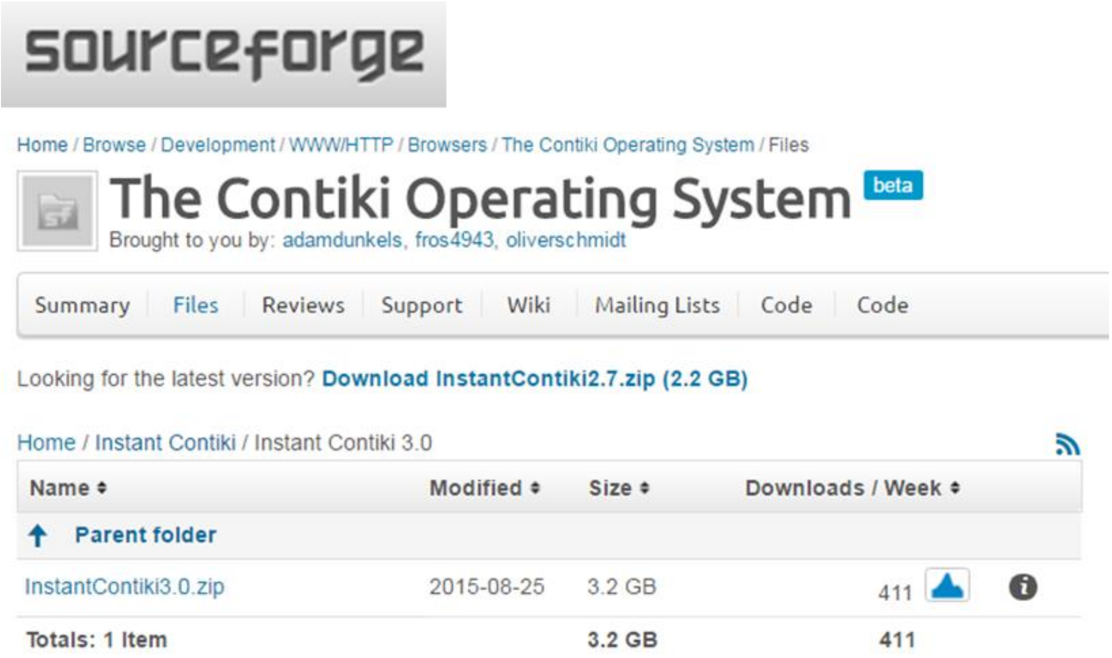


Figure 5.1: Contiki Operating System at SourceForge

Once the compressed Instant Contiki is downloaded, it can be used on any host operating system. The Instant Contiki is available on sourceforge.net as compressed file which is required to be extracted. The uncompressed or extracted Instant Contiki can be executed on VMWare Player which is a virtualization tool. The VMWare Player can be downloaded free and available on http://www.vmware.com/go/downloadplayer/.

In the extracted folder of Instant Contiki, there is an executable file Instant_Contiki_Ubuntu_12.04_32-bit.vmx.

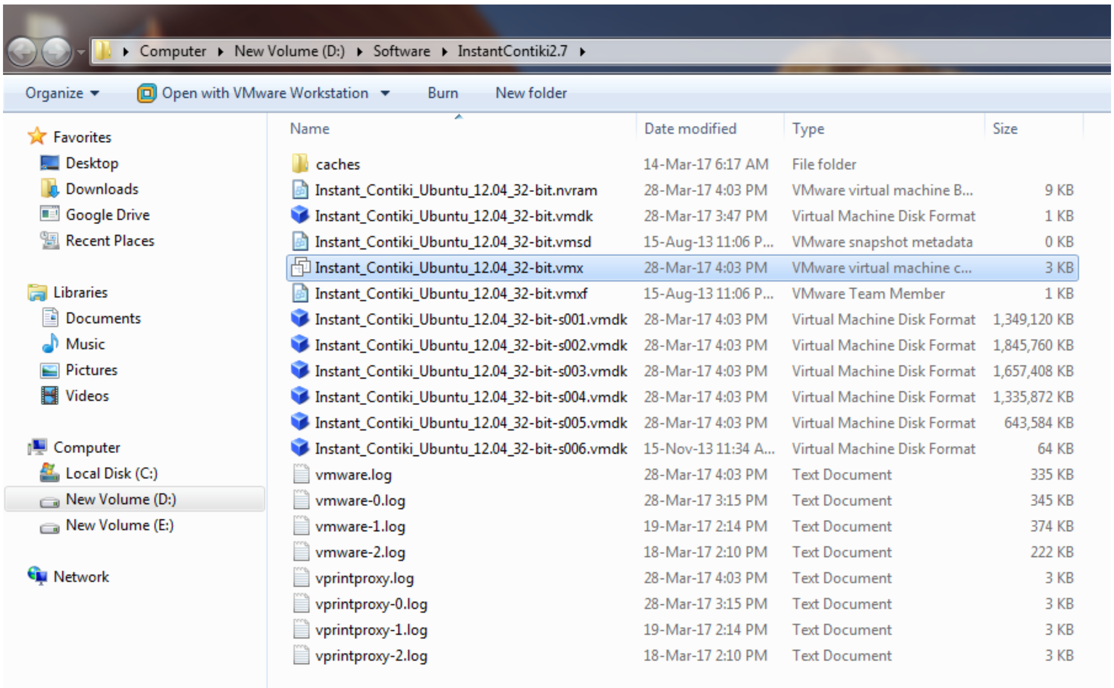


Figure 5.2: Contiki Directory Structure

This executable file on executing will automatically open in VMWare Player and we will be ready to work with Contiki in Virtualization Software in parallel with any host operating system. The default password for Contiki operating system is “user”.

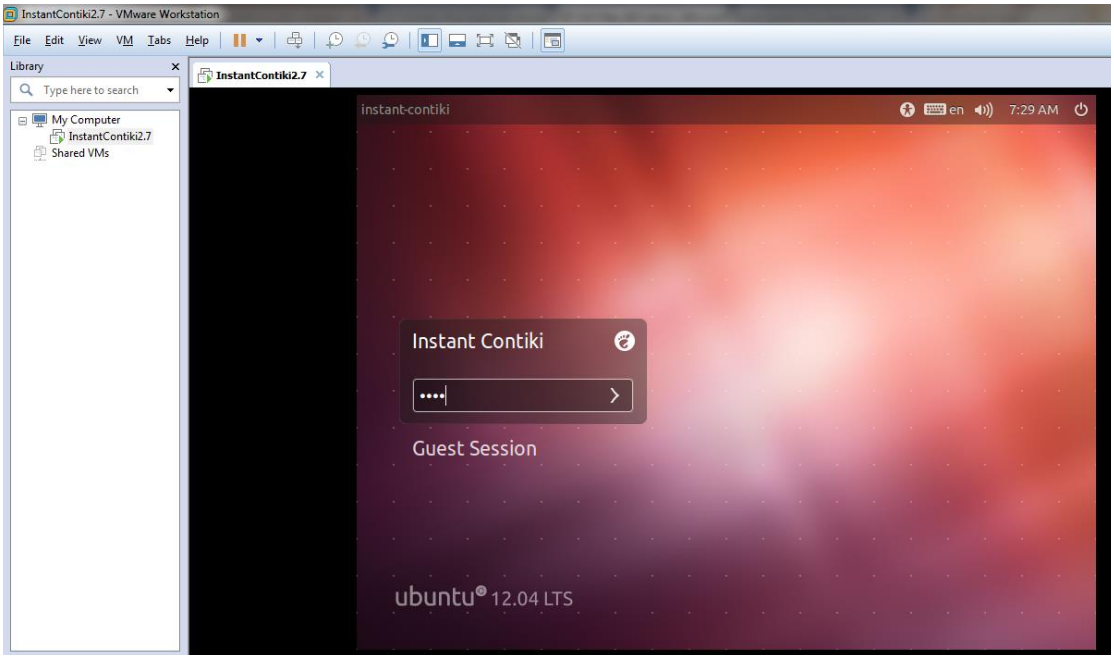


Figure 5.3: Login Panel of Contiki

After loading Contiki O.S., the following commands are executed in the Terminal of Contiki so that the Cooja Simulator gets loaded for implementation of IoT.

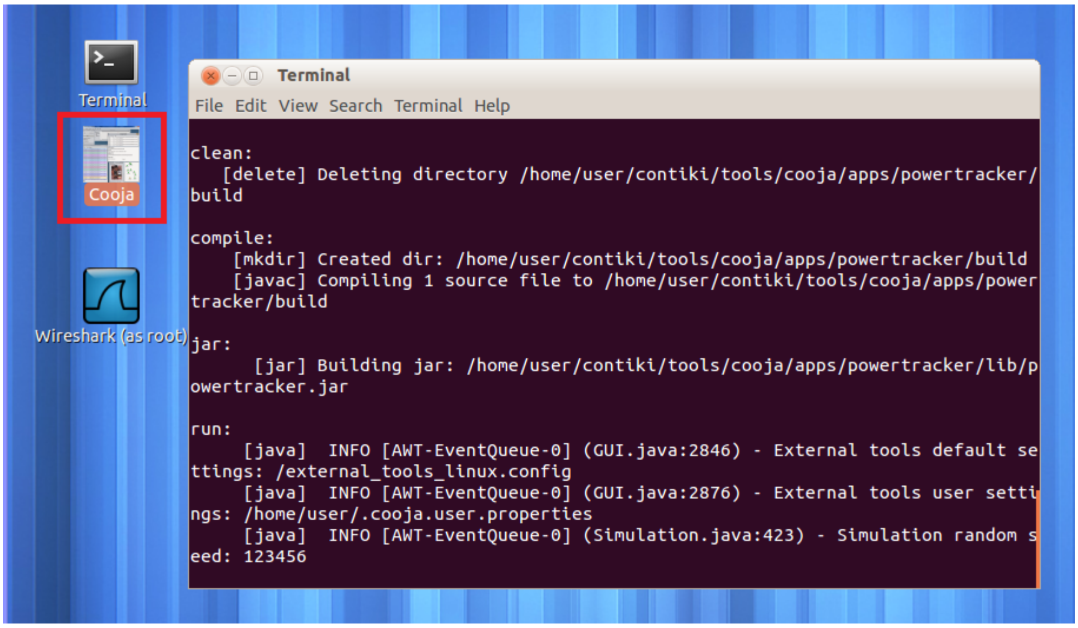


Figure 5.4: Loading Cooja Simulator in Contiki

5.3 Creating New Network in Cooja Simulator

In File Menu of Cooja, select New Simulation as follows

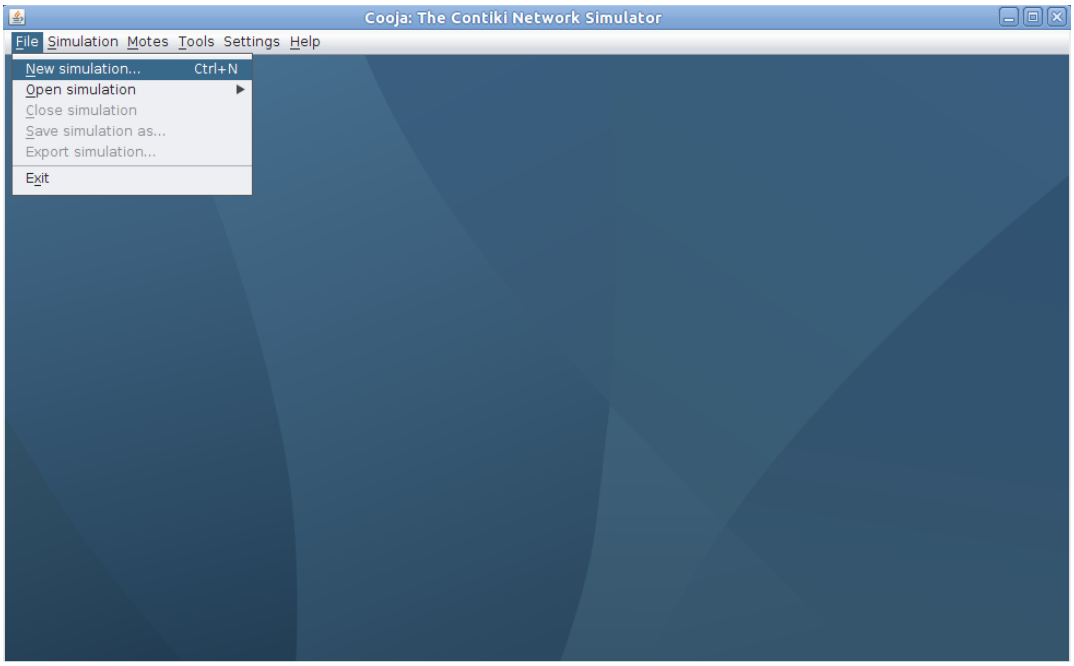


Figure 5.5: Creating New IoT Simulation in Cooja

In the dialog box, the basic network parameters are set which includes the Name of Simulation, Radio Medium, Startup Delay and Random Seed.

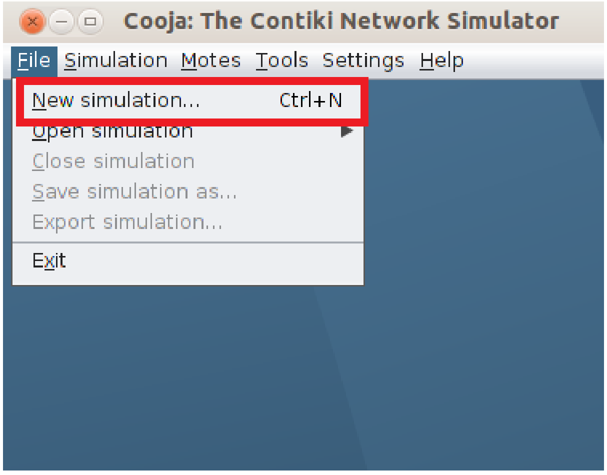


Figure 5.6: Enable Simulation Scenario in Cooja

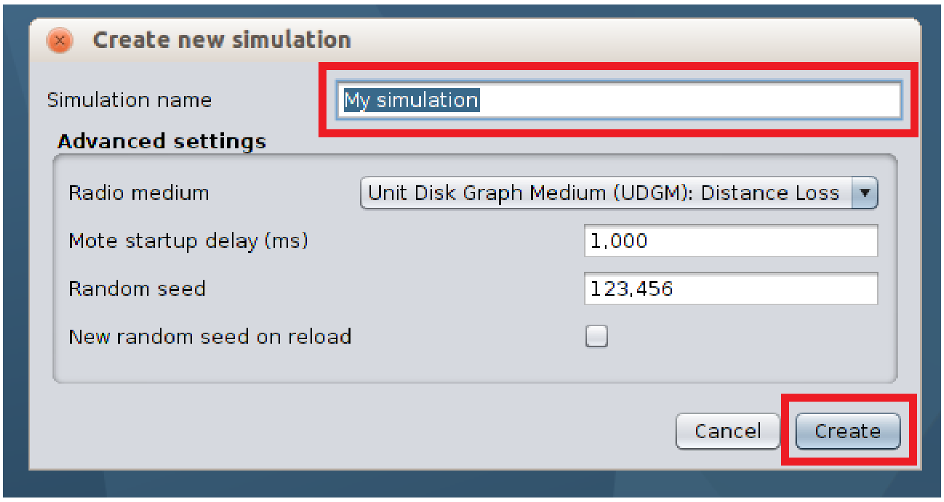


Figure 5.7: Creating New Simulation

Once the basic layout and working environment is prepared, there is need to import the RFID tags, sensor nodes or any other wireless devices which are required to be connected and communicating in IoT. In wireless networking and IoT, these are known as motes. There are many types of motes in Cooja which can be programmed.

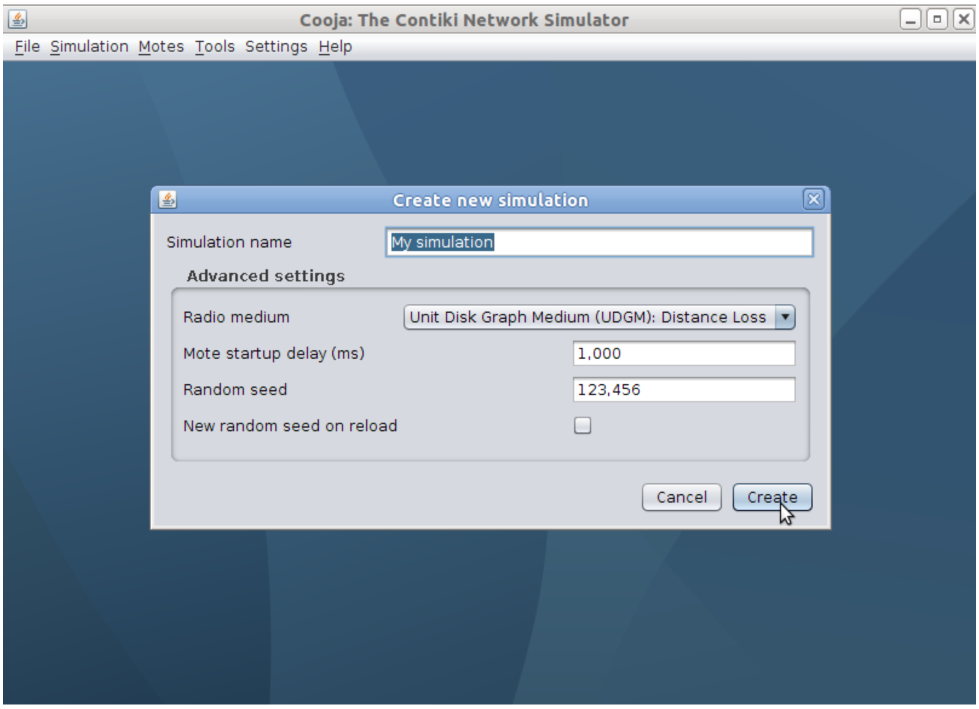


Figure 5.8: Setup of basic properties of simulation in Cooja

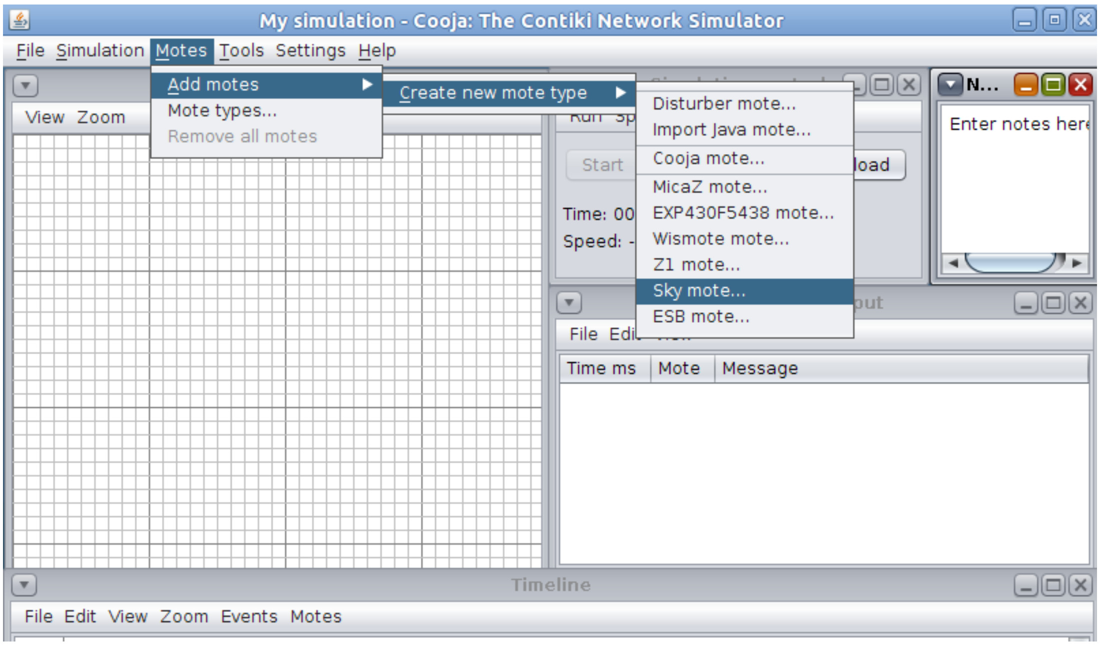


Figure 5.9: Invoking Wireless and RFID Motes in Cooja Simulator

Even physical motes can be connected using ports on the system so that real time interfacing can be done. Every mote with the base properties and programming APIs are specified in the source code of C at back-end of Cooja. These C source code files can be customized and recompiled to get the new or desired output from these motes.

CHAPTER 6

IMPLEMENTATION AND EXPERIMENT

6.1 Outcome and Performance Aspects

- Higher Degree of Security and Performance in IoT Network
- Dynamic Key Exchange improve the data communication with greater degree of security and overall efficiency
- The overall temperature and energy aspects in the IoT nodes are consistent
- The parameters related to overall performance and efficiency are optimized including power, temperature and packets loss.

6.2 Creating and Integrating IoT Modes

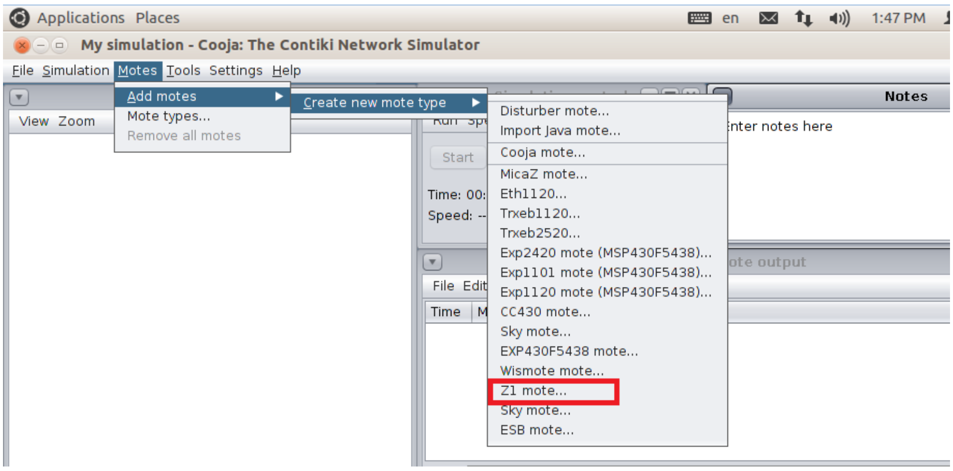


Figure 6.1: Adding Motes in Cooja

Figure 6.1 depicts the integration of any type of mote in the IoT Scenario. As in the figure there is Z1 mote, like this any other type of mote can be integrated. There are assorted motes in Cooja simulator which can be used for different applications and domains of IoT implementations.

6.3 Customizing the Back-End C Code and Recompiling

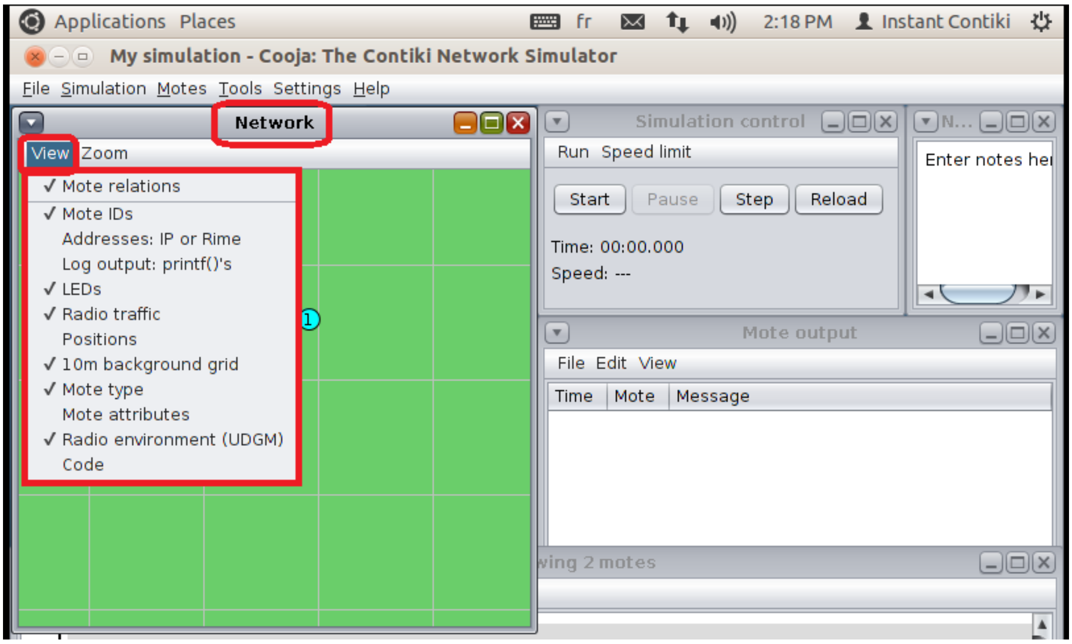


Figure 6.2: Setting Properties in Cooja

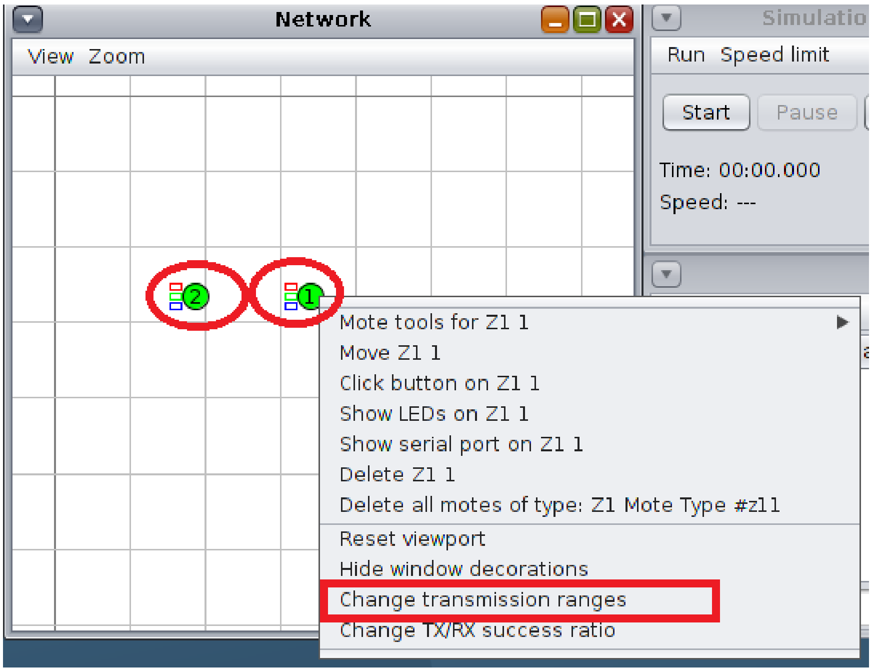


Figure 6.3: Setting Radio Properties

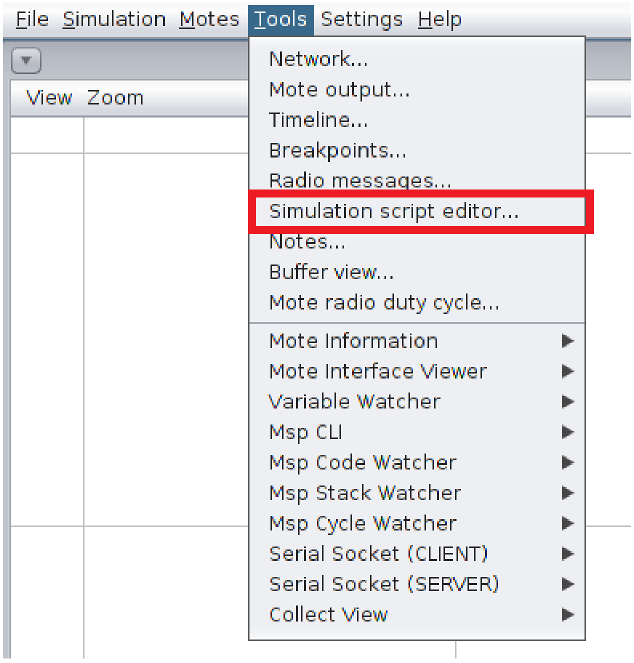


Figure 6.4: Simulation Script Editing

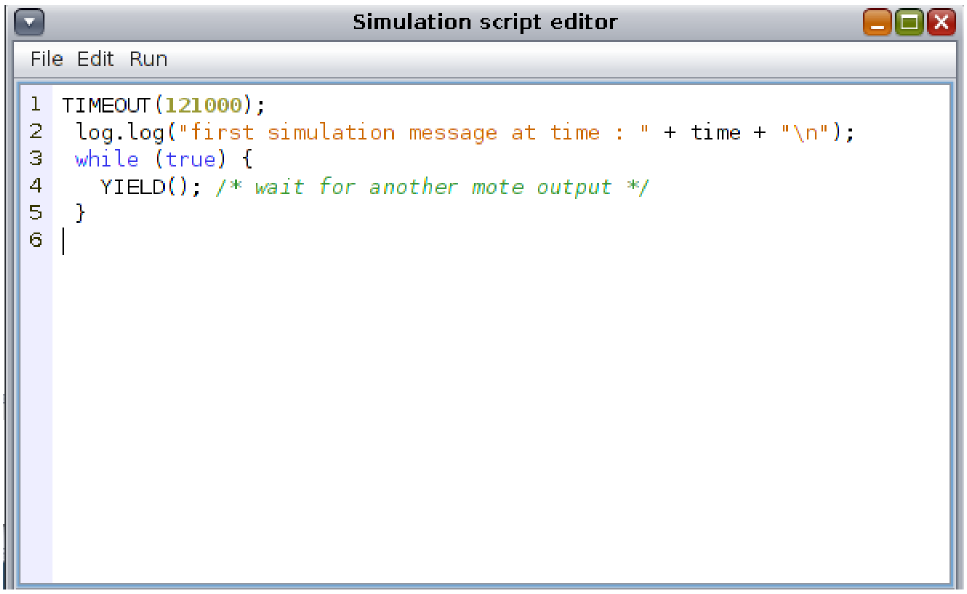


Figure 6.5: Editing Code in C

After compilation of C code, the number of virtual motes can be imported in the simulation area so that the transmission of radio signals can be viewed and analyzed.

6.4 Activation and Execution of Simulation in Cooja

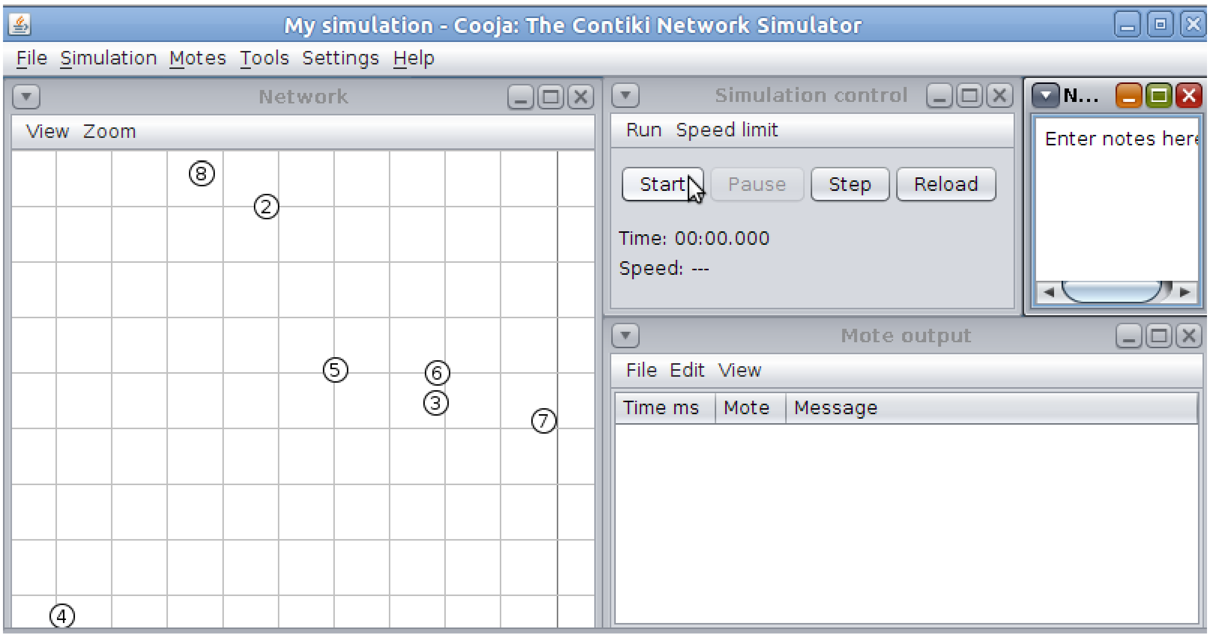


Figure 6.6: Viewing wireless motes with positions in Cooja

After Code customization, we recompile the code in CONTIKI-COOJA

You can see that the Dynamic Key is generated at each iteration

This key is generated using SECURED KEY that is implemented in existing code

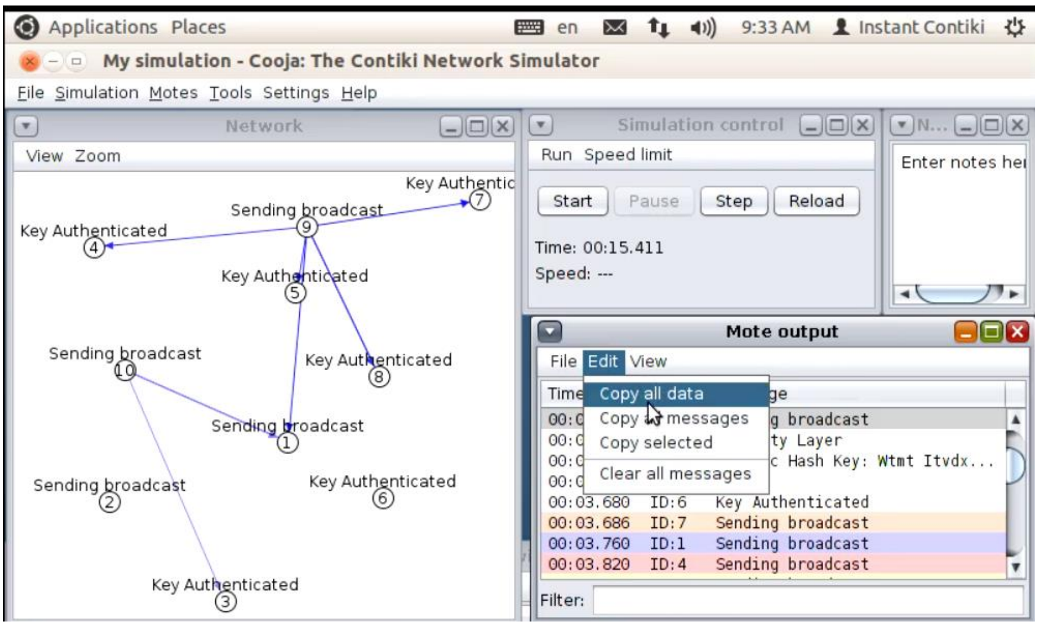


Figure 6.7: Running of Simulation and Behavior Analytics of Motes

As in the figure above, the network motes broadcast can be deeply investigated and the key authentication process which is the major aspect of implementation is presented.

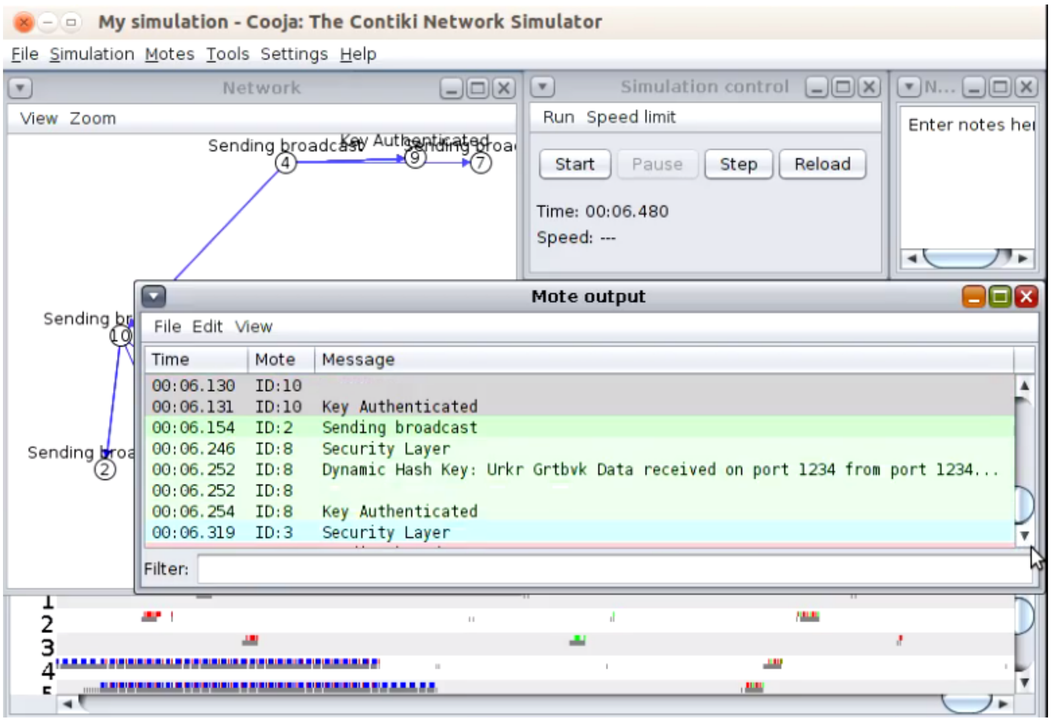


Figure 6.8: View of Dynamic Key Exchange

The figure depicts the mote output with the detailed analytics of dynamic hash key by which the overall environment is made secured.

6.5 Fetching Results and Logs for Analysis

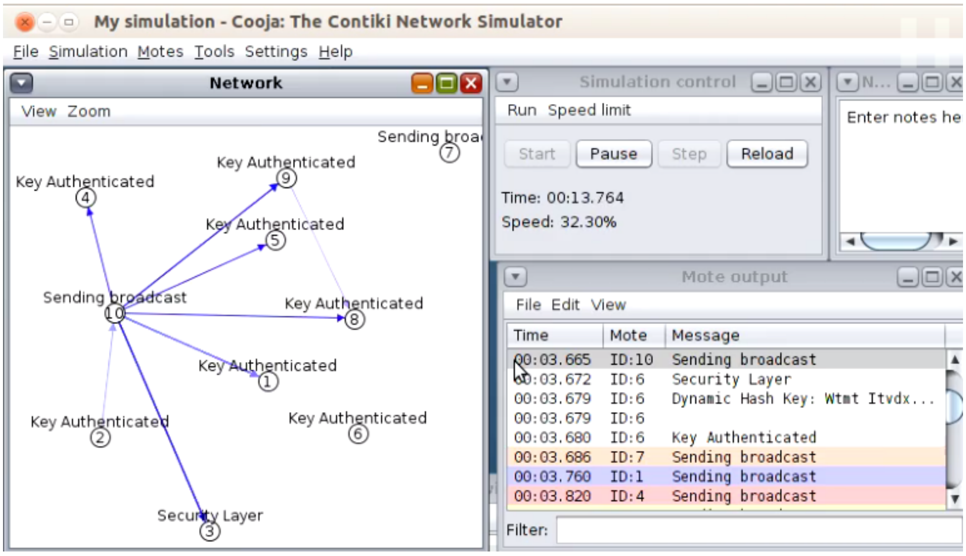


Figure 6.9: Key Authentication Process in Cooja Simulation

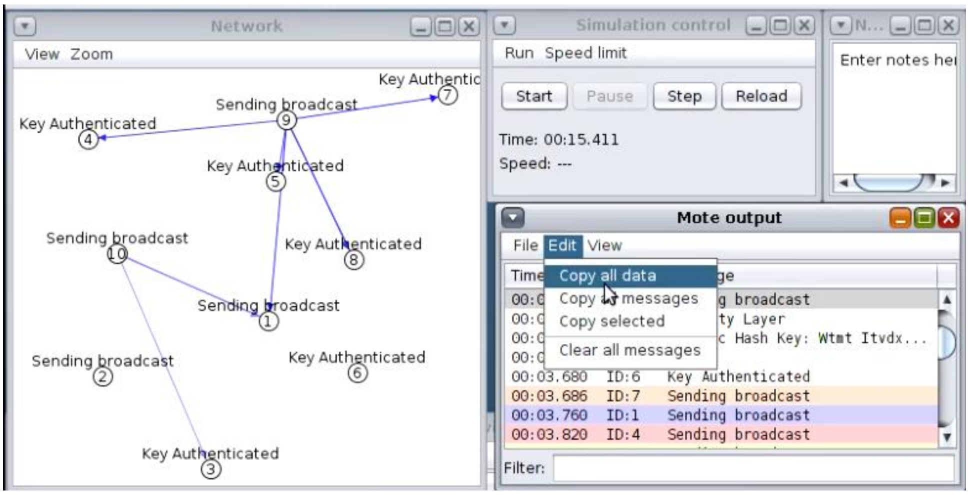


Figure 6.10: Fetching the data and messages for plotting graphs

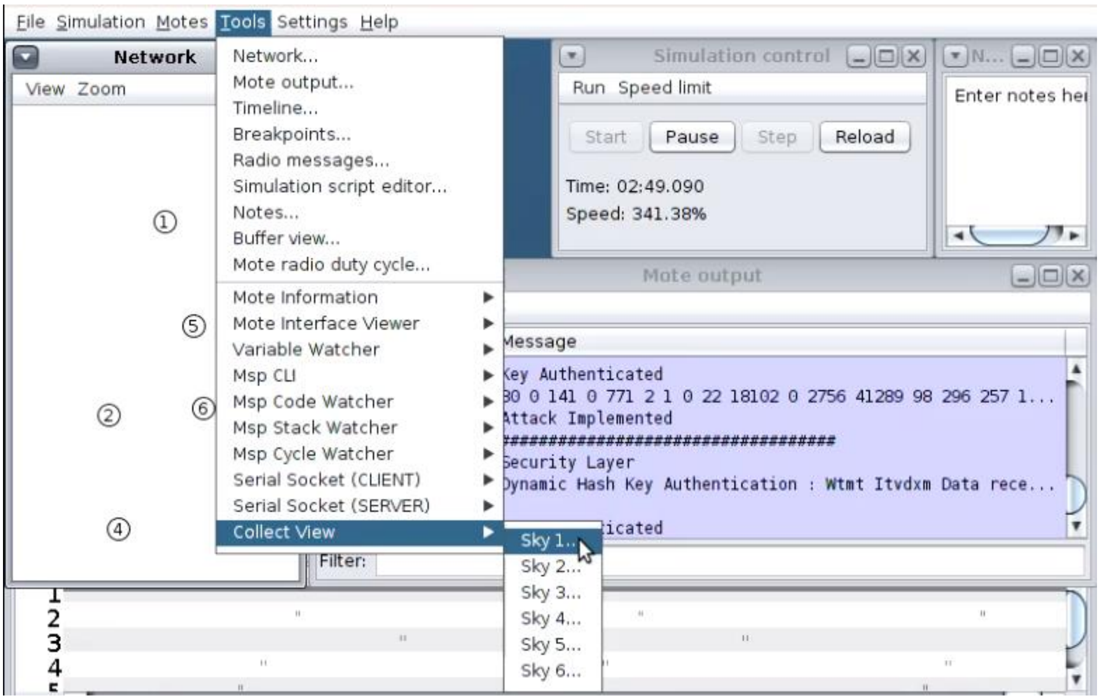


Figure 6.11: Collect View Activation for Detailed Logs

```
00:14.206       ID:9    Dynamic Hash Key: Gdwd Sdfnhw Data received on port 1234 from
port 1234 with length 4
00:14.206       ID:8
00:14.206       ID:2    Dynamic Hash Key: Yvov Kvxfzo Data received on port 1234 from
port 1234 with length 4
00:14.206       ID:10   Dynamic Hash Key: Zwpw Lwygap Data received on port 1234 from
port 1234 with length 4
00:14.206       ID:6    Dynamic Hash Key: Xunu Juweyn Data received on port 1234 from
port 1234 with length 4
00:14.206       ID:9
00:14.206       ID:2
00:14.206       ID:10
00:14.206       ID:6
00:14.207       ID:5    Key Authenticated
00:14.207       ID:8    Key Authenticated
00:14.207       ID:9    Key Authenticated
00:14.207       ID:10   Key Authenticated
00:14.207       ID:2    Key Authenticated
00:14.207       ID:6    Key Authenticated
00:14.210       ID:3    Security Layer
00:14.216       ID:3    Dynamic Hash Key: Wtmt Itvdxm Data received on port 1234 from
port 1234 with length 4
```

6.6 Collecting Sensor Data for Deep Evaluation

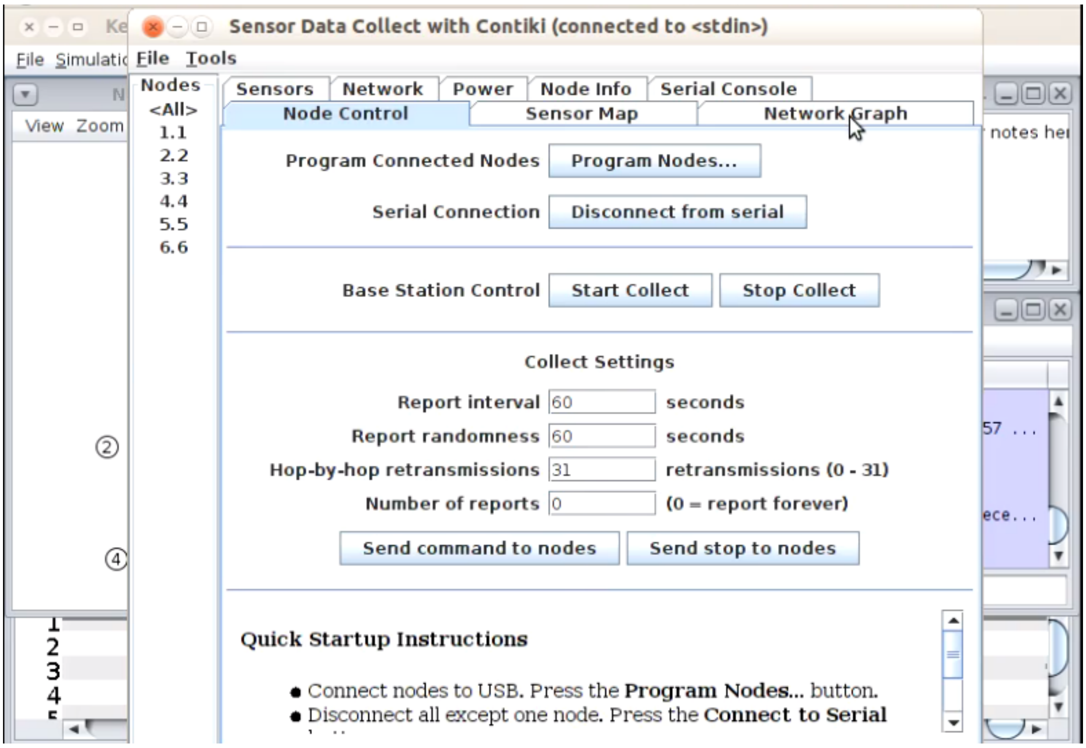


Figure 6.12: Network Graph Panel in Cooja

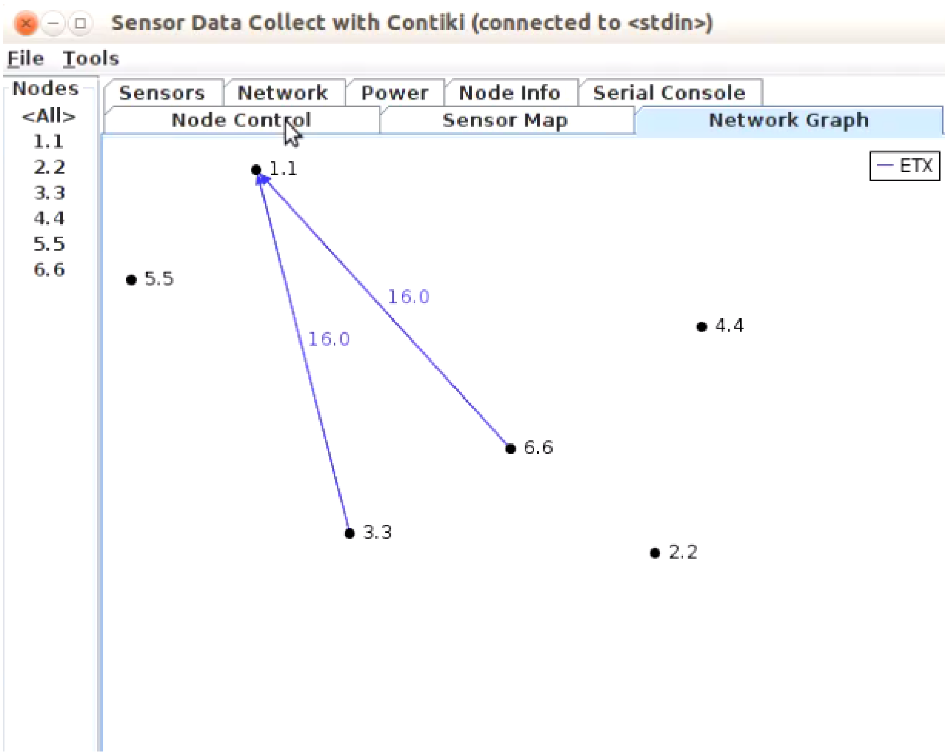


Figure 6.13: View of Network Graph for Dynamic Topology

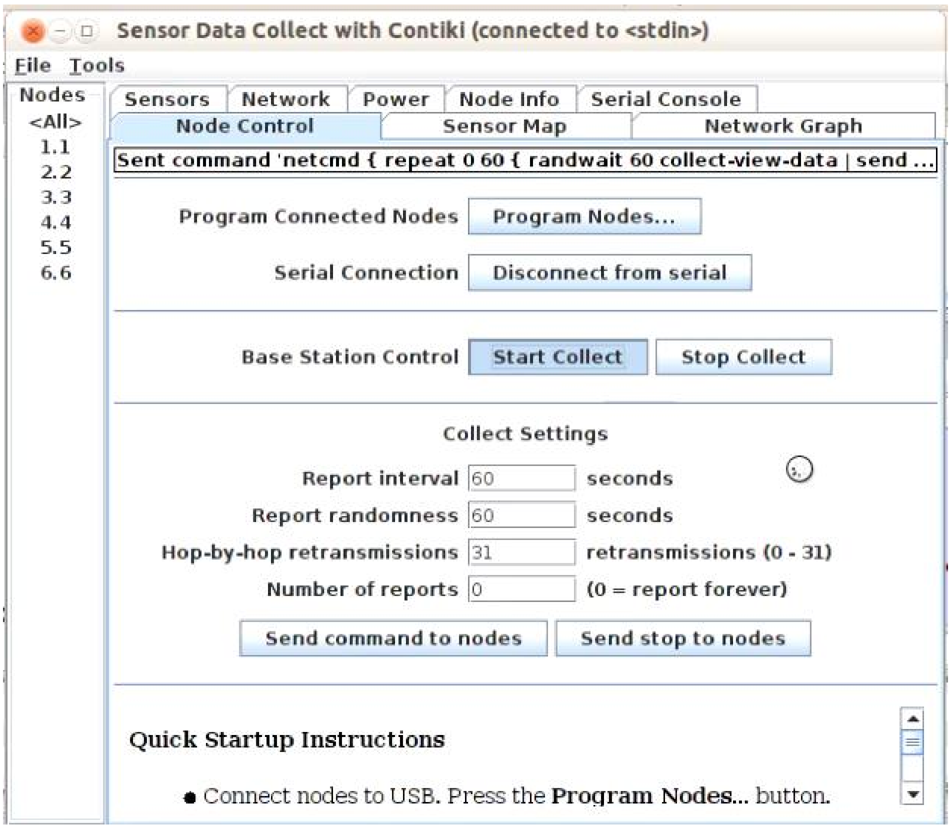


Figure 6.14: Node Control and Start Collect Mode in Cooja

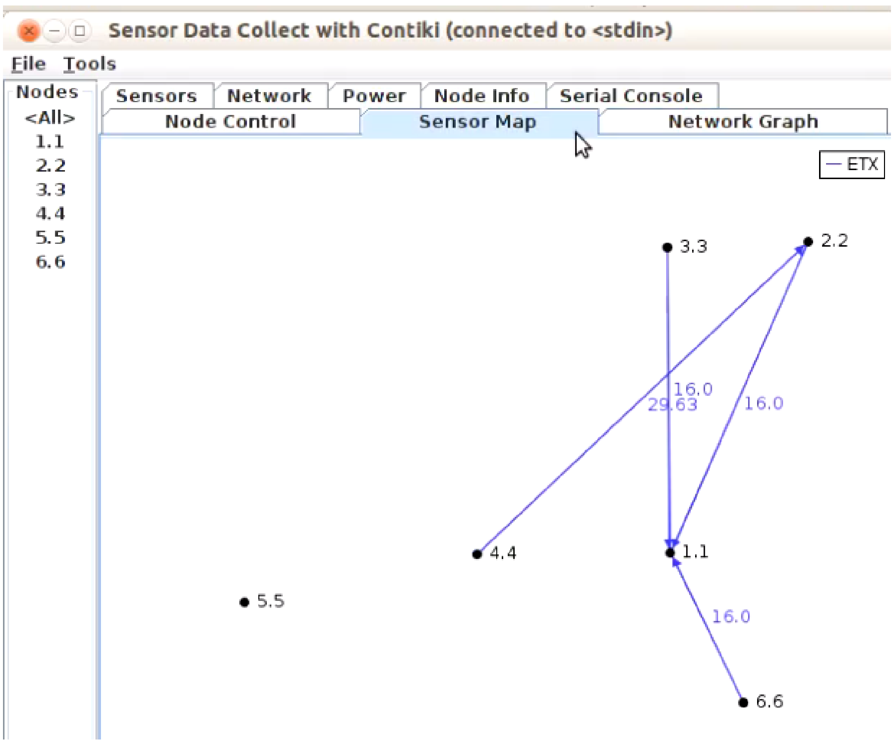


Figure 6.15: Sensor Map and Parameters Logging

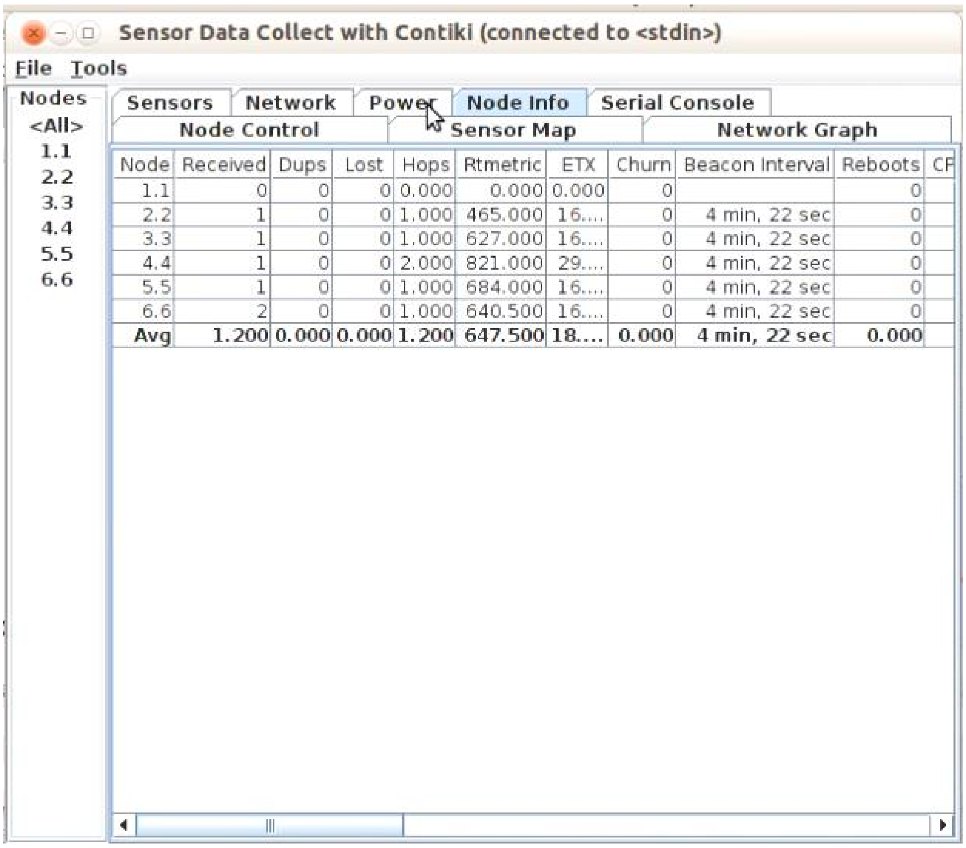


Figure 6.16: Node Information with Related Parameters

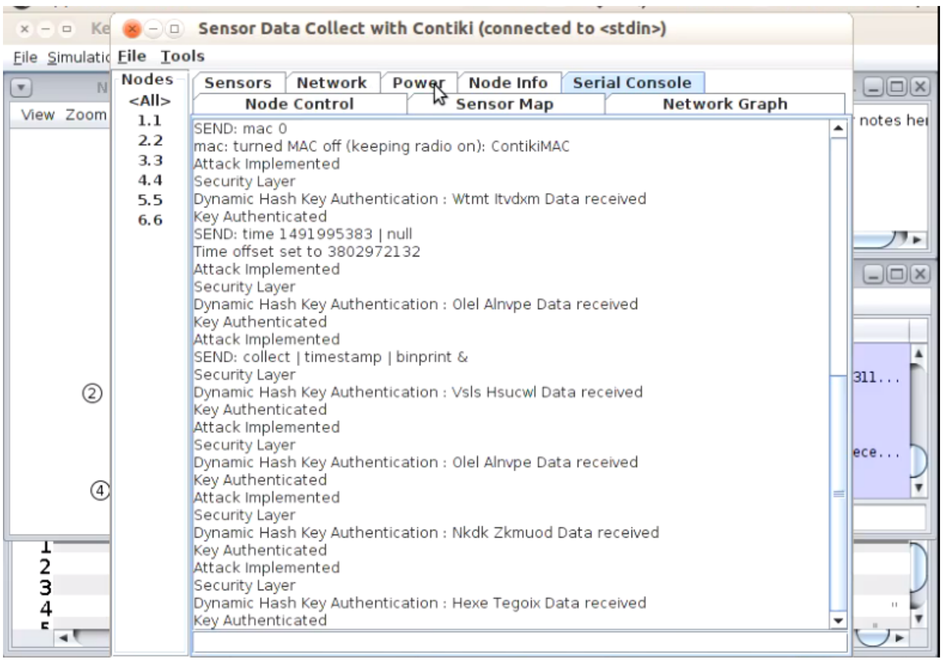


Figure 6.17: Serial Console to Validate the Results and Key Exchange

6.7 Plotting Results in form of Graphs

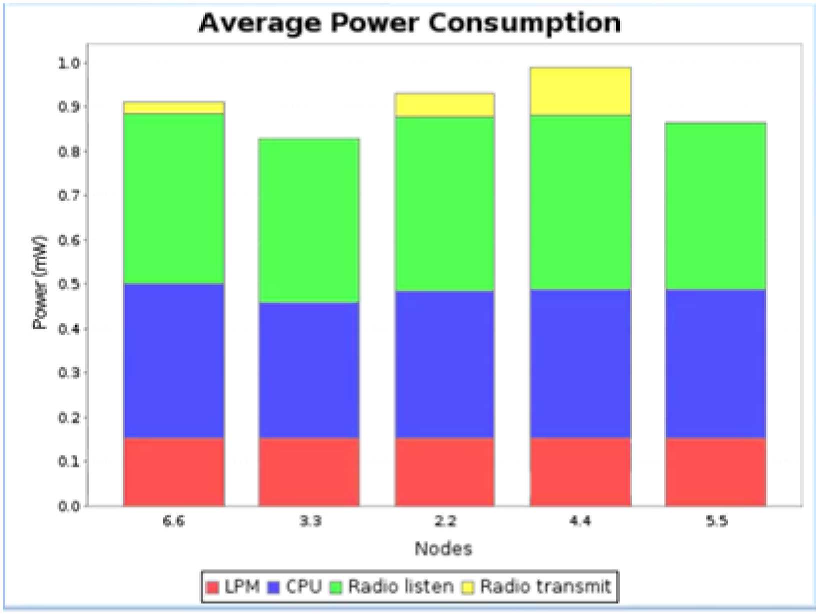
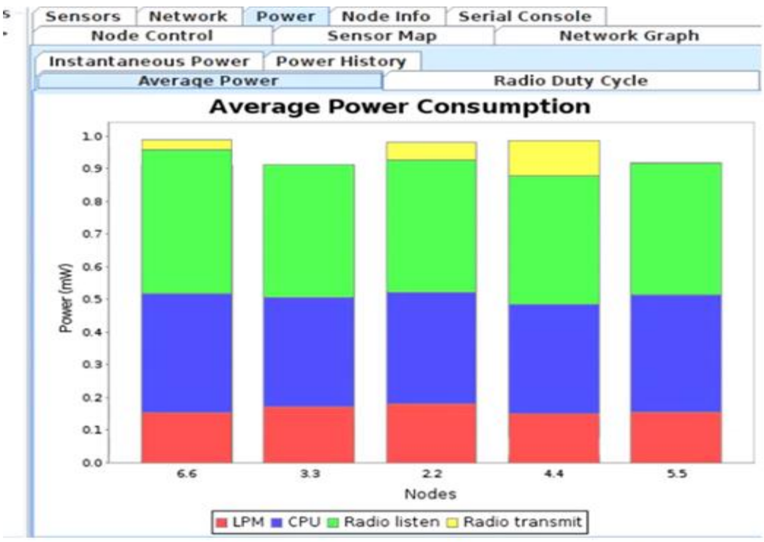


Figure 6.18: Average Power Consumption without VeRA

As depicted in the abovementioned figure, there are enormous parameters including LPM, CPU, Radio Listen and Radio Transmit during the IoT simulation. The graphical results in the above cited graph are consistent and low power mode is in the integrity mode. In addition, the radio listen the having the consistency.



Average Power Consumption in the Motes without VeRA

Figure 6.19: Power consumption with VeRA

CHAPTER 7

CONCLUSION

This is the chapter that is having the conclusion and future work of the research work done. In this chapter, the final conclusion about the research work and proposed work is explained. In the future work, the research work enhancement perspectives are explained. “Conclusion and future work” summarizes the outcomes of the research work and outlines possible direction for future research. In this work, there is the mechanism to avoid and detract the malicious node attacks, the effective location based identifier is integrated in the network that will generate a dynamic key. The generated hash key shall be matched in the source and destination channel and it will lead the transmission. Using this approach, the genuine packets shall not be lost. In case there packet loss, it is associated with the malicious node because in the algorithmic approach, the malicious node that is communicating with the data packet, then the data packet shall be dropped to avoid the security issues and improvement in the integrity. In the simulation scenario, the overall integrity and reliability of the network is improved using the proposed algorithm. The proposed algorithm can be integrated with Ant Colony Optimization that is one of the famous meta heuristic techniques for solving the combinatorial optimization problem. Using this technique, the dropped packet can be taken by the adjacent nodes (ants) then can it can be handed over to the destination.

7.1 Conclusion

As the wireless networks are vulnerable from different types of attacks, there is need to develop and implement a secured mechanism with highly integrated keys so that the interceptions cannot be done. In this research work, a unique and effective approach is implemented for avoidance of interceptions and integration of security during data transmission in network environment. The proposed approach is effective and giving better results than the classical greedy based approach with less secured keys. The proposed system can be implemented for any type of network and security can be integrated with dynamic keys.

With the integration of dynamic key exchange that is having higher level of integrity with multiple hash keys and final key as more security, there is enforcement of anti sniffing attempts and therefore the entire system is more secured and in integrity based mode.

7.2 Future Work

In this research work, the key focus is on the security, integrity and effectiveness of the wireless network. The current proposed and novel approach is effective in terms of higher degree of security with the implementation of hybrid key generation and transmission in the wireless scenario so that the intrusion cannot happen. To enhance the work with higher degree of security, the use of multiple cryptography approach at each phase can be done so that the security can enforced.

With the fast development of wireless networking in the world, the energy efficiency of wireless networking protocols becomes a concern of many wireless networking. So, the energy and power optimization can be integrated so that the wireless network can work effectively with minimum energy loss.

In another innovative approach, a password may be set which would help decide the algorithms to be used from an array of them and also the sequence of those algorithms to be used would be decided by the unique password. Clocked Hybrid Encryption Standard algorithm can be used in which the key and the data both are generated at same time which can prevent the information from side channel attack. Clocked Hybrid Encryption Algorithm will be more secure if the no. of rounds will increased. The no. of rounds can be increased and decreased according to the security purpose.

REFERENCES

[1] Chan H., & Perrig A. “Security and privacy in sensor networks, Computer Networks, 36(10), pp. 103-105, Oct. 2003.

[2] Huang Q., Cukier J., Kobayashi H., Liu B., & Zhang J., Fast authenticated key establishment protocols for self-organizing sensor networks, In Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications, pp. 141-150, ACM, Feb. 2003.

[3] Gura N., Patel A., Wander A., Eberle H., & Shantz S., Comparing elliptic curve cryptography and RSA on 8-bit CPUs, In International Workshop on Cryptographic Hardware and Embedded Systems, pp. 119-132, Springer Berlin Heidelberg, 2004.

[4] Watro R., Kong D., Cuti S. F., Gardiner C., Lynn C., & Kruus P., TinyPK: securing sensor networks with public key technology, In proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, pp. 59-64, ACM, 2004.

[5] Liao W.H., & Huang C. C., SF-MAC: A spatially fair MAC protocol for underwater acoustic sensor networks, IEEE Sensors Journal, 12(6), pp. 1686-1694, Jan. 2012.

[6] Rodríguez-Colina E., Multiple attribute dynamic spectrum decision making for cognitive radio networks, In 2011 Eighth International Conference on Wireless and Optical Communications Networks, pp. 1-5, IEEE July 2011.

[7] Ioannis K., Dimitriou T., & Freiling F. C., Towards intrusion detection in wireless sensor networks, In Proc. of the 13th European Wireless Conference, pp. 1-10, 2007.

[8] Sung W. T., Multi-sensors data fusion system for wireless sensors networks of factory monitoring via BPN technology, Expert Systems with Applications, 37(3), pp. 2124-2131, 2010.

[9] Monaco U., Cuomo F., Melodia T., Ricciato F., & Borghini M., Understanding optimal data gathering in the energy and latency domains of a wireless sensor network, Computer Networks, 50(18), pp. 3564-3584, 2006.

[10] Alcaraz C., Najera P., Lopez J., & Roman R., Wireless sensor networks and the internet of things: Do we need a complete integration?, In 1st International Workshop on the Security of the Internet of Things (SecIoT’10), (2010).

[11] Akyildiz I. F., & Stuntebeck E. P., Wireless underground sensor networks: Research challenges, Ad Hoc Networks, 4(6), pp. 669-686, 2006.

[12] Kulkarni S. S., & Arumugam M., Infuse: A TDMA based data dissemination protocol for sensor networks, International Journal of Distributed Sensor Networks, 2(1), pp. 55-78, 2006.

[13] Ergen S. C., & VaraiyaP., TDMA scheduling algorithms for wireless sensor networks, Wireless Networks, 16(4), pp. 985-997, 2010.

[14] Yu C., Cui Y., Zhang L., & Yang S., Zigbee wireless sensor network in environmental monitoring applications, In 2009 5th International Conference on Wireless Communications, Networking and Mobile Computing, pp. 1-5, IEEE, 2009.

[15] Fu H. L., Chen H. C., & Lin P., APS: Distributed air pollution sensing system on Wireless Sensor and Robot Networks, Computer Communications, 35(9), pp. 1141-1150, 2012.

[16] Zia T., and Zomaya A., A security framework for wireless sensor networks, In Proceedings of the IEEE Sensors Applications Symposium, pp. 49-53, 2006.

[17] Aydos M., Sunar B., and Koc C. K., An elliptic curve cryptography based authentication and key agreement protocol for wireless communication, In 2nd International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications Symposium on Information Theory, 2003.

[18] Biswas K., Muthukkumarasamy V. and Singh K., An Encryption Scheme Using Chaotic Map and Genetic Operations for Wireless Sensor Networks, Sensors Journal, IEEE, 15(5), pp. 2801-2809, 2015.

[19] Bussi K., Dey D., Kumar M. and Dass B.K., A Lightweight Hash Function, International Association for Cryptologic Research, 2016.

[20] Carl Endorf, Eugene Schultz and Jim Mellander, Intrusion Detection & Prevention, McGraw-Hill, 2004.

[21] Chen C.L., Chen C.C. and Li D.K., Mobile Device Based Dynamic Key Management Protocols for Wireless Sensor Networks, Journal of Sensors, 2015.

[22] Cochavy, Baruch, Method of efficiently sending packets onto a network by eliminating an interrupt, US Patent, 2004.

[23] Dimitris M. Kyriazanos, Neeli R. Prasad, Charalampos Z. Patrikakis, A Security, Privacy and Trust Architecture for Wireless Sensor Networks 50th International Symposium ELMAR-2008, Zadar, Croatia 2008.

[24] Donna Andert, Robin Wakefield, and Joel Weise, Professional Services Security practice, Sun Blue Prints OnLine, Trust Modeling for Security Architecture Development, 2002.

[25] Ghosal A., and Das Bit S., A lightweight security scheme for query processing in clustered wireless sensor networks, Computers &Electrical Engineering, 41, pp.240-255, 2015.

[26] Kiruthika B., Ezhilarasie R. and Umamakeswari A., Implementation of the Modified RC4 Algorithm for Wireless Networks, Indian Journal of Science and Technology, 8(S9), pp.198-206, 2015.

[27] He D. & Zeadally S., An Analysis of RFID Authentication Schemes for Internet of Things in Healthcarm Environment Using Elliptic Curve Cryptography, IEEE Internet Things J. 2, pp. 72–83, 2015.

[28] Mallikarjunaswamy N. J., Latha Yadav T. R., and Dr. Keshava Prasanna, Message Authentication Protocol for Lifetime Proficient Hash Based Algorithm in Wireless Sensor Networks, Int. J. Advanced Networking and Applications, vol. 07, pp. 2963-2966, 2016.

[29] Naveena A., and Dr. K. Ramalinga Reddy, A Review: Elliptical Curve Cryptography in Ad-hoc Networks, International Research Journal of Engineering and Technology (IRJET), vol. 03, June 2016.

[30] Thakur T., An Access Control Protocol for Wireless Sensor Network Using Double Trapdoor Chameleon Hash Function, Journal of sensors, 2016.

[31] Bandyopadhyay, D., & Sen, J. (2011). Internet of things: Applications and challenges in technology and standardization. Wireless Personal Communications, 58(1), 49-69.

[32] Pathre, A., Agrawal, C., & Jain, A. (2013, July). A novel defense scheme against DDOS attack in VANET. In Wireless and Optical Communications Networks (WOCN), 2013 Tenth International Conference on (pp. 1-5). IEEE.

[33] Ding, J., Cheung, S. Y., Tan, C. W., & Varaiya, P. (2004, October). Signal processing of sensor node data for vehicle detection. In Intelligent Transportation Systems, 2004. Proceedings. The 7th International IEEE Conference on (pp. 70-75). IEEE.

[34] He, W., Yan, G., & Da Xu, L. (2014). Developing vehicular data cloud services in the IoT environment. IEEE Transactions on Industrial Informatics, 10(2), 1587-1595.

[35] Lee, S., Tewolde, G., & Kwon, J. (2014, March). Design and implementation of vehicle tracking system using GPS/GSM/GPRS technology and smartphone application. In Internet of Things (WF-IoT), 2014 IEEE World Forum on (pp. 353-358). IEEE.

[36] Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012, August). Fog computing and its role in the internet of things. In Proceedings of the first edition of the MCC workshop on Mobile cloud computing (pp. 13-16). ACM.

[37] BBC www.bbc.com/news/world-asia-india-36496375

[38] NDTV sites.ndtv.com/roadsafety/important-feature-to-you-in-your-car-5/

[39] Biswas, K., Muthukkumarasamy, V. and Singh, K.. An Encryption Scheme Using Chaotic Map and Genetic Operations for Wireless Sensor Networks. Sensors Journal, IEEE, 15(5), pp.2801-2809.(2015)

[40] Bussi, K., Dey, D., Kumar, M. and Dass, B.K. Neeva: A Lightweight Hash Function.(2016)

[41] Carl Endorf, Eugene Schultz and Jim Mellander, Intrusion Detection & Prevention, McGraw-Hill, (2004)

[42] Chen, C.L., Chen, C.C. and Li, D.K.. Mobile Device Based Dynamic Key Management Protocols for Wireless Sensor Networks. Journal of Sensors. (2015).

[43] Cochavy, Baruch, Method of efficiently sending packets onto a network by eliminating an interrupt, US Patent (1998)

[44] Dimitris M. Kyriazanos, Neeli R. Prasad, Charalampos Z. Patrikakis, A Security, Privacy and Trust Architecture for Wireless Sensor Networks, 50th International Symposium ELMAR-2008, Zadar, Croatia (2008)

[45] Donna Andert, Robin Wakefield, and Joel Weise, Professional Services Security Practice, Sun BluePrintsOnLine,Trust Modeling for Security Architecture Development (2002)

[46] Ghosal, A. and Das Bit, S. A lightweight security scheme for query processing in clustered wireless sensor networks. Computers & Electrical Engineering, 41, pp.240-255. (2015)

[47] Kiruthika, B., Ezhilarasie, R. and Umamakeswari, A., Implementation of the Modified RC4 Algorithm for Wireless Networks. Indian Journal of Science and Technology, 8(S9), pp.198-206. (2015)

[48] He, D. & Zeadally, S. An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography. IEEE Internet Things J. 2, 72–83 (2015).

[49] I. Message Authentication Protocol for Lifetime Proficient Hash Based Algorithm in Wireless Sensor Networks. 2966, 2963–2966 (2016).

[50] Naveena, A. & Reddy, K. R. A Review : Elliptical Curve Cryptography in Wireless Ad-hoc Networks. 1786–1789 (2016).

[51] T. An Access Control Protocol for Wireless Sensor Network Using Double Trapdoor Chameleon Hash Function. 2016, (2016).

[52] Winter, T. (2012). RPL: IPv6 routing protocol for low-power and lossy networks.

[53] Gaddour, O., & Koubâa, A. (2012). RPL in a nutshell: A survey. Computer Networks, 56(14), 3163-3178.

[54] Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. Ad hoc networks, 1(2), 293-315.”