Volume 3, No. 12, December 2012
Journal of Global Research in Computer Science
ISSN-2229-371X
RESEARCH PAPER
Available Online at www.jgrcs.info

DESIGN OF WIRELESS NETWORK BASED ON NS2

Sirwan A.Mohammed
M.Sc. Student
Faculty of electrical engineering
University of Sulaimani-Iraq

Prof. Dr. Sattar B.Sadkhan
Chairman of IEEE IRAQ SECTION
University of Babylon

***Abstract*—**The main goal of this paper is to present how to use NS2simulation for designing wireless networks and using Cryptography algorithm as to security information. It briefly describes the basic wireless networks categories, analyzes wireless LAN networks, briefly describes their components and technologies, explains the Wi-Fi technology and analyzes property sources related to wireless networks simulators and its detailed description, Specify the configuration for the simple wireless network and create corresponding model by using ns-2 simulator, demonstrates selected characteristics of the specified network configuration using the simulation model, and show scenario of transmission data among nodes.

Keywords: NS2, Wireless Network, Security, RC5 algorithm.

INTRODUCTION

Design of wireless Network uses NS2, as a base on Security evaluation, and describes the proposed model of the system and complete description of the Simulations and software program needed for implementing the Network. Ns-2 is a widely used tool to simulate of networks. Network simulator is a part of software that predicates the performance of a network without a real network being there.NS2 is a vital simulation tool for networks. It supports a number of algorithms for routing and queuing. NS2 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 simulators and are heavily used in ad-hoc networking res. and support popular network protocols, offering simulation results for wireless networks. Also using security in the network the basic conceptions in the security of the network, then it discuss encryption and decryption concept the implementation of non-conventional (both blocks and stream ciphers).

WIRELESS NETWORK

Network is described as a network of devices which communicates by using wireless technologies [7]. Network Wireless communication is used as a term for transmission of information from one place to another. This may be one-way communication as in broadcasting systems (such as radio and TV), or two-way communication (e.g. mobile phones ground to Air and Computer network). In telecommunications, Network wireless communication is the transfer of information and without the use of wires [5].Wireless Network communication refers to any type of computer or devices (for examples Access point, wireless Router) network that is commonly associated with communications wireless network to interconnections nodes. [6]Network security is a related topic in many organizations.

The widespread apprehension over network security is due to the connectivity of many.[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 an Networks.[8]Information security means that protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, eavesdrop, recording or destruction. The terms information 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; however, there are 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 area network [1]. Common examples of area network types are:

a. PAN - Personal Area Network
b. WLAN - Wireless Local Area Network
c. WAN - Wide Area Network
d. MAN - Metropolitan Area Network
e. DAN - Desk Area Network

FEATURES OF NS2

NS2 (Network Simulator version2)**:** NS2 is a discrete event simulator targeted at networking research. It provides support for simulation of TCP, routing, and multicast protocols over all networks wireless.NS2 can be employed in most UNIX systems and windows (XP, VESTA and 7), and in this paper windows XP is used. Most procedure processes of the NS2 code are written in C++. It uses TCL as its scripting language, Otcl adds object orientation to TCL.NS (version 2) is an object oriented, discrete event driven network simulator that is freely distributed and open source.

STRUCTURE OF NS2

a. NS is an object oriented discrete event simulator
(a). Simulator maintains list of events and executes one event after another.
(b). Single thread of control: no locking or race conditions.
b. Back end is C++ event scheduler.
(a). Protocols mostly.
c. Source code:
(a). Most of process procedures of NS2 code are written in C++ code.
d. Scripting language:
(a). It uses TCL as its scripting language OTcl adds object Orientation to TCL.
e. Protocols implemented in NS2:
(a). Transport layer (Traffic Agent) – TCP, UDP.(TCP using in our design of wireless network).
(b). Interface queue, Drop Tail queue.
f. Scalability:
(a). Per-packet processing must be fast;
(b). Separating control and packet handling.
g. Import C++ code to TCL script program
Figure 1 refers to directory of NS2 to run tcl program to show Nam tool and show nodes:

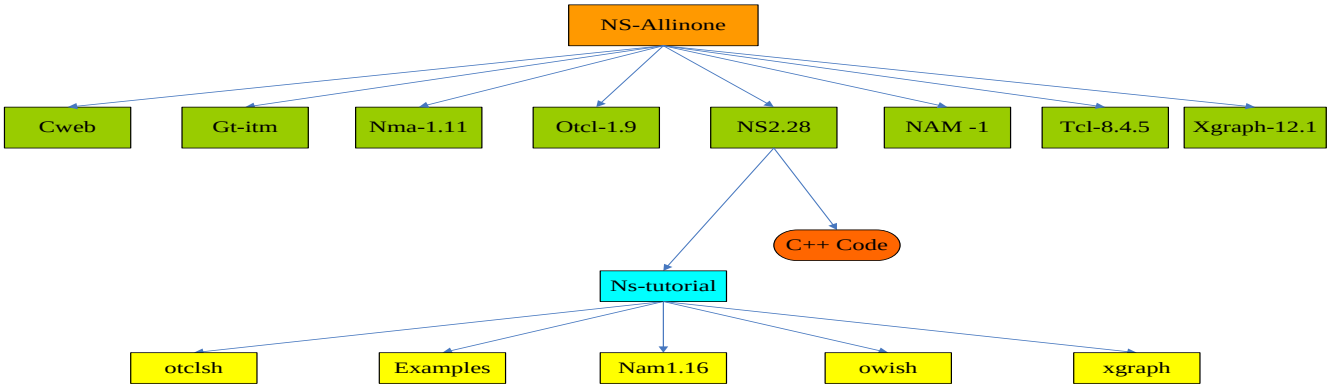

Figure 1 The NS2 Directory Structure

PROGRAMMING LANGUAGE IN NS2

The reason for having two programming languages from the aimis to have an easy to use, yet fast and powerful simulator. C++ forms an efficient class hierarchy core of ns-2 that takes care of handling packets, headers and algorithms. Object Tcl, or OTcl, is also an object oriented programming language utilized in ns-2 for network scenario creation, allowing fast modifications to scenario scripts. OTcl and C++ interact with each other through Tcl/C++interface called Tcl/C++ as depicted in figure 2:

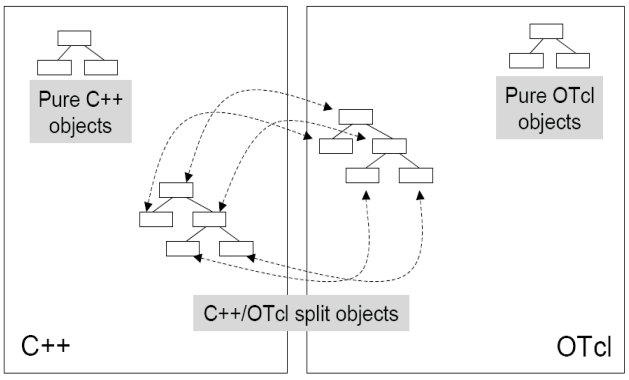

Figure 2 C++ and OTcl Communication

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

a. It allows a fast development.
b. It provides a graphic interface.
c. It is compatible with many platforms.
d. It is flexible for integration.
e. It is a scripting language.

OTcl in ns-2 enables full control over simulation setup, configuration, and occasional actions (e.g. creating new TCP flows). It is a language that compromise between speed and abstraction level offered to the user. In my Scenario, using Tcl language to design wireless network (Set parameters node ,node configurations, topology, Connection between nodes, transfer packages and simulation time) and C++ language using to Security package (encryption /decryption of data transfer between nodes)are achieved.

SECURITY

Security Goals:

All security system must provide a pack of security functions that can confirm the secrecy of the system. These functions are usually referred to as the goals of the security system. These goals can be listed under the following three main categories in this paper:

a. Confidentiality
b. Integrity
c. Availability

In this paper, the information Encryption uses cryptography algorithms symmetric to encryption data information to send data securely between nodes. The system must encrypt the data or" systematically scramble information so that it cannot be read without knowing the coding key". This operation is determined to a certain level of the security system; the harder it is to break the encrypted message, the more secure the system is to be. Figure 3shows the common use of encryption/decryption techniques, where unsecured messages (plain text) are encrypted using a special encryption technique for my propose using Symmetric cryptography (RC5 algorithm), sent over the network, then decrypted at the destination to viewed back a sun encrypted messages.

Volume 3, No. 12, December 2012
Journal of Global Research in Computer Science
ISSN-2229-371X
RESEARCH PAPER
Available Online at www.jgrcs.info

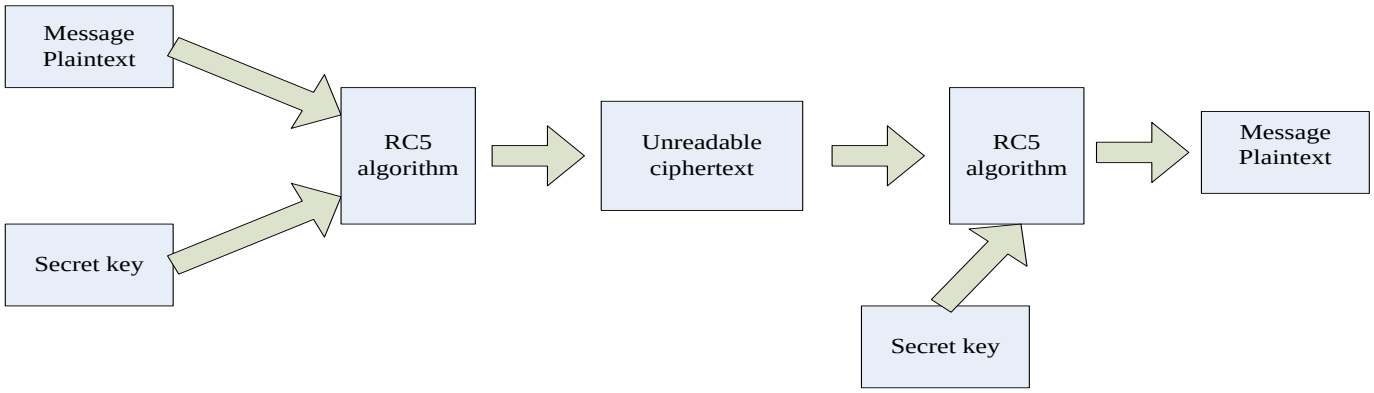

Figure 3 Encryption and decryption information

RC5 Algorithm:

In this Paper, to design wireless network using RC5 algorithm to security of information (data), RC5 algorithm was developed by Ronald Rivest in 1995 as a parameterized symmetric encryption. RC stands for "Rivest Cipher", oral ternatively, "Ron's Code". RC5 parameters are: a variable block size (w), a variable number of rounds (r), and a variable key size (k).Allowable choices for the block size (w) are 32, 64 and 128 bits. The number of rounds range from 0 to 255 bits, and the key size range from 0 to 2040 bits in size. RC5 has three modules: key-expansion, encryption and decryption units. Generally, implementing ciphers in software and hardware is not efficient based on its speed in terms of computation and hence the use of hardware devices is an alternative The RC5 algorithm uses three primitive operations and their inverses.

a. Addition/subtraction of words modulo 2w, where w is the word size.
b. Bit-wise exclusive-or denoted by XOR.
c. Rotation: the rotation of word x left by y bits is denoted by x<<<y. The inverse operation is the rotation of word x right by y bits, denoted by x>>>y.

Data-dependent rotation (RC5 incorporates rotations (Circular bit shifts) whose amount is data dependent. The RC5 algorithm is designed to have the following objectives:

(a). Symmetric block cipher.
(b). Suitable for hardware and software.
(c). Fast (RC5 is simple algorithm and is word oriented, the basic operations work on full words of data at a time).
(d). Variable –length cryptography key(k) (0 -2040)bits.
(e). Adaptable to processors of different word-length.
(f). Variable number of rounds(r)(0-255).
(g). Simple (RC5 simple structure is easy to implement and eases the task of determine the strength of the algorithm.
(h). High Security (It should provide high security when suitable parameter values are chosen).
(i). Low memory requirement's (This property makes the algorithm suitable for smart cards and other devices with restricted memory).

Flow Chart:

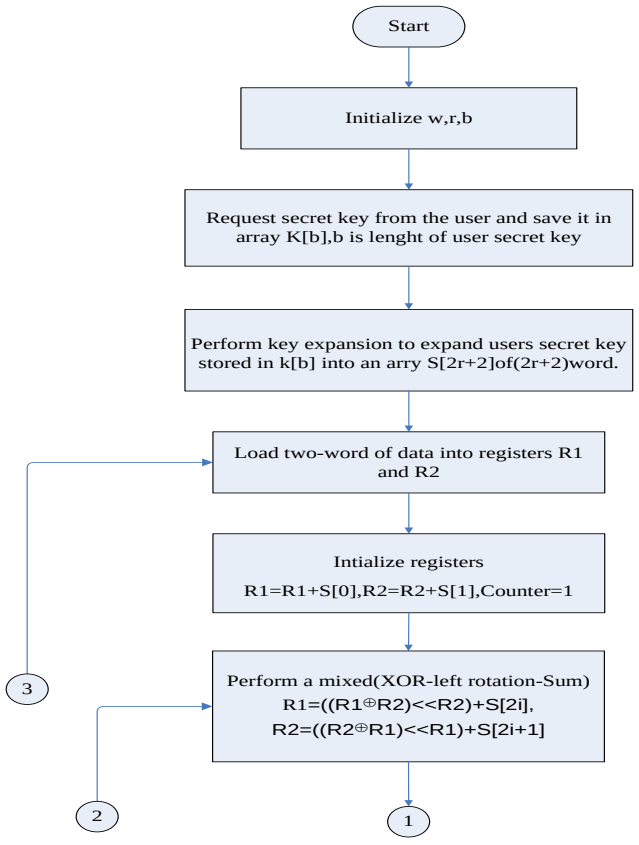

Figure 4: RC5 algorithm encryption

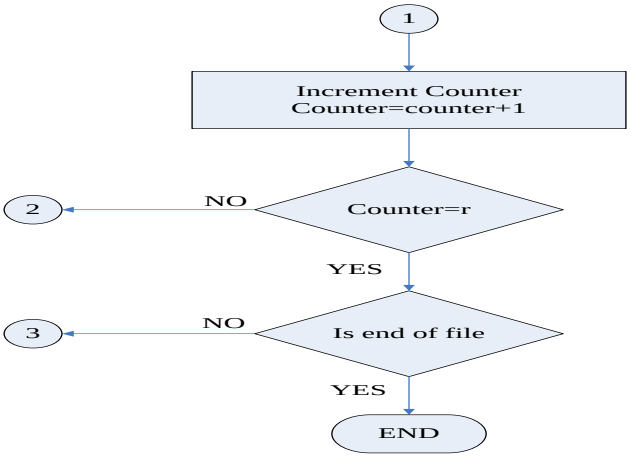

Figure 5 Complements of RC5 Encryption

To design Wireless network to be known all variable and define options to nodes. In this paper used to two way communication between nodes; some parameters using in wireless network to design show below:

a. Routing Protocol: AODV.
b. MAC layer Protocol: TDMA.
c. Physical layers: different channels, directional antenna, Omni directional antenna.
d. QoS: Diffserv.
e. Radio propagation, mobility models, Energy Models.
f. Topology Generation tools.
g. Visualization tools (NAM), Tracing.

Figure 6 to show layout of wireless network.

WIRELESS NETWORK DESIGN

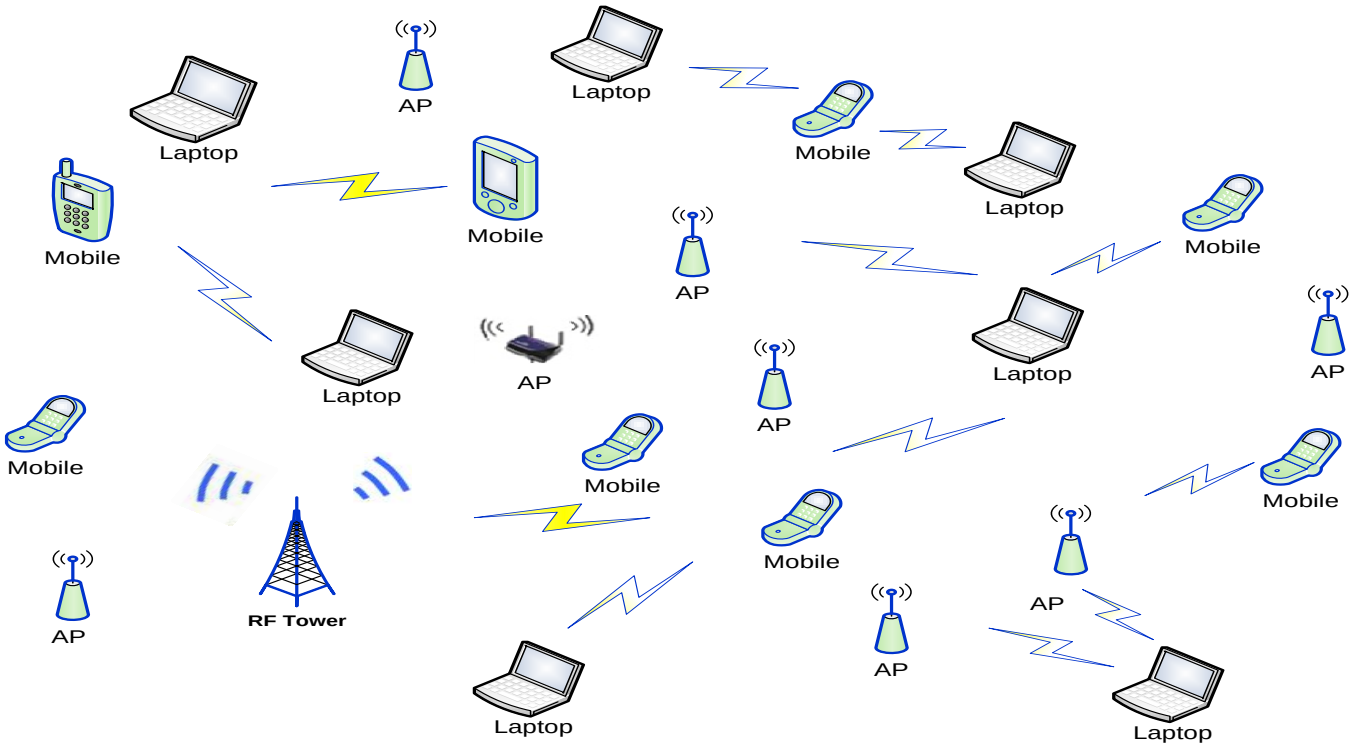

Figure 6 Wireless network Layout

SIMULATION SCENARIO

In this section, wireless network performance depends mainly on the end to end. We are going to present simulation scenario aimed at activating the network security through network throughput, packet transfer between nodes within the scenario by using cryptography algorithms; in our simulator we uses RC5 algorithm to cipher package information that transfer between nodes .

Simulation principles and strategies adopting the separated object model and using two languages C++ and tclNS2 fulfills the achievement of simulation for specific protocols and the configuration nodes and establishment of network simulation environment respectively. Table 1 refers parameter using in scenario, using the aided software like NAM to make a further study, and simulation process and results analysis. First of all, we set the topology and the configuration of nodes properties and also properties of MAC layer like 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 figure 7 and nodes layout before transferring information between them.

Figure 8 refers to propagation of all nodes and is coverage of nodes at some time. Figure 9 refers to transfer information (package information) between nodes and coverage are of radio single and send information (information secure), this information convert from plaintext to cipher text are (Kurdistan regional government) between node (0) and node (24) as scenario. Figure 10 refer to two scenario transmission information between (node0 and node24, node 17 and node 9) at some time, also information is transferred between nodes (17 and 9) are (Sulaimaniyah

International Airport). Figure 11 refer to drop of packages when simulation finished.

Table 1

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

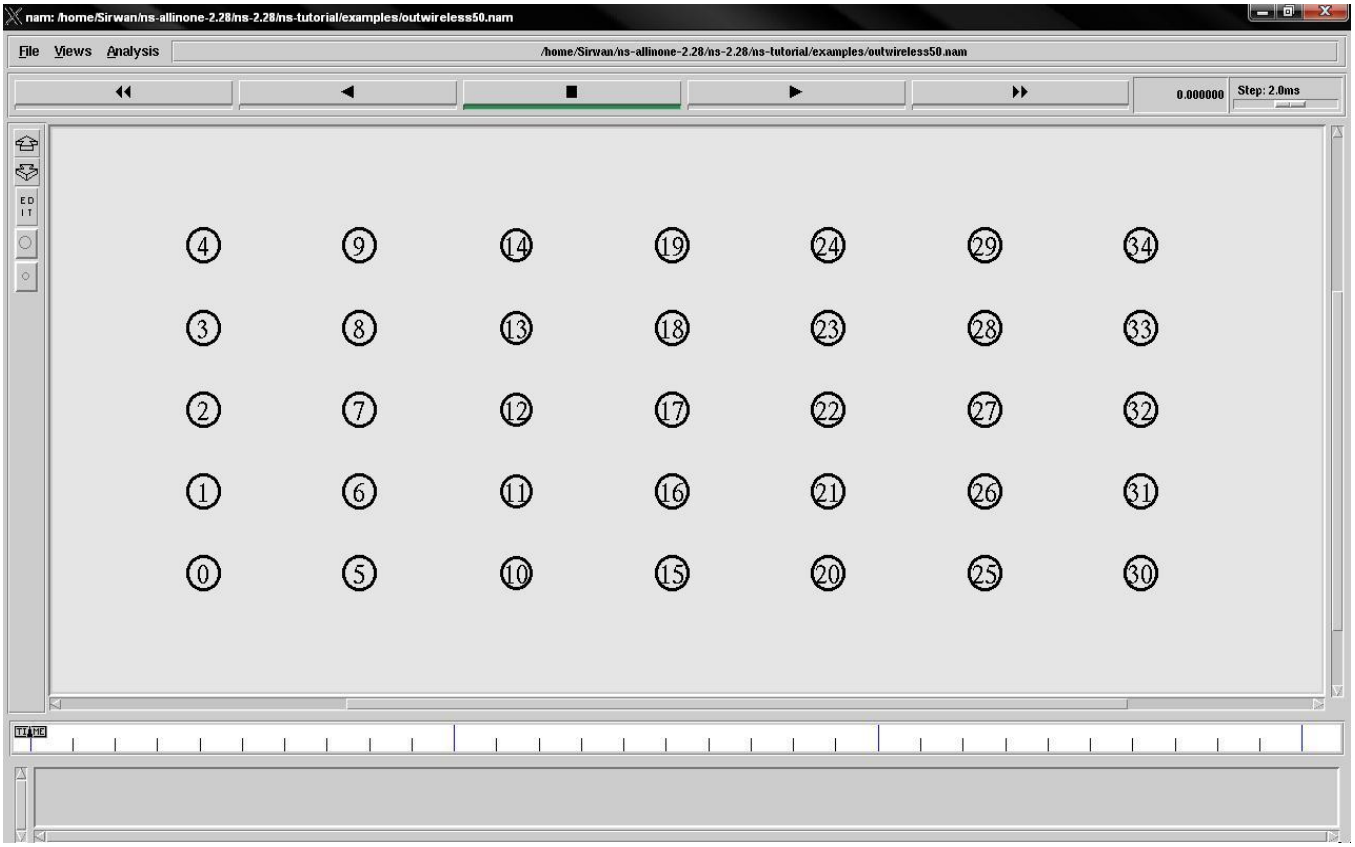

Figure. 7 Nam output showing nodes of wireless networks

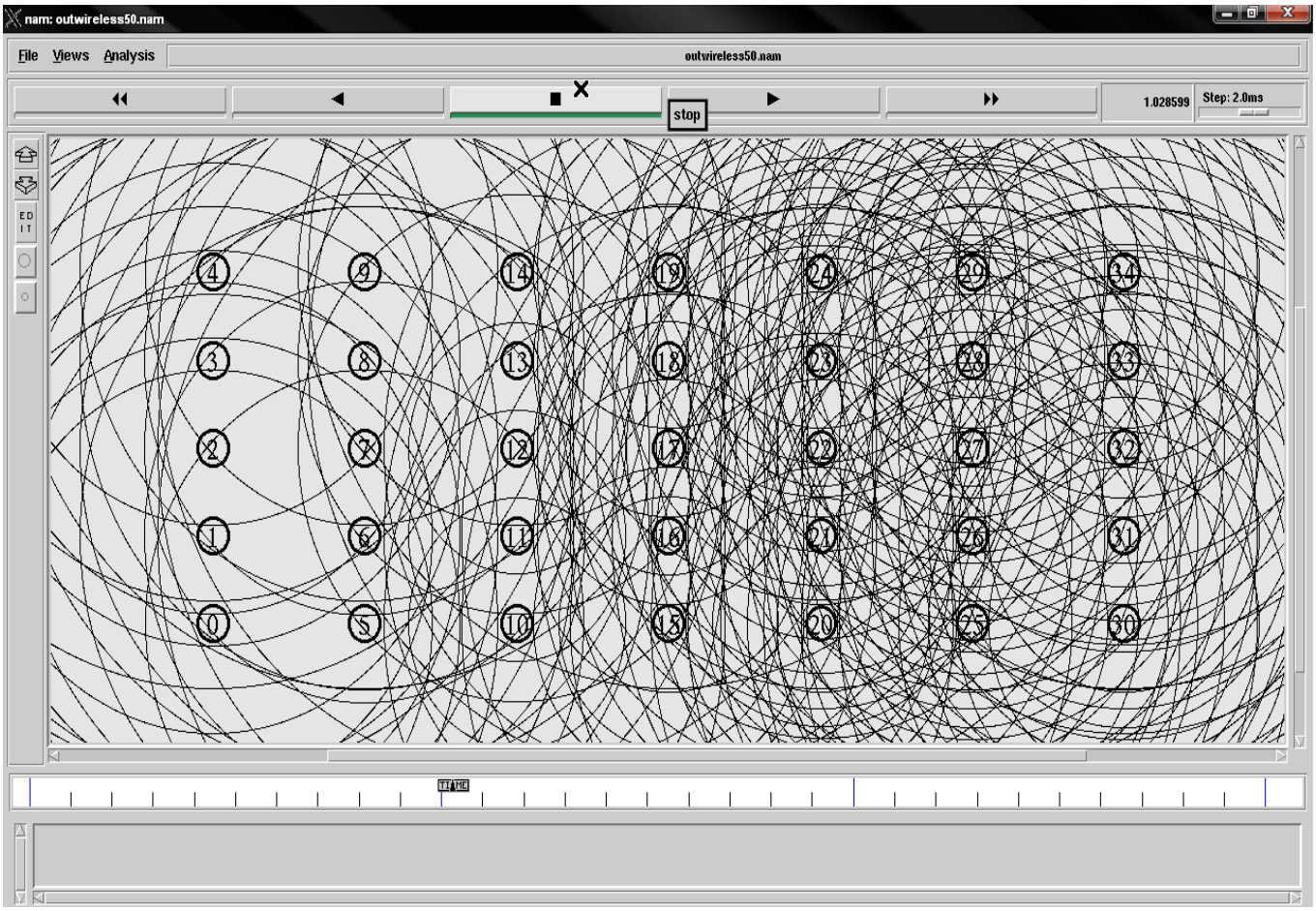

Figure. 8 Nam output showing Signal propagation of wireless nodes

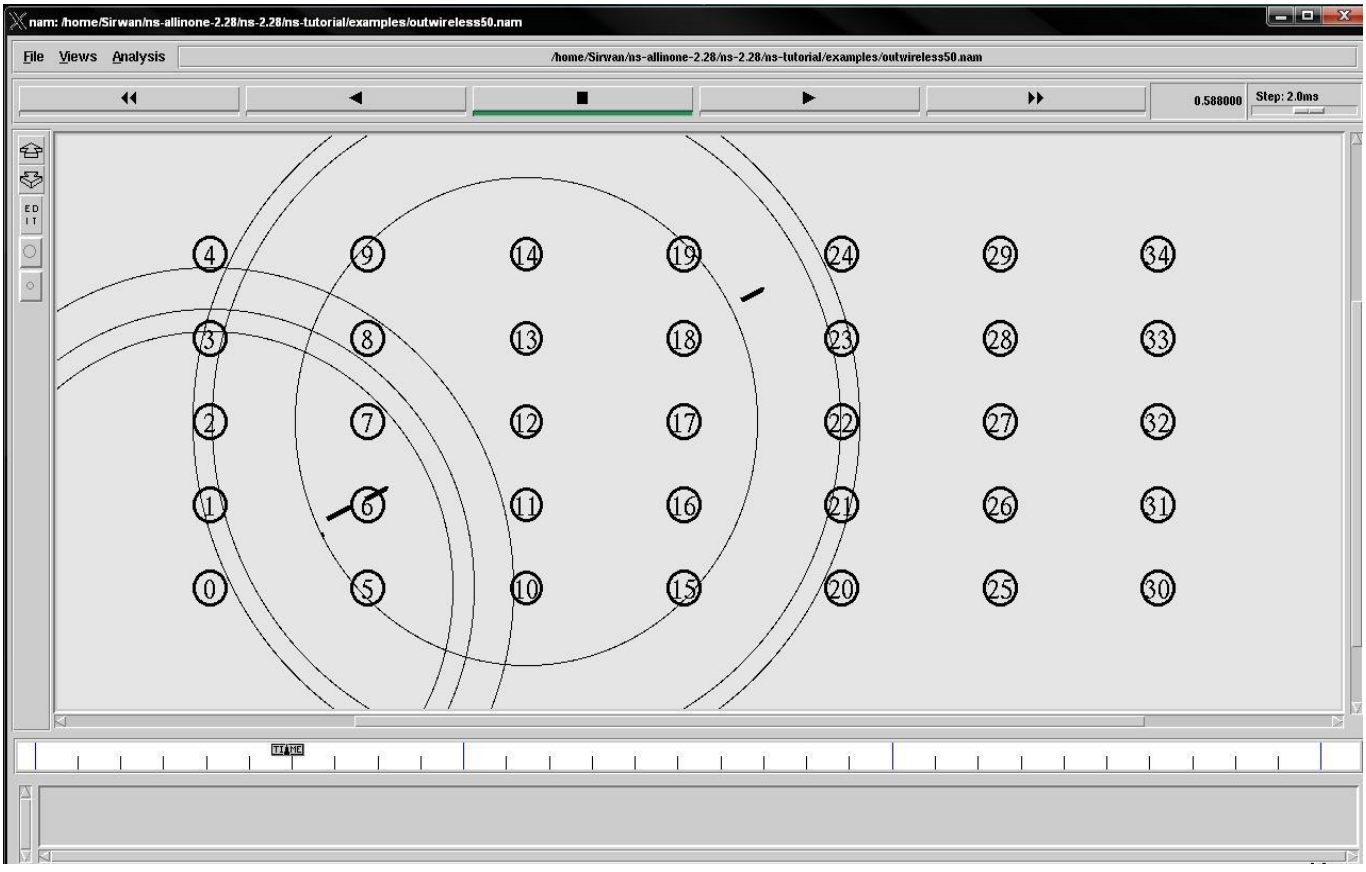

Figure. 9 Nam output – Transmission Security packets (one Scenario)

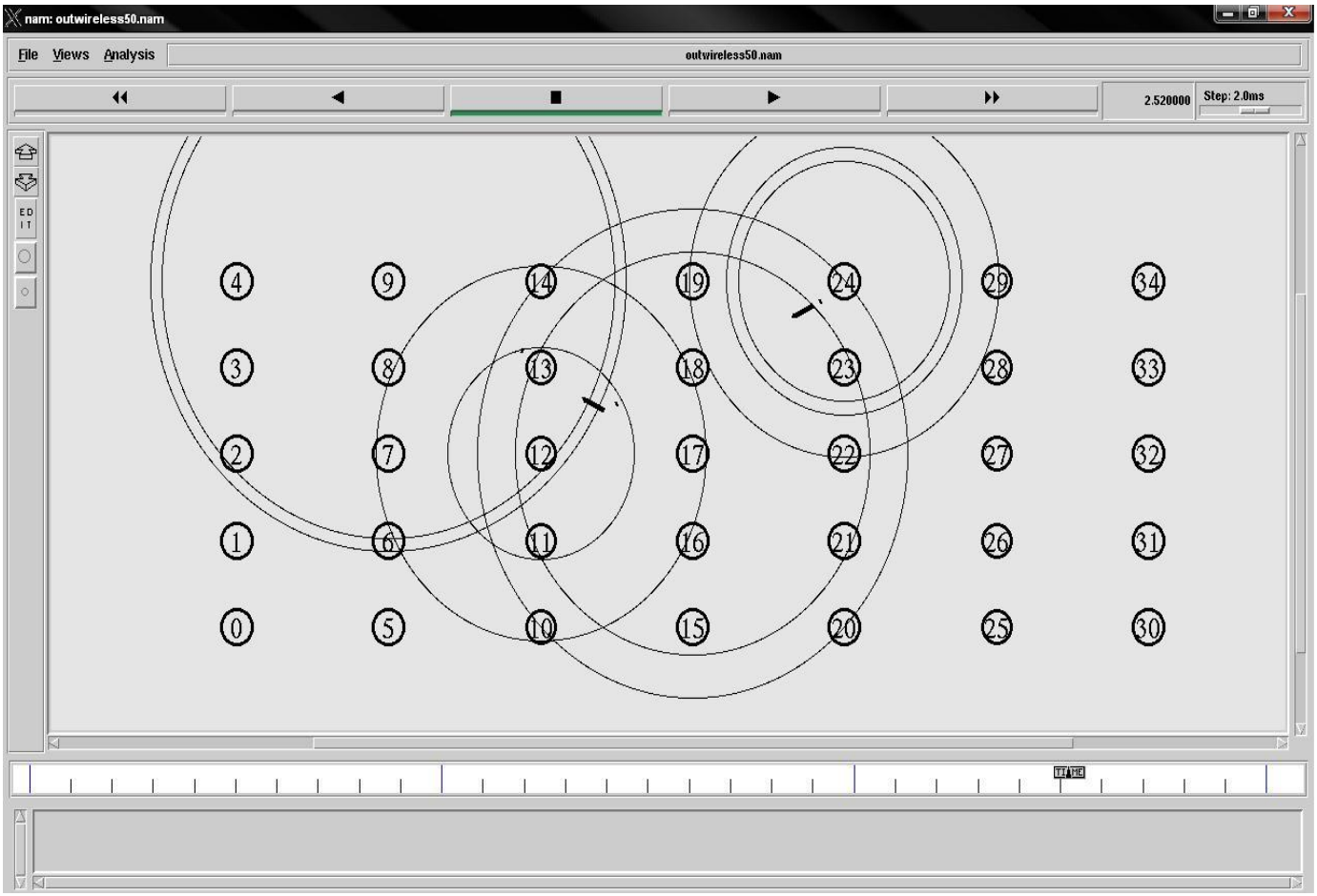

figure 10Nam output – Transmission Security packets (two Scenario)

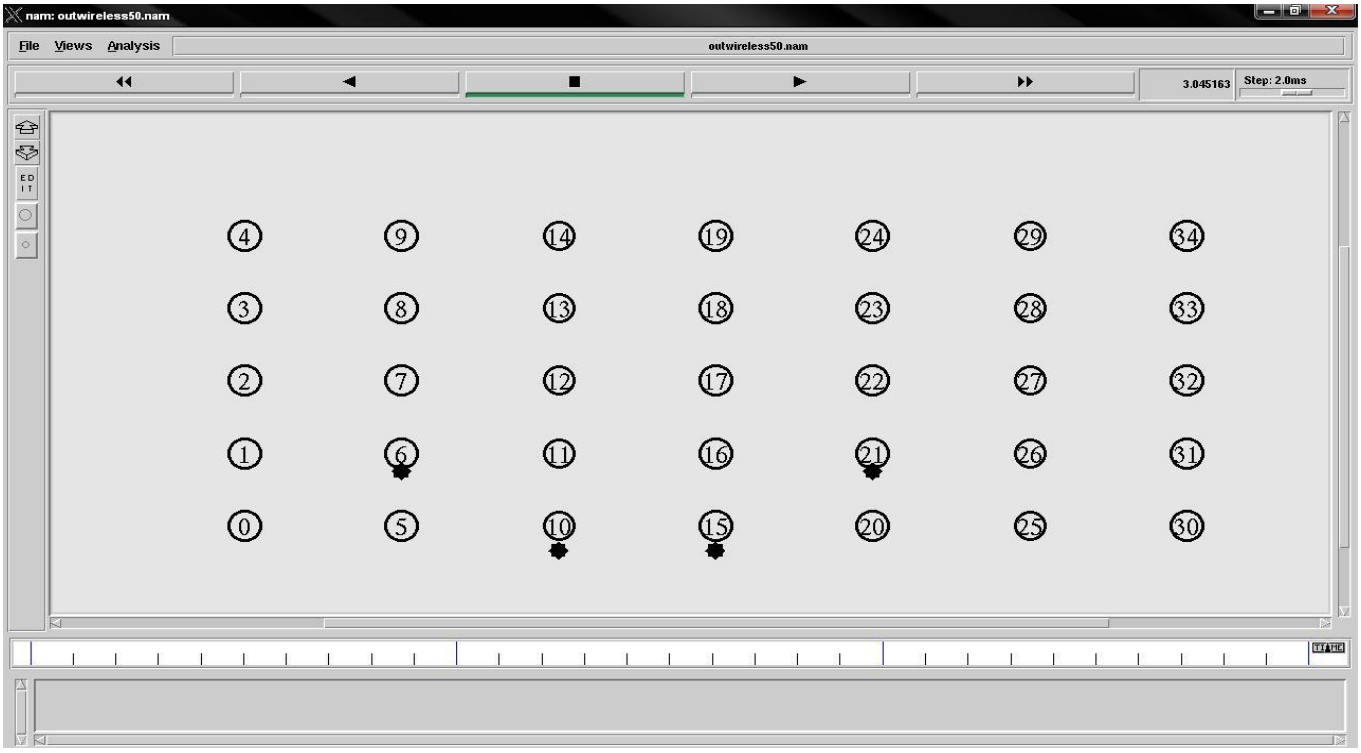

Figure 11 packets are dropped

CONCLUSION AND FUTURE WORK

Wireless network is a computer or devices network which are wireless, and they are commonly associated with a telecommunications network whose interconnections between nodes are implemented 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. The wireless network is likely used because it is efficient especially in those areas that wiring is impossible compared to other networks. When designing wireless networks and/or studying their behavior under various conditions, software simulation tools are often used. In this paper, the software tool Network Simulator (Version 2), widely known as ns-2, is described and used for the simulation of selected illustrative examples of wireless networks. In general, ns2 provides users with a way of specifying network protocols and simulating their behavior. The result of the simulation are transfer information secure between nodes .In the paper we have ns2.28 simulator the end user performance of wireless network consisting 35 nodes ,the simulation result in following conclusion about network behavior:

a. First is 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).
b. Second using Cryptography algorithm (RC5 algorithm) to secure information of package transfer in communications.
c. Third important feature of simulation using C++ program to security information and tcl language for scenario script.
d. For future work to use combine of 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]. http://en.wikipedia.org/wiki/Information_security, September 2012.

[4]. Richardkissel,kevinStine,and Matthew "Information Security" NIST Special publication 800-64 Revision 2,October 2008 .

[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.

