International Journal of Electronics, Communication & Instrumentation Engineering Research and Development (IJECIERD)
ISSN 2249-684X
Vol.3, Issue 1, Mar 2013, 237-248

DESIGN AND SIMULATION OF NETWORK USING NS2

SIRWAN A. MOHAMMED

MSc Student, Faculty of Electrical Engineering University of Babylon, University of Sulaimani, Iraq

ABSTRACT

The main goal of this paper is to present how to use network simulator(NS2)simulation for designingnetworks and using Cryptography algorithm as to security information. It briefly describes the basic networks categories, analyzes networks, brieflydescribes their components and technologies, explains the Wi-Fitechnologyand analyzesproperty sources related to networksimulatorand its detaileddescription, specify the configuration for thesimple network and create corresponding model by using NS2 simulator, demonstrates selected characteristics of the specifiednetwork configuration using the simulation model, and show scenario of transmission data among nodes. Two languages using in this paper to simulate tool. Finally to show facility of simulate uses cryptography to secure information packets transfer among nodes using C++ language to process because faster than tcl.

KEYWORDS: NS2, TCL, C++, Wire Network, Wireless Network, Information Security, RC5 Algorithm

INTRODUCTION

In this study Network Simulator (NS2) has been designed by using networks, as a base ofsecurityevaluation and it describes the proposedmodel of the system and complete description of the simulations and software program needed for implementing the Network. NS2 is a widely used tool to simulate of networks. It is a part of software that predicates the performance of a network without a real network being there [1].

Moreover, NS2 is a vital simulation tool for networks. It supports a number of algorithms for routing and queuing. It is very helpful because it is very costly to verify viability of new algorithms, test architectures, check topologies, check data transmission etc. Network simulators are names for series of discrete event network simulatorsand are heavily used in ad-hoc networking res. and support popular network protocols, offering simulation results for wire and wireless networks [2]. Also using cryptography in the network the basic conceptions in the security of the network, then it discusses encryption and decryption conceptthe implementation of non-conventional of cryptography algorithms (both blocks and stream ciphers) [12].

WIRELESS NETWORK

WirelessNetwork is described as a connection of deviceswhich communicate by using wirelesstechnologies [7]. Network Wireless communication is used as a term for transmission ofinformation from one place to another. This may be one-way communication as in broadcastingsystems, or two-way communication(e.g. mobile phones, Willkie talkie, ground to Air and Computer network). Intelecommunications, Networkwireless communication is thetransfer of informationwithout the use of wires [5].Itscommunication refers to any type of computer or devices (for examples Access point, wireless Router, Wi-Fi)network that is commonly associated with communications wireless network to interconnectionsnodes [6].Network security is a relatedtopic in many organizations. The widespread apprehensionover network security is due to the connectivity of many devices [4].Consideration of security in the System Development Life Cycle and save information is essential for implementing and integrating a comprehensive strategy for managing risk for

all information technology assets in networks[8].Information security refers to protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection,eavesdrop, recording or destruction. The termInformation Security, Computer Security and Assurance are frequently used interchangeably. These fields are interrelated often and share the common goals of protecting the confidentiality, integrity and availability of information despite of having some subtle differences between them[3].

CATEGORIES OF NETWORK

Wireless networks can be classified into some categories depending on different criteria(e.g. size of the physical area that they are capable of covering and domain of their use).The Wireless networking refers to nearly every type of design as some kind of areanetwork [1]. Common examples of area network types are:

- PAN - Personal Area Network
- WLAN - Wireless Local Area Network
- WAN - Wide Area Network
- MAN - Metropolitan Area Network
- DAN - Desk Area Network

FEATURES OF NS2

NS2 are discrete simulation events aimed in networks of researches. It provides support for simulation of Transmission Control Protocol (TCP) and it is one of the core protocols of the Internet protocol suite. TCP is one of the two original components of the suite, complementing the Internet Protocol (IP), and therefore the entire suite is commonly referred to as TCP/IP, routing, and multicast protocols over all networks including wired and wireless networks. NS2 can be employed in most UNIX and it is a multitasking, multi-user computer operating systems and windows (XP, VESTA and 7), In this project windows server pack 3has been employed. Most of the NS2 code processing is in C++ language. It uses Terminal Command Language (TCl) as its scripting language[2].

STRUCTURE OF NS2

● NS is an object oriented discrete event simulator

– Simulator maintains list of events and executes one event after another.

– Single thread of control: no locking or race conditions.

● Back end is C++ event scheduler

– Protocols mostly.

●Source code

– Most of NS2 code is in C++.

●Scripting language

– It uses TCL as its scripting language.

●Protocols implemented in NS2

– Transport layer, traffic agent, TCP.

– Interface queue, drop tail queue.

●Scalability

–Per-packet processing must be fast;

–Separating control and packet handling

●Extensibility:

–Must be easy to add new objects.

–Object trees to understand hierarchy:

- In C++;
- In tcl.

●C++ and tcl trees are split:

– If not needed nothing have to be changed at a certain level.

Figure 1in the following refers to directory of NS2 to run (Tcl) program to show NAM tool and to show nodes in this project:

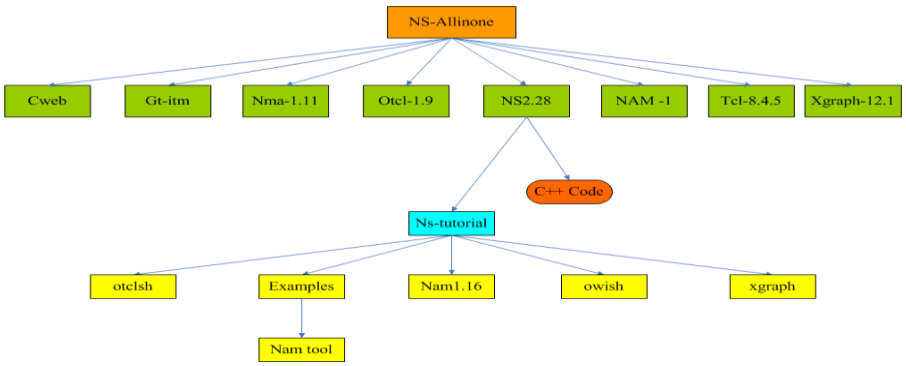

Figure 1: The NS2 Directory Structure

PROGRAMMING LANGUAGE IN NS2

The reason for having two programming languages is to have an easy to use, yet fast and powerful simulator. C++ forms an efficient class hierarchy core of NS2 that takes care of handling packets, headers and algorithms. Object Tcl, or OTcl, is also an object oriented programming language utilized in NS2 for network scenario creation, allowing fast modifications to scenario scripts. Simulation scenario contains network nodes, applications, topology and connections between the nodes. OTcl and C++ interact with each other through Tcl/C++ interface calledTcl/C++as depicted in figure2 [9].

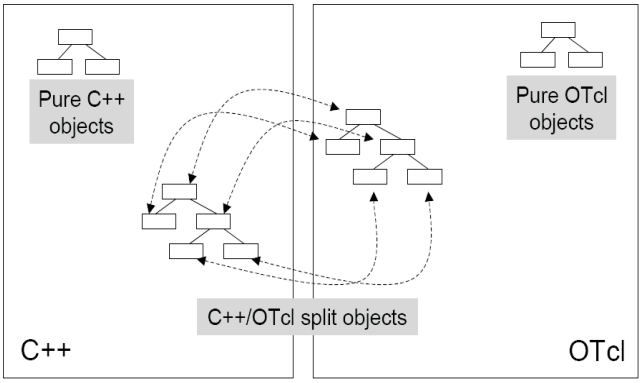

Figure 2: C++ and Tcl Communication

Tcl/Otcl is a language with very simple syntaxes that allowseasy integration with other languages. Tcl was created by JohnOuster out. The characteristics of these languages are :

- It allows a fast development.
- It provides a graphic interface.
- It is compatible with many platforms.
- It is flexible for integration.
- It is a scripting language.

Tcl in ns-2 enables full control over simulation setup, configuration, and occasional actions (e.g. creating new TCPflows). It is a language that compromise between speed andabstraction level offered to the user. In the scenario of this project the Tcl language is used to design the network(set parameters, node configurations, and topology, Connection between nodes, transfer packages and simulation time).Furthermore, C++ language is used for the security package (encryption /decryption)[9].

CRYPTOGRAPHY ALGORITHMS

The information encryption is cryptography algorithms which comprises (symmetric and asymmetric) and hash function to encryption to send data securely between two nodes. The system must encrypt the data orsystematically scramble information so that it cannot be read without knowing thecoding key. This operation determines to a certain level the strength of the security system; theharder it is to break the encrypted message the more secure the system is to be. Figure 3in the following shows the common use of encryption/decryptiontechniques, where unsecured messages (plain text) are encrypted using a specialencryptiontechnique for this propose of the project(RC5) algorithm is used, sent over the network, then decrypted at the destination toviewed back asunencrypted messages.

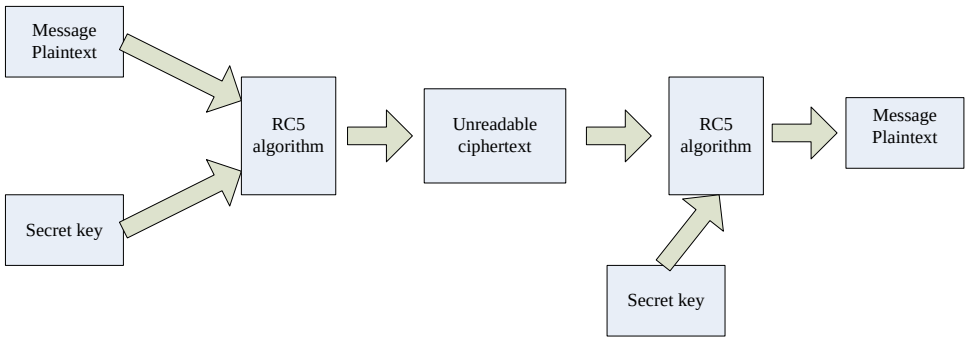

Figure 3: Encryption and Decryption Information

RC5 Algorithm

In this propose wireless network design uses RC5 algorithm to security of information.RC5 algorithm which was developed byRonald Rivest in 1995 as a parameterized symmetric encryption. RC stands for "Rivest Cipher", oralternatively, "Ron's Code". RC5 parameters are; avariable block size (w), a variable number of rounds (r) and a variable key size (key length) (k).Allowable choices for the block size (w) are 32, 64 and 128 bits. The number of rounds can range from 0 to 255, while the key size canrange from 0 bits to 2040 bits[12].

RC5 has three modules: key-expansion, encryption and decryption units. Generally, implementing ciphers insoftware is not efficient based on its speed in terms ofcomputation and hence the use of hardware devices is an alternative.The RC5 algorithm uses three primitive operationsand their inverses:

- Addition/subtraction of words modulo 2w, where w is the word size.
- Bit-wise exclusive-or denoted by XOR.
- Rotation: the rotation of word x left by y bits is denoted by x<<<y. The inverse operation is the rotationof word x right by y bits, denoted by x>>>y. The RC5 algorithm was designed to have the following objectives [10]:
- Symmetric block cipher.
- Suitable for hardware and software.
- Fast(RC5 is simple algorithm and is word oriented ,the basic operations work on full words of data at a time).
- Adaptable to processors of different word-length.
- Variable –length cryptography key (k) (0 -2040) bits.
- Variable number of rounds(r) (0-255).
- Simple (RC5 simple structure is easy to implements and eases the task of determine the strength of the algorithm).
- Low memory requirement’s (This property makes the algorithm suitable for smart cards and other devices with restricted memory).
- High security (It should provide high security when suitable parameter values are chosen).
- Data-dependent rotation (RC5 incorporates rotations (Circular bit shifts) whose amount is data dependent. This indicates to strengthen the algorithm against cryptography.

Flow Chart

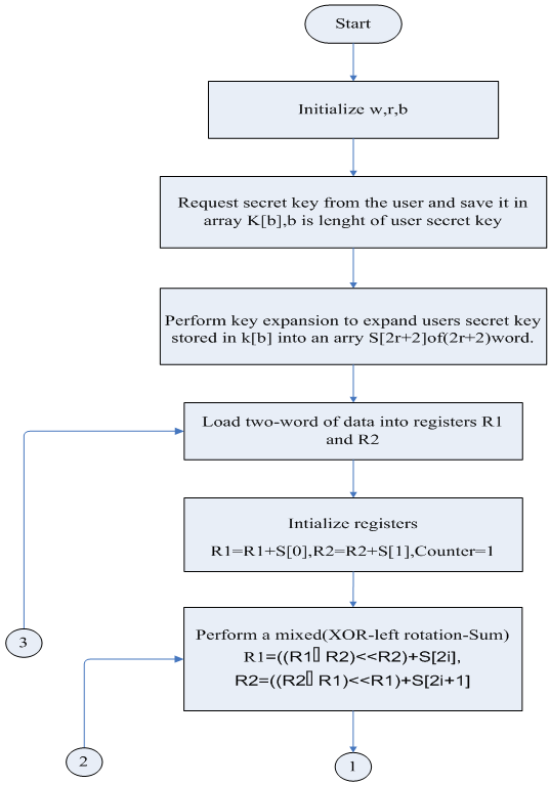

Figure 5: RC5 Algorithm Encryption

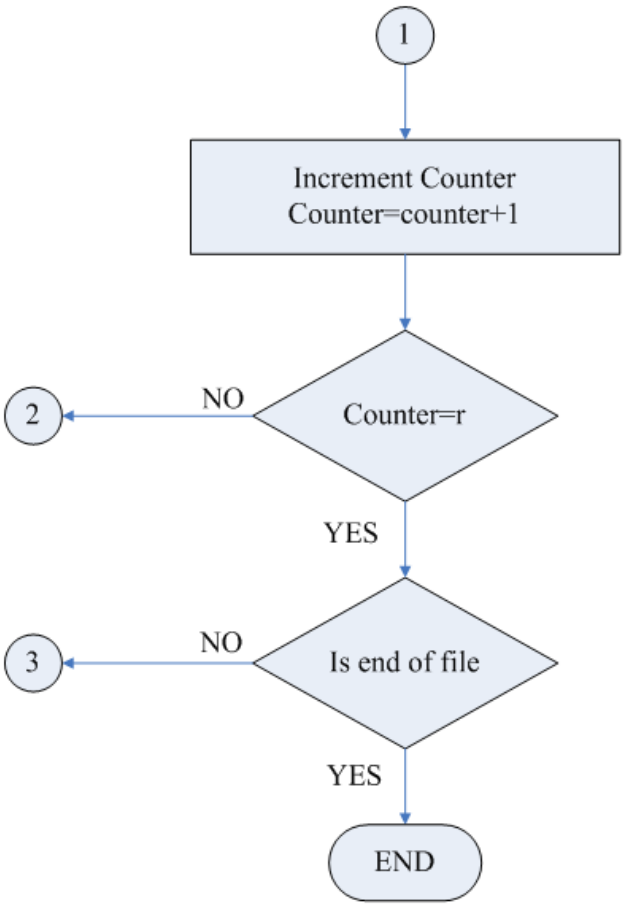

Figure 6: Complements of RC5 Encryption

DESIGN OF WIRE NETWORK

Nam Output to Wire Network

The Nam class outputs at run time in the simulation sets the diagram which isthat shows network consisting of eight wire nodes and topology of network which are connected between nodes the topology is tree. The figure 7 shows the transmissioninformation (traffic of packets) among nodes after press on play button on Nam simulation.

(Performance Evaluation for CAST and RC5 Encryption Algorithms)ieee Paper for RC5

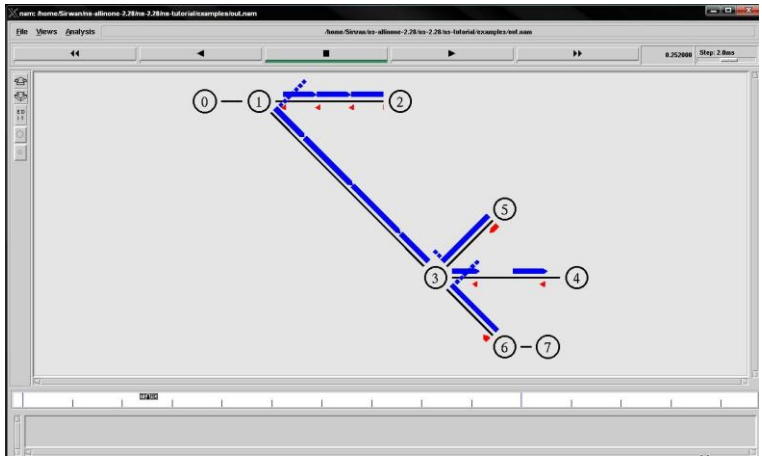

Figure 7: Nam Output Transmission Packets between Nodes

Blue color shows transferring data among nodes forward and red color refers backward s data. This shows that NS2 can be used for wire network; however, this is not the main purpose of this study. Therefore, in the next part we will focus on the Wireless network type.

WIRELESS NODES

To design wireless network the information about all the components in nodes are required. These are some description of some parameters of wireless networks:

A mobile node consists of network components:

- Link Layer (LL)
- Interface Queue (IfQ)
- the MAC layer
- the PHY layer: the wireless channel that the node transmit and receive signals from

At the beginning of a wireless simulation, the definition of kind of each for network components is required, and definition of the other parameters as well such as:

- The type of antenna.
- The radio-propagation model.
- The type of ad-hoc routing protocol used by mobile nodes etc.

Figure 8 shows description and parameters of mobile node of wireless network and connect to channel.

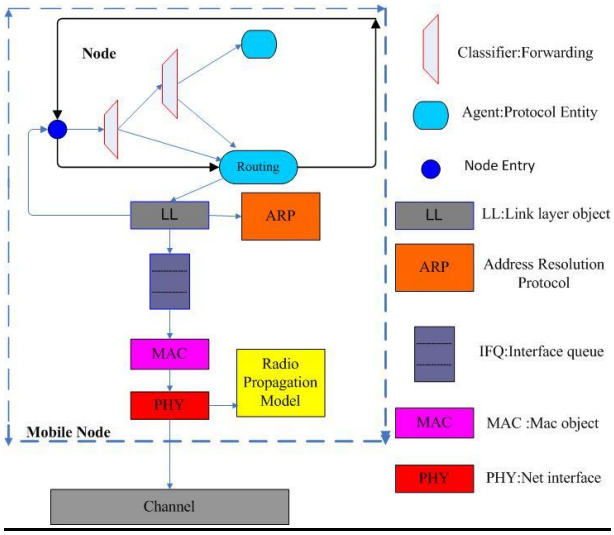

Figure 8: Wireless Node Descriptions

WIRELESSNETWORK PARAMETERS

To design a wireless network all the variable should be known and definitionof all options to nodes. Some parameters which are used in the wireless network design shown below:

- Routing Protocol: AODV, DSDV, and DSR.
- MAC layer Protocol: TDMA, CDMA, IEEE Mac 802.x
- Physical layers: different channels, directional antenna, and omnidirectional antenna.
- QoS:Diffserv.
- Radio propagation, Mobility models, Energy Models.
- Topology Generation tools.
- Visualization tools (NAM), Tracing.

Wireless Network Layout

In this section the process of applying Wi-Fi technology for connecting various devices will be discussed. Figure 3.15 shows layout of wireless network and figures (3.16, 3.7, and 3.18) are shown to design wireless network flow chart to using cryptography algorithm in encryption information:

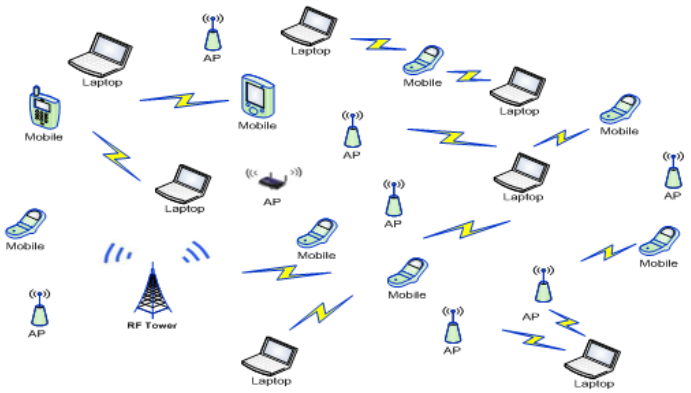

Figure 9: Wireless Network Layout

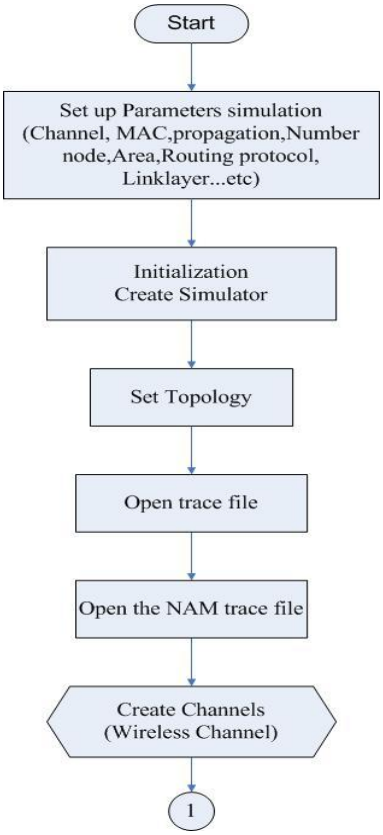

Figure 10: Flow Chart to Reference Station Program

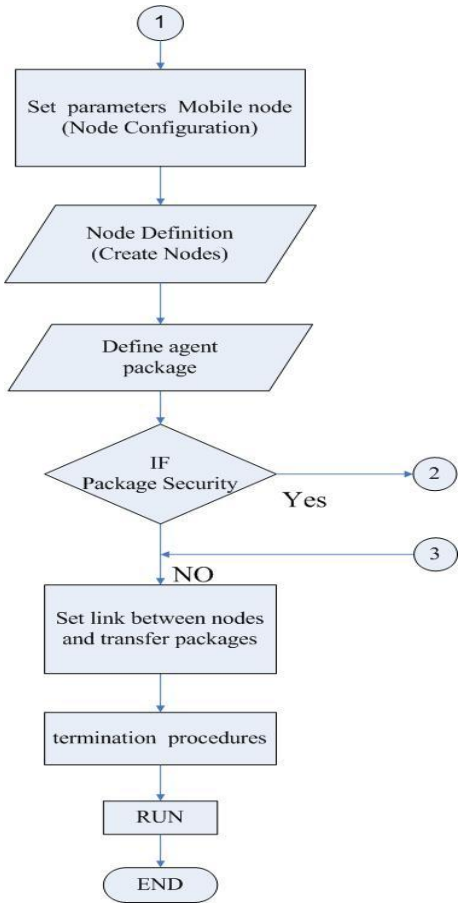

Figure 11: Complement Flow Chart to Reference Station Program

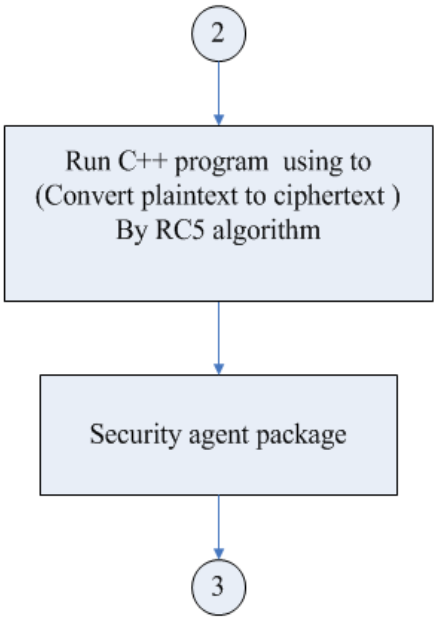

Figure 12: References to C++ Process

Simulation Scenario

In this sectionthe wireless network performance depends mainly on the end to end,and to present simulation scenario aimed at stimulating the network security through network throughput, packet transfer between nodes within the scenario by using cryptography algorithms.In the simulation used RC5 algorithm to cipher package information that transfer between nodes.

In the wireless network used the aidedsoftware like NAM to make a further study. Simulation process and results analysis first of all, to set the topology and the configuration ofnodes properties, and also properties of MAC layer for some address type, protocol type, channel type, simulation time, modulation type, tx ,rx,idle ,sleep power and transmission way of wireless.The following is the parameters of simulation scenario shows in table 3.1

Table 3.1: Description of Wireless Network

Parameters	Values
Area of Simulation	(500X500)m
Nodes number	35
Types of Routing protocol	AODV
Internet protocol type	TCP
Antenna Model	Omnidirectional
Max package	50
Type of the MAC	802.11
Transmission speed	1,2 Mbps
Bandwidth	20MHz
Security algorithm	RC5

After saving file of the program and start the simulation, when click on the (Run) button in the Nam window see that propagation signal of all nodes show in figure 13 and coverage area of nodes .After 30 second of start running the simulation to show sending data packets(packets secure) from node 0 to node 24andnode 17 node 9 refer as is showing in figure 14.

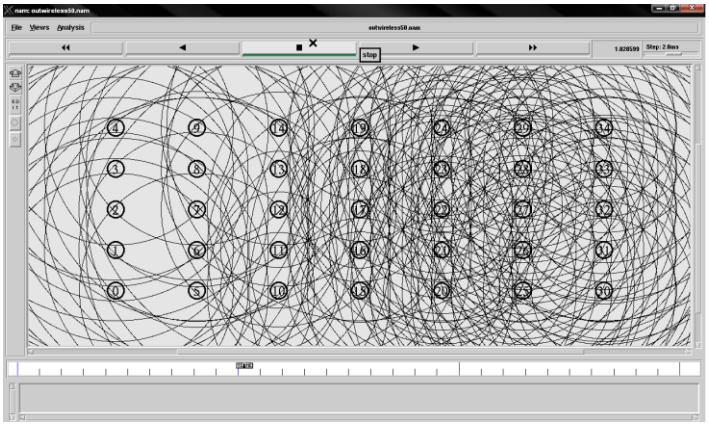

Figure 13: Nam Output Showing Signal Propagation of Wireless Nodes

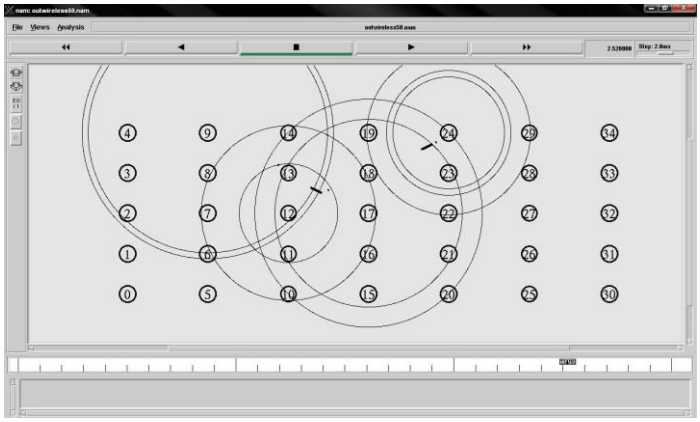

Figure 14: Nam Output –Transmission Security Packets (Two Scenario)

CONCLUSIONS AND FUTURE WORK

Wireless network is a computer or devices networkwhichare wireless,and they are commonly associated with a telecommunicationsnetwork whose interconnections between nodes areimplemented without the use of wires. Wireless telecommunication networks are generally implemented with some type of remote data transmission system and control or to automation that uses electromagnetic waves, such as radio waves, for the carrier, and this implementation usually takes place at the physical level or (layer) of the network.

In conclusion, we found out that network simulator (NS2), is used as a tool to design the result of the simulation are transfer information secure between nodes. In this paper NS2.28 simulator the end user performance of wireless network consisting 35 nodeshas been used. The simulation results will be discussed in the following about network behavior:

- First stepis transfer information package between nodes (two scenario once if node 0 and node24 as two way communication between them, and node 17 and node 9 also two way communication).
- Secondstep includes using Cryptography algorithm (RC5 algorithm) to secure information of package transfer in communications.
- Third step is the important feature of simulation using C++ program to security information and tcl language for scenario script.

It is suggested that for future work to usecombineof two type cryptography algorithm as(hybrid) to more secure information transfer among nodes.

REFERENCES

1. Network types, link: http://compnetworking.about.com/od/basicnetworkingconcepts/a/network_types.htm, December 2012.
2. NS-2, link: http://www.isi.edu/nsnam/ns/tutorial/ , November 2012.
3. Bidgoli H., "Handbook of Information Security", john Wiley & Sons, Inc. Volume 1, 2006.
4. Richardkissel,kevinStine,and Matthew “Information Security” NIST Special publication 800-64 Revision 2,October 2008, pages 4 ,5 .
5. Wireless Communication, link http://www.atis.org/ , Archived from theoriginal on 2008-01-02.
6. Andrea Goldsmith, Wireless Communications, Cambridge UniversityPress, September 2005, ISBN13: 9780521837163.
7. William Stallings, Wireless communications and networking, WilliamStallings books on computer and data communications technology,Publisher Prentice Hall, 2002, ISBN10 0130408646, ISBN139780130408648, Length 584 pages.
8. Jody L. Schivley” Network Security and the NPS internet Firewall”September 1994,.
9. Rackley Steve, "Wireless Networking Technology", First published, 2007.
10. Elkeelany Omar, and OlabisiAdegoke,"Performance Comparisons, Design, and Implementation of RC5 Symmetric Encryption Core using Reconfigurable Hardware" JOURNAL OF COMPUTERS, VOL. 3, NO. 3,(2008),48-55.
11. 12.Verma Harsh Kumar, Singh Ravindra Kumar," Performance Analysis of RC5, Blowfish and DES Block Cipher Algorithms", International Journal of Computer Applications , Volume 42,No.16,2012.