Simulation of Key Management Services in MANETs using Mobility Profiling

Tahir Mahmood[1], Shaftab Ahmed[2]

[1]Department of Computer Science, SZABIST
Islamabad

[2]Faculty of computer Science, Bahria University
Islamabad

Abstract: *Mobile ad-hoc networks, MANET, is a class of wireless networks that can be formed dynamically and randomly without the need for an infrastructure. It consists of independent and dynamic mobile nodes which can detect and establish connection with each other while in the transmission range. MANETs are vulnerable to attacks because of transmission through wireless medium, which can be easily intercepted and misused by the intruder.*

A number of solutions have been proposed for secure communication in MANET. Symmetric key cryptography requires key distribution services and MANET does not have an infrastructure so it is difficult to designate server nodes for key distribution. Hence alternate methods are adopted like threshold cryptography. The contextual awareness of a node activity is used for role assignment to designated nodes.

A case study "Contextual Mobility Profiling Secure Routing Infrastructure For Mobile ad-hoc Networks" is selected for simulation. This paper shows the use of Key Management Services in mobile ad-hoc networks (MANETs) through a set of nodes selected on the mobility profile.

Index Terms: *MANET, PKI, TTP, CA, KDC, OLSR, NS-2*

1. INTRODUCTION

A Mobile Ad-hoc Network (MANET) is formed by wireless nodes. These nodes are dynamically connected when switched on. They disseminate routing information under a protocol like OLSR. To extend the range of MANET multi-hopping technique is used. The nodes falling outside direct range are provided routing services by intermediate mobile nodes. Hence the role of each wireless node can be a sender, a receiver or a router. When the node plays a role as a sender, it can send messages to any specified destination node through some route. When acting as a receiver, the node can receive messages from other nodes. The node can relay the packet to the destination or next router in the route when it plays a role as a router. Nodes can buffer packets awaiting transmission when required [4].

Mobile Ad-hoc networks save money and time because of their nodes capability to work in infrastructure-less environment [2]. Applications of MANETs are military, emergency, disaster recovery, collaborative networking and sensor networks. A lot of research work has been done in the area of routing in mobile ad-hoc networks. However the security over MANETs needs to be addressed before it can be used in critical areas where secure information exchange is essential. The security protocol for MANETs should be light-weight i.e. low computational complexity) and must be highly secured [8].

2. RELATED WORK

Secure communication over a MANET is a challenging task because of the vulnerability of the nodes communication that can be captured in the wireless domain. A number of methods have been proposed for secure communication through encryption. The symmetric key distribution mechanism requires certification authority and a communication system to provide keys to the nodes engaging in a secure session. The contextual mobility profiling [7] may be used to choose suitable nodes to form a key distribution structure which changes its shape with the passage of time. The dynamic changes in the node status are derived from a mobile profile vector maintained at a management node called profile manager. The node status varies from stationary (ST), relatively stationary (RS), mobile (MB) and highly mobile (HM). The mobile units may appear and join the MANET and may vanish on account of loss of power or weak signals.

The simulation of the proposed model of contextual mobility profiling has been carried out using the network simulation tool NS-2. The results are presented in this paper.

2.1 Simulation

Network simulation is used to test different network protocols and new proposed models of network by researchers. This helps researchers to reduce their cost of research by avoiding the use of physical network components. A network simulator may be used to forecast the network's behavior which is virtual rather than physical. The other benefit is the research time which is greatly reduced because of simulation in which different scenarios can be built in short time as compared to implementing a physical network. Hierarchical networks can be designed by using different types of nodes like routers, switches, bridges, computers, laptops, mobiles, PDAs etc.

A network simulator is used to check the performance of network after proposing a new design. Some available network simulators are simple while others are complex. A network simulator should at least provide the facility for the user to define the network topology, nodes, links and traffic between the nodes and could additionally provide the facility to define the protocols in detail. Different graphical applications provide a visual view of simulations. Normally, common protocols are supported by simulators i.e. UDP, TCP, IPV6 etc.

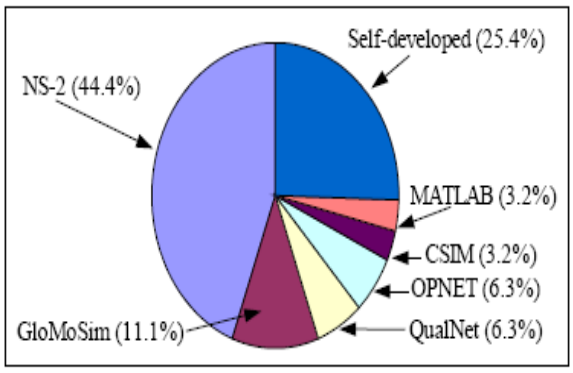

Figure 1. Usage of different network simulators [8]

Some popular network simulators are NS-2, GloMoSim, QualNet, NetSim, OMNet++ and OPNET Modeler while a large number of researchers develop their own simulators [8]. As shown in Figure 1, NS-2 and GloMoSim are widely used in universities and are free/open source. NS-2 runs on Linux and Microsoft Windows.

NS-2 is a discrete event simulator in which a list of pending "events" is stored, and those events are processed in order, with some events triggering future events such as the event of the arrival of a packet at one node triggering the event of the arrival of that packet at a downstream node. NS-2 provides substantial support for simulation of TCP, routing, and multicast protocols over wired and wireless (local and satellite) networks [9].

Outputs of simulations are the trace files which can document every event that occurred in the simulation and are used for analysis. Network Access Management (NAM) trace file is used by NAM to show the simulation in visual form. Visual analysis of a wireless environment is important to validate the accuracy of a mobility model.

The NS-2 network simulator was selected for our simulations because it has been extended for wireless networks, which includes wireless LAN, MANET (Mobile ad-hoc networks) and sensor networks. NS-2 uses two languages, C++ for core of NS Simulator and OTCL (Object Tool Command Language) for scripting the NS-2 simulation setup and configuration. TCL is fast to write and change but slow to run while C++ is fast to run but hard to write and change. Both have their own scope of use.

OTCL is used to quickly explore a number of scenarios by changing different network parameters. The target of our simulation is to find nodes of four types in a given scenario. Detailed protocol simulation or changing in protocol requires C++ i.e. byte manipulation, packet processing, algorithm implementation. The whole thing together makes NS, which is an Object Oriented extended TCL interpreter with network simulator libraries [10] as shown in Figure 2.

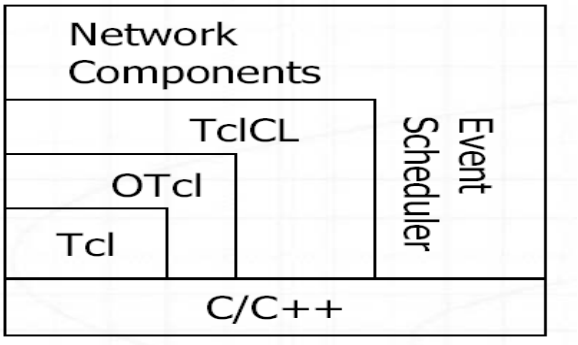

Figure 2. NS-2 Architecture [10]

Different simulation steps in NS-2 are as follows:-

Design simulation Build NS-2 script using TCL and if necessary implement algorithm using C++ Run simulation Analyse simulation results using graphs, animation and view of data files.

In design of simulation scenario, the network topology is selected. Network topology in MANETs consists of the number of nodes, moving range of nodes, Initial positions moving pattern (direction, velocity, acceleration).

Node configuration is then defined after designing topology in which different parameters for nodes are set, such as selection of routing protocol, Mac type, Antenna type, Link layer and physical layer.

Trace files can be created during simulation for NAM (Network Animator) and graphs to analyze the results. These trace files contains special characters which have special meanings i.e. "s" means send and "r" means receiving packet.

The first stable version of NS-3 was launched in June 2008. It is more refined and has support for current protocols and using Python and C++ language.

2.2 Secure key distribution over MANETs

Different key management schemes for MANETs were studied in our first Independent study. It was observed that key management is difficult due to dynamic network topology because of mobility and decentralized nature of MANETs.

The mobility feature of MANETs is the basis of our simulations. Contextual mobility profile is proposed for key management in [7]. According to [7], the following four types of nodes should be noted and keys will be distributed to Stationery nodes or relatively stationery nodes:

i. Stationery
ii. Mobile
iii. Highly Mobile
iv. Relatively Stationery

Stationery nodes are those which remain at the same position throughout the simulation. Mobile nodes change their position during the simulation. Highly mobile nodes are those nodes which are moving faster than mobile nodes. Relatively stationery nodes are those which move very slowly during simulation.

3. KEY MANAGEMENT SERVICES IN MANETS

The simulation study was carried out for a key management services solution presented in [7] for contextual mobility profiling of mobile nodes, the theme of research is as follows:

The security of information transport between participating nodes is of prime importance in MANET. This is because the communication is vulnerable as an intruder can easily listen, capture, modify or overwhelm a node with spurious traffic. In this hostile environment the transport of key to be shared between nodes for a session is quite difficult. Furthermore MANET does not have a stable infrastructure to support secure key transport. The mobile nodes also perform routing and dynamically join or leave a particular scope. The root node which is usually stationary is usually chosen as the initial key manager. It designates other nodes for key dissemination through a ranking mechanism based on various properties like mobility, power and signal strength.

PKI is a widely accepted mechanism for wired network. It is based on the choice of a Certificate Authority which provides certificates to registered nodes to enter in secure session. However in ad-hoc networks the classical PKI is not feasible. The additional factors are link quality, signal strength, battery power and node mobility history have to be considered before designating a node to the status of key distributor.

Single CA in wireless domain may result in a central point of failure and may cause network congestion. The behavior of network is inconsistent due to dynamic variation of node positions hence a node initially closest to the root may be farther than many newly joining nodes in nearby locations. The vulnerability of the node which may be captured physically adds another dimension to the problem in wireless communication [6].

A number of methods have been proposed to handle the above said problems. Threshold Cryptography, Secure OLSR etc. are some of them. These methods rely on distribution of trust by choosing a set of nodes for key distribution; periodic updates are dynamically made in response to the node status.

4. CONTEXTUAL MOBILITY PROFILING BASED SECURE ROUTING PROTOCOL

The nodes in MANET do not exhibit the same properties over time. Hence they should not be treated in the same manner instead they should be assigned roles of infrastructure like routing, control and key distribution etc. The ranking is based on mobility, behavior, power transmission range, computation capacity etc according to current status recorded and propagated through Profile Vectors (PV) [7]. The profile vector may include the fields

like DC-Device Category, BP-Battery Power, AM-Average Mobility, SS Signal Strength, ANN-Average Number of Neighbors and PF-Priority Factor. A rating mechanism is used for this purpose.

5. SIMULATIONS OF KEY MANAGEMENT SERVICES IN MANETS USING MOBILITY PROFILING

In this simulation, the target is to find stationery or relatively stationery nodes so that the keys could be distributed in only these nodes in a battlefield scenario. Mobile and highly mobile nodes are not selected for key distribution.

We used NS-2 version 2.27 on windows XP operating system for our simulation [13]. Table 1 shows the simulation parameters used.

TABLE 1. SIMULATION PARAMETERS

AREA OF NETWORK	**600M X 600M**
TOTAL NUMBER OF MOBILE NODES	**10**
SIMULATION TIME	**5 SECONDS**
NODE MAXIMUM SPEED	**0, 0.5, 2, 6MS**

Our criteria or protocol to assign role of KDC (key distribution center) to different nodes for key management service is as follows:-

If a node is stationery it will be given status of "**ST**".

If a node is mobile then the speed of mobile node is checked according to the following criteria.

i. If moving speed of a node is >= 0.5 m/s and speed < 2 m/s a status of "**RS**" which means relatively stationery will be given to the node.

ii. If moving speed of a node is >= 2 m/s and speed < 6 m/s a status of "**MB**" which means mobile will be given to the node.

iii. If moving speed of a node is >= 6 m/s then it will be given the status of "**HM**" which means highly mobile node.

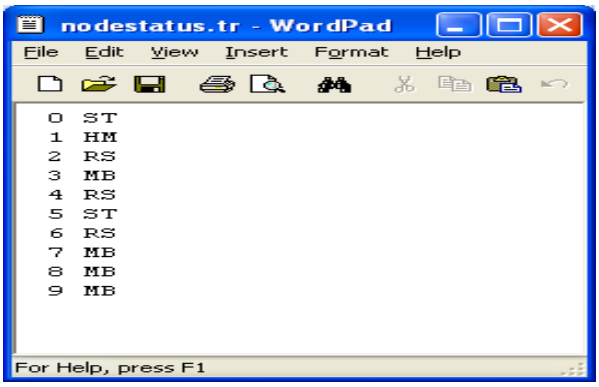

Figure 3. Contents of nodestatus.tr file

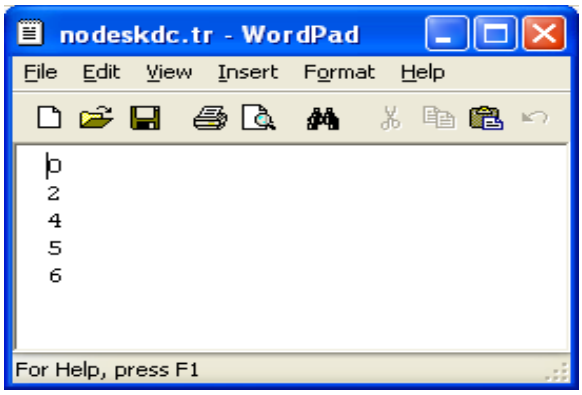

Figure 4. Contents of nodeskdc.tr file

When all nodes are given status according to above criteria then stationery "nodes with "ST" status and relatively stationery nodes with "RS" status are selected as KDC (Key distribution centers). Key can be distributed through these selected KDC nodes and will not be given to the remaining nodes which not only reduce network traffic but also increase network security and performance.

The first simulation runs for five seconds in which ten nodes participate and eight out of ten nodes move towards east. Two nodes remains stationery during the simulation. After five seconds our algorithm checks and assigns new status to ten nodes.

The status of these ten nodes is saved in a file named "nodestatus.tr" which can be viewed in MS-Word or WordPad as shown in figure 3.

Another file is also created by the algorithm with name nodeskdc.tr which contains the nodes numbers which are selected as KDC nodes as shown in figure 4.

After making "nodestatus.tr" and nodeskdc.tr files NAM is executed and simulation runs in visual form. Figures 5, 6 and 7 shows snapshot of start and different stages of simulation.

Nodes are labeled as stationery, relatively stationery, mobile, highly mobile after five seconds. Nodes with stationery and relatively stationery status are marked with hexagon around the node in red color. Nodes marked with Hexagon are KDC nodes, as in Figure 8.

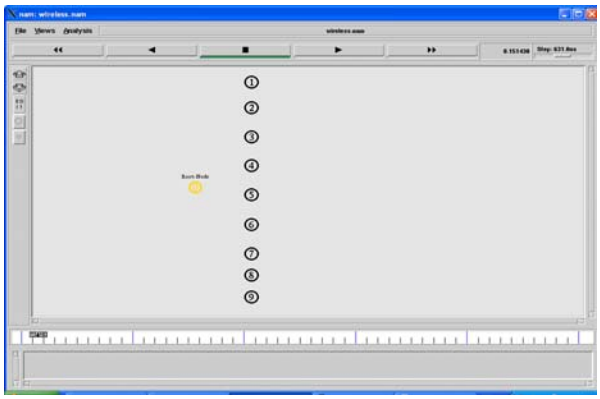

Figure 5. Start of first simulation at 0.15 second

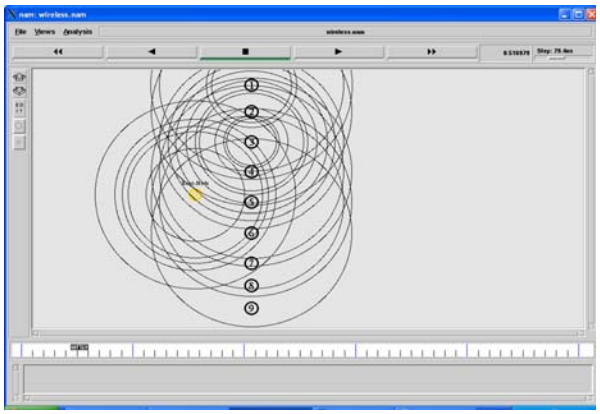

Figure 6. Snapshot of first simulation at 0.516 second

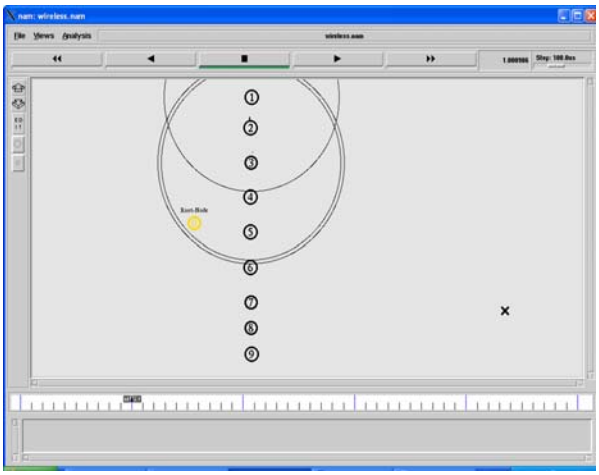

Figure 7. Snapshot of first simulation at 1 second

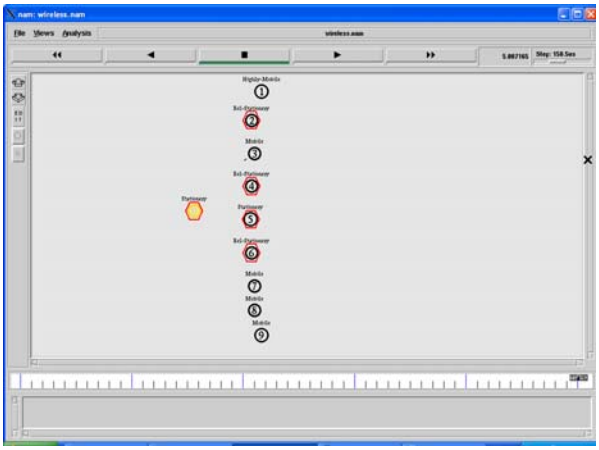

Figure 8. Snapshot of first simulation at 5 seconds

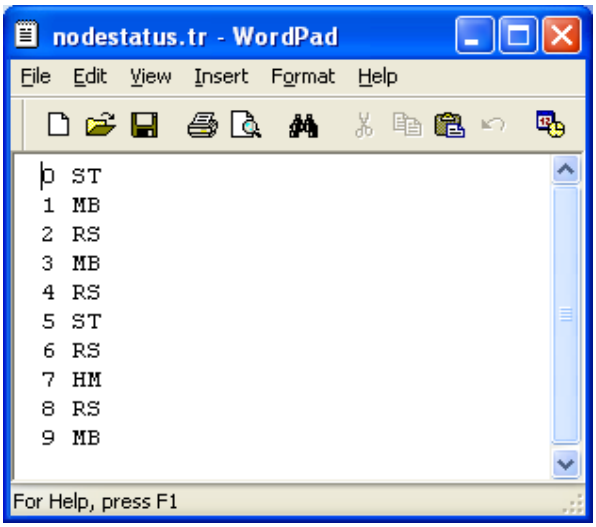

Figure 9. Contents of nodestatus.tr file

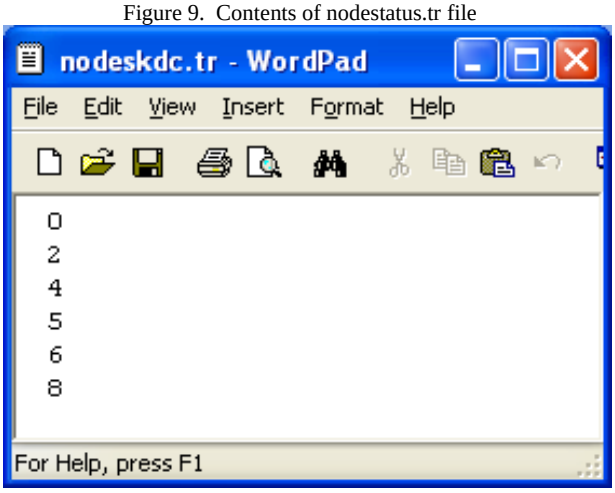

Figure 10. Contents of nodeskdc.tr file

The second simulation runs for five seconds in which ten nodes participate and eight out of ten nodes move towards east. Two nodes remains stationery during the simulation. After five seconds our algorithm checks and assigns new status to ten nodes. The status of these ten nodes is saved in a file named “nodestatus.tr” which can be viewed in MS-Word or WordPad as shown in figure 9.

The ”nodesskdc.tr” file contains six nodes selected as KDC nodes (figure 10). NAM is executed after making “nodestatus.tr” and nodeskdc.tr files and simulation runs in visual form. Figures 11, 12 and 13 shows snapshot of start and different stages of simulation. Nodes are labeled as stationery, relatively stationery, mobile, highly mobile after five seconds.

Nodes with stationery and relatively stationery status are marked with hexagon around the node in red color. Nodes marked with Hexagon are KDC nodes (see figure 14). Our simulations also shows transmission ranges of nodes in the forms of circles around the nodes and packets delivery between node 0 and node 1.

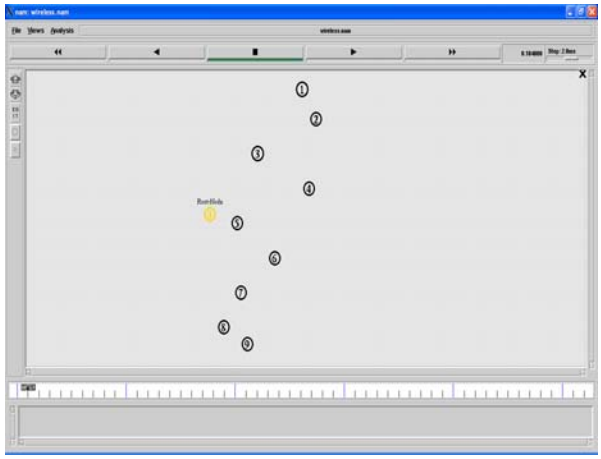

Figure 11. Start of 2nd simulation at 0.1 second

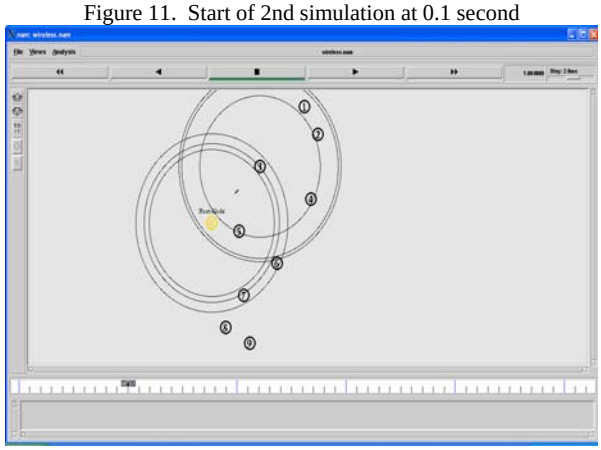

Figure 12. Snapshot of 2nd simulation at 1 second

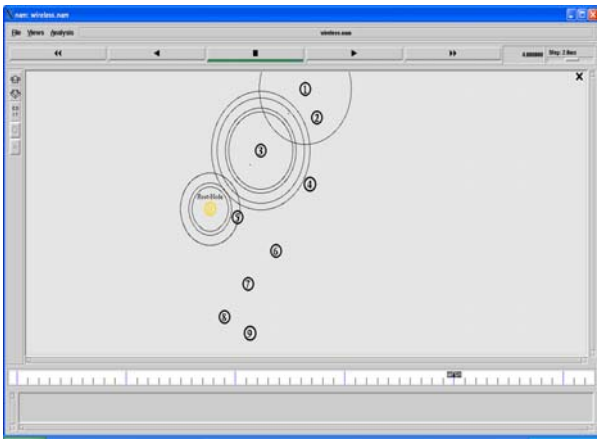

Figure 13. Snapshot of 2nd simulation at 4 seconds

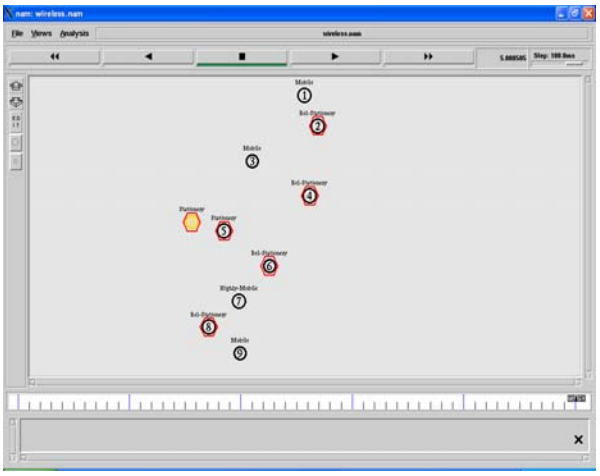

Figure 14. Snapshot of 2nd simulation at 5 seconds

6. CONCLUSION AND FUTURE WORK

The understanding of NS-2 has been thoroughly attained and sample runs have been taken. The work is in progress to simulate a variety of real world examples to test the concepts of distributed key management services. A module will be developed on the server end to provide coordinator functions.

The algorithm can be enhanced for larger number of nodes. The intelligence could be included in our algorithm to select only those nodes as KDC which are present in the communication range of root server instead of selecting all stationery and relatively stationery nodes.

REFERENCES

[1] A. Shamir, “How to Share a Secret”, CACM, 22(11): 612-613, 1979.

[2] L. Zhou and J. Z. Haas, “Securing Ad Hoc Networks" IEEE Network Magazine, vol. 13, no.6, 1999.

[3] Yi, S. and Kravets, R. 2001. “Practical PKI for ad hoc wireless networks”. Tech. rep. UIUCDCS-R-2002-2273, UILU-ENG-2002-1717. Department of Computer Science, University of Illinois at Urbana-Champaign, Urbana, IL.

[4] Yi, S. and Kravets, R. 2002a. ”Key management for heterogeneous ad hoc wireless networks”. Tech. rep. UIUCDCS-R-2002-2290, UILU-ENG-2002-1734. Department of Computer Science, University of Illinois. at Urbana-Champaign, Urbana, IL.

[5] Yi, S. and Kravets, R. 2003. MOCA: ”Mobile certificate authority for wireless ad hoc networks”. In Proceedings of the 2nd Annual PKI Research Workshop (PKI 2003).

[6] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang, “Providing Robust and Ubiquitous Security Support for Wireless Mobile Networks" ICNP, pages 251-260, 2001.

[7] Shaftab Ahmad and Syed Zubair Ahmad, 2006. “Contextual mobility profiling secure routing infrastructure for mobile ad hoc networks.” Presented in HONET 2006. Bahria University & M. A. Jinnah University Islamabad, Pakistan.

[8] S. Kurkowski, T. Camp, and M. Colagrosso, MANET Simulation Studies: The Current State and New Simulation Tools, Technical Report MCS-05-02, The Colorado School of Mines, February 2005.

[9] (2008) The NS website. [Online]. Available: http://www.isi.edu/nsnam/ns

[10] (2008) The nile website. [Online].Available: http://nile.wpi.edu/NS/

[11] (2008) The ISI Network website. [Online]. Available: http://www.isi.edu/nsnam/ns/tutorial/

[12] William Stallings, Network Security Essentials: Applications and standards, First Indian Reprint 2001, ISBN 81-7808-307-8

[13] (2008) The hpds website. [Online]. Available: http://hpds.ee.ncku.edu.tw/~smallko/ns2/mysetup_en.htm