International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 8 (2015) pp. 19715-19728

http://www.ripublication.com

A New Simulator Modelling and Real Time Implementation in Android OS for WSN

S. Gayathri[1], R.Ramesh[1], G.Rajesh[2]

[1]Electrical and Electronics Engineering, CEG, Anna University, Chennai-600025, India,
Email: gayathri.in50 @gmail.com, rramesh@annauniv.edu]
[2]Assistant Manager, IT Dept, REPCO Bank, Government of India,
Email: rajeshg66@gmail.com

Abstract

Wireless sensor networks routing travels through a wide range of network simulation technique and give different approaches in designing a network protocol. Traditional routing techniques were designed based on performance, cost, optimization, application and a well adopted environment. A new framework is proposed in which all of the above factors are taken in to consideration. The framework runs the proposed RSSPR algorithm for finding a secure shortest path. RSSPR algorithm introduces a new shortest path routing and applied digital signature algorithm (RSA) for secure transmission and reception. The proposed framework is built with cluster based topology to overcome the limitations in hardware. RSSPR is using a flooding method of route discovery and the adjacent nodes are visible to the user. The proposed method is using an application oriented approach. The advantage of this approach is user can able to add as many features as per the requirement. The RSSPR prevents the nodes from eaves dropping and ethical hacking by the implementation of digital signature algorithm.

Keywords: Simulation Technique, Routing, GUI, Cluster, Digital Signature, Java Net Beans 7.0.

1. Introduction

Several network simulators have arisen to meet the need for evaluating network scenarios before deployment. Various forms of models and implementations can emphasize different aspects of a networking system. This might include laboratory experiments and field exercises, analytical models, and other, independently developed simulations. The reason for better simulation results not only depends on performance but also depends on deployment of nodes. The classical network simulation frameworks in use are DaSSF, JiST, J-Sim, NS-2, NCTUns, OMNET++, and Ptolemy. They use a layered architecture, similar to the real protocol stack. These simulation tools include scripting, graphical support and target system. Among these factors powerful scripting and graphical support are the important criteria taken in to consideration. Hence Java is the powerful tool for scripting and also for advanced graphical user interface. Java net beans, one of the powerful java tool supports a highly application dependent operation of WSN. Java provides an excellent edition and debugging property compared to Ns-2 and OMNET++ by S. Lu1 J.A. Schormans 2008**.** . Also the power GUI provides a component based design and supports ad hoc network. Visualization effects should be more clear and understandable as mentioned by Mousavi S.M, Rabiee H. R et.al, 2007.

A new GUI is developed for WSN nodes using java for better results and optimized algorithm. One of the main reasons for developing GUI is to improve and eliminate the draw backs faced in other simulator. The complete path is shown in the graphical window. If any further advances is in need will also be accomplished using the developed GUI. The proposed RSSPR GUI using the centroid formula because of the cluster formation in placing the nodes. The X and Y coordinates are calculated using the centroid equation. The nodes are differentiated using different colours to differentiate the cluster head and gate node each one will be unique in their jobs and the cluster head plays the key role in our work as it has all the responsibilities and know the routing in and out of the clusters as it has multiple clusters in the group. Clustering involves normal nodes cluster head node and gateway node. Another important Factor in the proposed GUI is real time implementation can be feasible in implementing the GUI into real Time Ad hoc nodes. The real time ad hoc nodes are Mobile; tablet PC, Laptop and Digital note.

2. Related work

S. Lu1 J.A. Schormans [2008] proposed a new simulator (SSIM) by focusing the errors and limitations of time stepped simulation. SSIM provides a session level simulation and the frame work is modelled with respect to discrete level simulation. An event rate(ER) and progress rate (PR) is put forth for finding the simulation terminating time. An analytical approach also made to rectify the simulation error.

Mousavi S.M, Rabiee H. R et.al.,[2007] developed a new simulator and introduced the node number, position, transition, source point, destination point and transition length.

Ryad Ben-El [2007] proposed a new simulation routing method which analyze the process trace files generated by different simulators. The paper released the first version named as YAVISTA 1.0, which compares different simulators input and visualize its performance through a graphic editor. The author compares NS2 and GLOMOSIM simulator and a timeline analysis shows the error of each simulator in comparison.

Kazuki Konishi et.al.,[2005] designed a new simulator based on real time parameters like mobility change, speed and route directions. The mobility is analyzed with real time activity like pedestrian movement in the city. A conditional probability event model is introduced for different pedestrian conditions at crowded, late, hurry, staying and over staying.

Hasan et.al.,[2008] introduces a co simulator approach which is very economical compared with core simulators. The implementations of the main simulators are expensive and time consuming, hence the model inter links SIMULINK and OPNET environment. Work concentrates on a pendulum coupled with a spring controlled system using 4 sensors and two actuators. The plant is modelled using OPNET and it maintains the co simulation time. The sensor states are read by the SIMULINK model.

Ahmad Jabas et.al.,[2008] completely focus on performance analysis of internet connections of MANETs and its design issue. A new solution was found to connect MANETs to fixed IP networks. The existing models were evaluated and made a performance comparison using different parameters like route request, a route retire and a reverse route life time.

The new simulators mentioned in the literature are still facing issues like secure transmission and reception. Shortest path is the main criteria faced by these simulators hence there is a need for developing a new simulator. The new simulator should support a real time environment and hardware compatibility software. Operating system support is also a main reason that most of the simulators failed to achieve.

3. Need for Development of the New Simulator

Network simulator design needs to satisfy challenging issues like environment compatibility (topology), hardware compatibility and user compatibility. Environment compatibility deals with the topology and the protocol design. Hardware compatibility represents the implementation of the proposed design. Finally user compatibility deals with the graphical interface of the simulator. Traditional simulators are designed to meet the standard specification and neglecting the issues stated above. The proposed framework is designed using Java Net beans simulator. Java simulator provides an excellent graphical user interface and ease of use. As for as routing strategy is concerned finding the shortest path is the principal task to be considered. Hence simulators should take care of this task and to achieve it to the level of best. In our proposed simulator we have introduced a shortest path routing. The destination time and the total time also calculated. The proposed algorithm using the framework displays the status of the route establishment.

4. Need for Security

Most of the simulator routing protocols are designed to run traditional routing techniques and to meet the standard specification .Nowadays MANETS are vulnerable to various attacks like ethical hacking and eaves dropping. Apart from routing techniques the simulator should take care of the security problem. Hence the proposed simulator implements a traditional digital signature algorithm along with the routing technique.

5. Development of Customized IDE

The Net Beans IDE is written in Java and can run on Windows, OS X, Linux, Solaris and other platforms supporting a compatible JVM. A pre-existing JVM or a JDK is not required. The Net Beans platform allows applications to be developed from a set of modular software called modules. Applications based on the Net Beans platform (including the Net Beans IDE) can be extended by third party developers.

6. Components of Proposed Framework

The GUI based user window is proposed and designed with the following blocks as given in subsection. Each block is created using Java Net beans and the routing parameters are specified using Java J frame simulation environment.

6.1 Node Entry

A graphical user interface is used for choosing the number of nodes. These nodes will be placed within the range in each cell. Hence the range of each cell is fixed and its user point of view. The user will extend the range by increasing its factor in the algorithm. The GUI for the number of nodes is shown in Fig. 1.

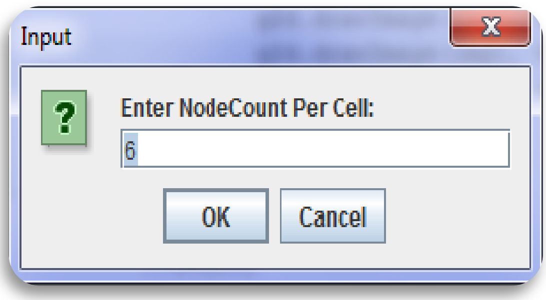

Figure 1. Node Entry

6.2 Cluster

The mobile nodes are aggregated into clusters and a cluster-head is elected. All nodes that are in the communication range of the cluster-head belong to its cluster. The simulation field is created as an interconnection of many hexagons with cluster of nodes. The reason for choosing hexagonal cluster is to accommodate the additional nodes like gateway node and cluster head. The gateway node is always placed at a distance away from centroid and the cluster head is placed nearer to the centroid. The cluster representation is shown in Fig. 2 and the centroid formula is given in equation 1 and 2. In the proposed framework centroid function is inbuilt which can be invoked from the variable centroid. This variable is separately declared in a separate class.

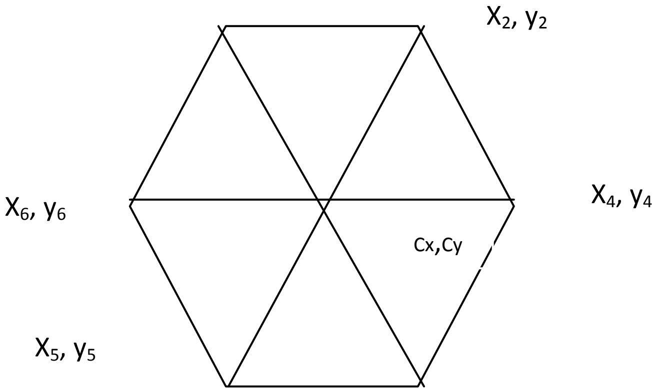

Figure 2. Cluster Topology

The centroid of a hexagon is defined by six vertices (x_0, y_0), (x_1, y_1)... (x_5, y_5) . The point of intersection of the vertices forms the centroid which is represented as

$$C_x, = \frac{1}{6A}\sum_{i=0}^{5}(x_i + x_{i+1})(x_i y_{i+1} - x_{i+1} y_i) \quad (1)$$

$$C_y = \frac{1}{6A}\sum_{i=0}^{5}(y_i + y_{i+1})(x_i y_{i+1} - x_{i+1} y_i) \quad (2)$$

Where A is the polygons signed are

$$A = \frac{1}{2}\sum_{i=0}^{5}(x_i y_{i+1} - x_{i+1} y_i) \quad (3)$$

6.3 Cluster Head

The framework built a cluster head for finding a secure shortest path. Each cluster will have a cluster head. In our algorithm the node which is placed within its cell will always try to locate its cluster head and the path is authenticated with its cluster head. The GUI for the cluster head is shown in Fig. 3. In Fig. 3 the yellow colour rectangle node present in the cluster is the cluster head node. In a dynamic network cluster head scheme can cause performance degradation due to frequent cluster-head elections, so CGSR uses a Least Cluster Change (LCC) algorithm. In LCC, cluster-head change occurs only if a change in network causes two cluster-heads to come into one cluster or one of the nodes moves out of the range of all the cluster-heads. Hence the cluster head is set near to the group's centroid.

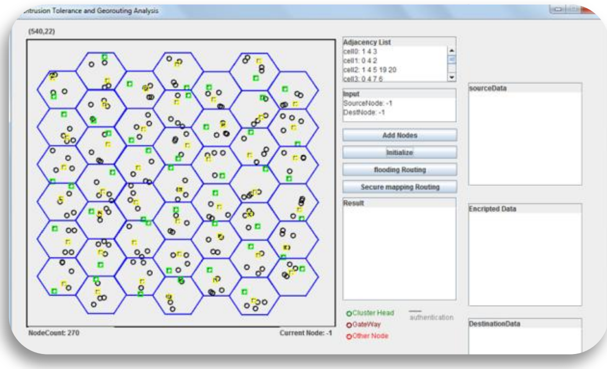

Figure 3. Cluster Head

6.4 The gateway node

Apart from the cluster head each cell is built with a gateway node. A gateway is a node that allows you to gain entrance into a network and vice versa. Usually a gateway is associated with a router. A router is a device or sometimes computer software that lets you know the next network data should be sent to next. A router can be connected to two or more networks at a time; it decides the next destination of the data based on its comprehension of the condition of the networks. A communication network with a gateway node is shown in Fig. 4. The green colour rectangle represents the gateway node.

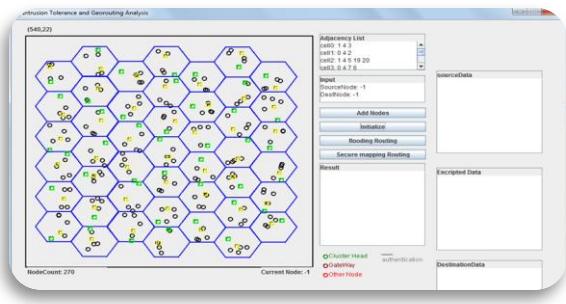

Figure 4. Gateway Node

7. Adjacency list

The GUI represents another button task which represents the adjacent cell list shown in Fig. 5. The adjacent cell addition is a user defined parameter. The user will map the adjacent cell of each cell in the window. Hence the adjacency list is created and it cannot be changed until the user map it with other cells. Adjacency is mainly used to find the shortest route as fast as possible through mapping.

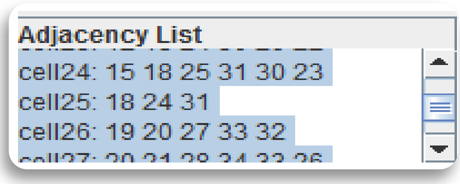

Figure 5. Adjacency List

8. Input method

The main advantage in the proposed framework is the input method. The user can choose the source and the destination in the GUI window rather within the program. Hence user can able to change the source and the destination as per the requirement. The task is done by four functions a) mouse clicking b) mouse exited c) mouse pressed and d) mouse released. The mouse clicking event is the most convenient approach in choosing the input when compared with program input. The input window is shown in Fig. 6

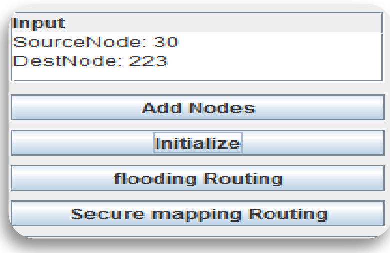

Figure 6. Input Method

9. Routing strategy

When the network topology changes the nodes propagate update messages throughout the network in order to maintain consistent and up-to-date routing information about the whole network. The traditional routing protocols differ in the method by which the topology change information is distributed across the network and the number of necessary routing-related tables. Hence a new protocol named as RAMESH Secure Shortest Path Routing Algorithm (RSSPR) is introduced. Proposed algorithm finds its shortest path using Table-driven routing protocols; each node maintains one or more tables containing routing information to every other node in the network. All nodes update these tables so as to maintain a consistent and up-to-date view of the network

10. Proposed routing algorithm

10.1 Ramesh Secure Shortest Path Routing (RSSPR)

Proposed RSSPR introduced a secure shortest path routing using Digital signature algorithm (RSA). The source of the packet transmits the packet to its cluster-head. From this cluster-head, the packet is sent to the gateway node that connects this cluster-head and the next cluster-head along the route to the destination. The gateway sends it to that cluster-head and so on till the destination is reached. The destination cluster-head then transmits the packet to the destination. The route discovery in RSSPR is divided into RSSPR Routing table entry, RSSPR route discovery and RSSPR path display.

10.2 RSSPR Routing Table

In the proposed RSSPR algorithm routing table creation is the first section in route discovery process. The routing table is created by finding the Euclidean distance between each node. Each node maintains a list of adjacent nodes.

10.3 RSSPR Route Discovery and Path Display

Route discovery in RSSPR is done by checking the neighbour node distance. The neighbour node discovery is done by finding the next node which got the shortest distance. The shortest distance is compared by the nodes which are within the transmission range. RSSPR algorithm is doing iteration so that the neighbour node should not already exist in the path. The path will be broken if the route discovery finds the neighbour node twice. The neighbour node with the shortest distance is always considered as the next node. RSSPR algorithm displays the path in the GUI window. Fig. 7 indicates the route discovery and its path displayed by the RSSPR algorithm.

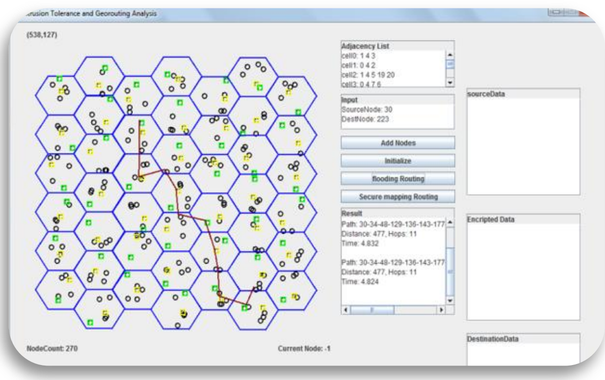

Figure 7. Route Discovery and Path Display

10.4 Routing Information in RSSPR

Routing information like time duration, no of hops, distance and path sequence for the above route discovery from source node 30 to the destination node 223 as mentioned in above Fig.7 is represented in Table 1.

Table I: Routing Table for Route Discovery

Routing Entries	Routing Information
Path	30-34-51-72-137-136-177-178-183-216-227-223 success
Distance	440
No of Hops	11
Time	4.883

10.5 Authentication using Digital Signature in RSSPR

The routing strategy and the route discovery methods as mentioned in section 2 is a normal routing technique. The route travels through a path which could be attacked by any malicious activity. To prevent any malicious activity the route discovery should be authenticated by any cryptographic method. The traditional digital signature algorithm RSA is for secure transmission and as well as reception as shown in Fig. 8**.**

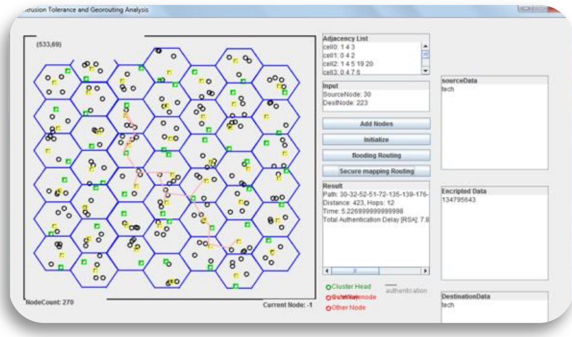

Figure 8. Secure Route Discovery Using RSA Algorithm

11. Routing table for digital signature in rsspr

The routing as shown in Table 2 clearly explains the secure routing with the encrypted and the decrypted values. In RSSPR secure transmission is done by sharing of private key with source node and the cluster head. The key generation takes place as per the steps explained in section 5.1.The decrypted message will also be displayed in the GUI window with the name mentioned as destination data in the right extreme corner. The difference between the normal route discovery and the secure route discovery shows the difference in the path taken by the nodes. The new path is different from the path shown in Fig. 7. Hence the destination node which shares this public key will decrypt the message using its own private key thereby creating a secure environment for good transmission and reception. This is implemented in the IDE which is shown in Fig. 8**.** The pink colour path explains the secure routing.

Table II: Routing Table for Digital Signature

Routing Entries	Routing Information
Path	30-35-48-52-73-143-139-146-184-187-227-223 success
Distance	400
No of Hops	11
Time	16.48 ms
Total Authentication Delay	7.59 ms
Source Data	Tech
Encrypted Data	381551100
Destination Data	tech

12. Real time implementation in android OS

The proposed GUI is implemented in real time using client –server communication. The traditional client- server model does not prove IP address based detection of mobile nodes. In our method we have used IPV4 address for each system or nodes as it is unique for the security purpose. Java Eclipse software is used for this client - server module. Among whole data access architecture we have used our GUI for secure login and for Authentication. The mobile node that we have assumed is laptop or android mobile consists of any version .We have established the developed client-server connection between android mobile to android mobile and laptop to android mobile which is successfully connected. In this connection we use the IPV4 address which is Public IP address which is automatically assigned in the server and should be entered in the address bar and then it is connected. Once connection is established the proposed GUI window is opened in the laptop node. Since the mobile nodes is client we have used laptop as server and the GUI for the android is made to open in the laptop using java eclipse software. The proposed client-server architecture will have a proper login and authentication using RSA algorithm and the GUI can be verified using' n' no of nodes.

12.1 IP address

The IPV4 (8 bit addressing) address is used for the connectivity and secure login between the server and the client nodes and due to the larger network we use the class c division in IP address and in later stage the IPV6 concept (16 bit addressing) is developed means we provided for that to in the application with little change in the server side.

12.2 Server Side Page Creation and Authentication Using RSA

The main agenda in creating a page and authentication in server side is to create a login page for the wireless client that we are going to connect through wireless media. The main reason is to show the created cryptographic algorithm in real time implementation consists of the My SQL database which can store data any files in any format and it can be accessed anywhere through registered clients or ad hoc nodes they can download or upload etc. The whole procedure is shown in Fig . 9.

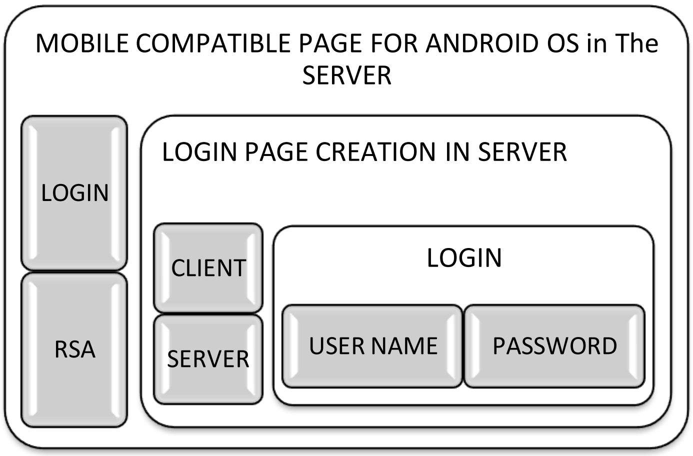

Figure 9. Server Side Page Creation and Authentication using RSA

12.3 Login Page Creation in ANDROID MOBILE using JAVA ECLIPSE

The login page in android is developed through eclipse software and in these android application we have to register first by communicating through the server ipv4 address after registering we can access n no of times and in these application we have provided dual communications for the better results i.e. Bluetooth and GPRS. The complete design module is shown in Fig . 10**.** As per client requirements and distance covered we can use accordingly. As soon as the android application is switched on the mobile node is communicated by verifying the password with the server side if it fails there will be login error. The authentication is done by running RSA in server side**.**

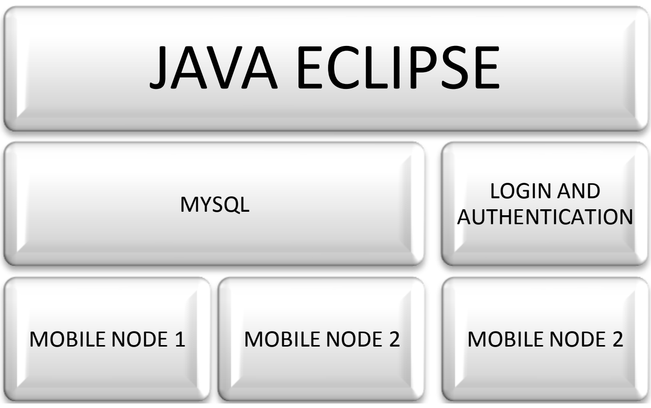

Figure 10. Login Page Creation in Android Mobile Using Java Eclipse

13. Android stimulator SDK

We register our mobile using server IP address for authentication and verification for the Security Purpose. In this screen as shown in Fig. 11 any alphabets and numbers can be given as inputs but it is case sensitive as it is highly secured.

Figure. 11. Register of Android Mobiles Using IP address

13.1 File Uploading Screen and Downloading Screen

After authenciation and verification of Password it will directly connected to the Server system through IP address and GSM .and This Process can mutually done in the Server as well as the Nodes(Mobiles) and There is a option to Choose File While clicking the Choose file it will automatically goes to the Gallery where we can choose any type of file and we can upload any fie like JPG,MPEC,MP3 and from the mobile it will be directly connected to the server system is shown in Fig. 12.

Figure 12. File Upload and File Download

This screen has two steps in the first step is used to scan the Bluetooth devices in the surroundings and it will detect them and after the proper authentication it will pair with them and the second step is by clicking connect we can transfer any file from the devices in them. The data transfer screen is shown in Fig. 13.

Figure 13. Transfer of Data between the nodes using Pair detector

14. Conclusion

The proposed work concentrates on several issues faced in the real time environment and put forth a new GUI model for the wireless sensor networks. Future work is going to be made on a specific attack in ad hoc networks like black hole, wormhole etc. Advanced cryptographic methods will be implemented to ensure secure transmission against the specific attack. The normal flooding routing technique will be improved with a better optimization routing technique.

15. Acknowledgement

Author thanks the faculty members for their full support and the continuous encouragement in completing the proposed work and for extending it to the near future. The author would like to acknowledge financial support of Council of Scientific and Industrial Research (CSIR), Govt of India.

16. References

[1] S. Lu1 J.A. Schormans**.** 2008**.** Time-stepped approach for accelerated simulation of mobile ad hoc networks IET Communication's 609–620.

[2] S.M. Mousavi, H.R Rabiee, Moshref.M and Dabirmoghaddam A. 2007. MobiSim: A Framework for Simulation of Mobility Models in Mobile Ad-Hoc Networks International Conference on Wireless and Mobile Computing (WiMOB), 82.

[3] Ryad Ben-El ,Kezadri Farouk Kamoun. 2007. Towards MANETs simulators massive comparison and validation. Personal Indoor and Mobile Radio Communications (PIMRC), 1-7.
[4] Viet Thi Minh Do, Lang Xie, Øivind Kure. 2011. Performance Evaluation of nsclick Simulator for Mobile Ad Hoc Network International Conference on Advanced Computing Technologies(ICACT), 736-741.
[5] Robatmili , Mozhdeh Abrishami, and Ali Movaghar. 2008. A comparison of various routing protocols in Mobile Ad-hoc Networks (MANETs) with the use of Fluid flow simulation method. International Conference on Wireless and Mobile Communications (ICWMC) , 260-267.
[6] Kazuki Konishi, Kumiko Maeda, Kazuki Sato, Akiko Yamasaki, Hirozumi Yamaguchi, Keiichi Yasumoto, and Teruo Higashino. 2005. MobiREAL Simulator– Evaluating MANET Applications in Real Environments , Modeling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS) IEEE 499-502 .
[7] Makoto Ikeda, Elis Kulla, Masahiro Hiyama, Leonard Barolli, Makoto Takizawa and Rozeta Miho . 2010. A Comparison Study Between Simulation and Experimental Results for MANETs International Conference On Network- Based Information Systems (NBIS), 317-378.
[8] Kumiko Maeda Takaaki Umedu Hirozumi Yamaguchi Keiichi Yasumoto and Teruo Higashino. 2006, "MobiREAL: Scenario Generation and Toolset for MANET Simulation with Realistic Node Mobility", Mobile Data Management (MDM), 55.
[9] M.S. Hasan, H. Yu, A. Carrington, T.C. Yang. 2008 .Co-simulation of wireless networked control systems over mobile ad hoc network using SIMULINK and OPNET, IET Communications, 1297–1310.
[10] Junghoon Lee.2007. An analytical modelling approach for a large scale mobile ad hoc network. Military communications conference(MILCOM), 1-4.
[11] M. Ruiz, Francisco J. Ros, Antonio Gomez-Skarmeta. 2005. Internet Connectivity for Mobile Ad Hoc Networks: Solutions and Challenges IEEE Communications Magazine 118-125.
[12] Ahmad Jabas , Rama M. Garimella , Ramachandram.S, 2008. Proposing an Enhanced Mobile Ad Hoc Network Framework to the Open Source Simulator NS2 Mosharaka International Conference on Communications, Computers and Applications (MIC-CCA) 14-19.