International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

Improving Performace of System using ECC and Detection of Selfish Node Attack using Aodv Protocol

Dinesh S Jadhav†* and V. S. Wadne†

†JSPM's Imperial College of Engineering & Research Wagholi, Pune, India

Accepted 14 Feb 2016, Available online 02 March 2016, **Vol.6, No.2 (April 2016)**

Abstract

This paper represents secure protocol based on Intrusion detection system for Spontaneous wireless ad hoc network. It is complete self configured system. It does not require any central server or any external infrastructure to communicate. We are using some security protocol to make system more secure. We are authenticating the each node in the network. Trust is formed by IDC exchange protocol and visual contact between the users. This system checks for IP duplication in the network. This system is based on symmetric/ Asymmetric cryptography scheme. The data, messages or exchange of keys will be done in encrypted form. We are using AES for symmetric key cryptography and RSA/ECC for asymmetric key cryptography. Intrusion detection system is one more protocol we have implemented to make system more secure than existing one. In this paper we are detecting selfish node attack and we have proposed algorithm for detection of selfish node in the network.

Keywords: *Spontaneous Network, IDS, AODV protocol, Selfish Node*

1. Introduction

There is exponential growth in the field of wireless networking in today's world. This growth is due to the mobility offered to the users. Users can access any information from anywhere. Flexibility and scalability is offered more to the users. (R Lacuesta *et al*, 2013, J Lloret *et al*, 2013, Miguel Garcia *et al*, 2013)

Spontaneous networking is nothing but the group of people at closed location communicates with each to share resources and services between them for limited time and then leave the network. We are using MANET network to form a ad hoc network. In spontaneous wireless ad hoc network it do not require any central authority. It also does not require any external infrastructure to communicate or to connect each other. Due to this property it is low cost network.

We are forming one MANET network for our system. MANET (Mobile Ad hoc Network) is nothing but a wireless type of network. MANET is set of mobile nodes connected for small period of time to communicate and then leave the network and it do not require any external infrastructure or any central authority. It is complete self-configured network (Manjeet Singh *et al*, 2013, Gaganpreet Kaur *et al*, 2013).

The main objective of MANET is to provide an instant service to user because it is infrastructure less. It should be light weight protocol because it is implemented in the devices like laptops, Mobiles and PDA's so it need to be light weight protocol because these devices have less memory capacity (R Lacuesta *et al*, 2013, J Lloret *et al*, 2013, Miguel Garcia *et al*, 2013).

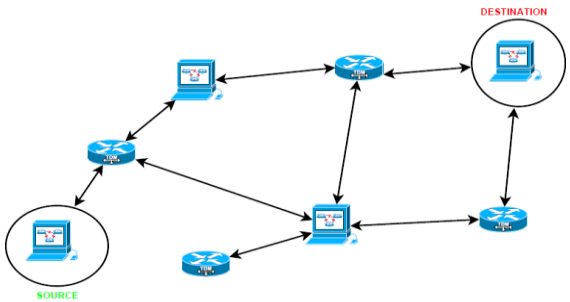


Figure 1: Structure of MANET

In infrastructure less networks security is less. When there is no central authority to manage the network it means network is vulnerable to attacks. So security is important issues in this type of network. We are using some protocol in our system to make system more secure. Some security level protocols are as follows:

- Registration and certificate
- Authentication
- IDC Exchange
- IP duplication checking for authentication
- Symmetric/ Asymmetric key cryptography
- Intrusion Detection System

*Corresponding author: **Dinesh S Jadhav**

Above are some protocols used in our system to make system more secure. Registration of each user in the network is done. Certificate is created for each user to form a trust. Authentication of each user is done. IDC is one of the protocols we have taken from the vehicular network systems. IDC is nothing but one type of identity card which having some private and public components. Public components contains photograph, public key, User ID, Signature. Private components contain private key and all secret data. IDS is exchanged to form a trust between users (J. Sun *et al* 2010, C. Zhang *et al*, 2010, Y. Zhang *et al*, 2010, Y. (Michael) Fang *et al*, 2010).

IP duplication is also one security protocol we are using to authenticate node using IP address. This check for duplicate IP in the network[3]. Symmetric and asymmetric key scheme is used in order to exchange the network data and messages. We are using ECC because of its high performance over small devices.

To enhance the security of a system we are implementing Intrusion detection system (IDS). We are working to concentrate on selfish node attack in the network. This detects the selfish node in the network and deletes that node from the network.

Studying scholars work we are proposing the Intrusion Detection System to detect the selfish node in the network. We are also comparing the performance of ECC algorithm over RSA. ECC gives high performance over RSA because 192 bit key size of ECC provides equal security over 2048 bit key size of RSA. ECC is better for mobile and small devices which have less battery and memory (J. Lopez *et al*, 2000, R. Dahab *et al* 2000).

We propose AODV routing protocol in which we are proposing selfish node detection algorithm. AODV protocol work as there are 4 types of messages are sent in AODV protocol:

- Hello message
- RREQ
- RREP
- RERR

Hello message is sent to all the nodes in the network to tell them am alive. RREQ message is sent to route request. RREP message is sent to reply from destination to source. Whenever there is error to forward a packet RERR message is sent.

Paper organized as section II gives studied work of scholars and in section III we explained the proposed work such as problem statement, architecture, and results. Section IV gives conclusion and references which are used for this work.

2. Literature Survey

Following are some scholars work studied during study and implementation of this project. This work is helpful to propose our system. We have taken some protocols from these scholars work and proposed one collaborative system.

In (L.M. Feeney *et al*, 2001, B. Ahlgren *et al*, 2001) author L. Fenny explained what is spontaneous ad hoc networking is. Author gives significant definition of spontaneous ad hoc networking. Spontaneous network is infrastructure less and it does not require any central administration means spontaneous ad hoc network is self configured type of network. Explains applications of spontaneous networking how collaborative work can be done simply securely using spontaneous networking. Five challenges are given in spontaneous networking and there solutions are given by the author.

In (Y. Xiao *et al* 2007, V.K. Rayi *et al*, 2007, B. Sun *et al* 2007, X. Du *et al* 2007, F. Hu *et al* 2007) author Y. Xiao explained what actually the wireless sensor networks are. Due to wide use of wireless sensor network in industries sensitive data can be sent. So security should be strong to send receive the data. Various key management schemes are used to secure the wireless sensor network and studied their results. Performance of ECC over RSA is compared how ECC is better where battery is less and devices have less memory and CPU size. Key management scheme should be strong in order to secure the data transmitted to and from wireless sensor networks.

In (R. Lacuesta *et al*, 2005, L. Penaver *et al*, 2005) author R. Lacuesta describes about the IP address configuration. Usually in the networks IP address are given or managed by the host. By DHCP, DNS protocols this IP configuration is done. Means in normal network IP address can be configured by server. But in networks like home network, aero plane network, vehicular network there is no server these networks does not have any central administration. Author gives solution for this problem by configuring node itself. IP address configuration is done itself.

In (J. Sun *et al* 2010, C. Zhang *et al*, 2010, Y. Zhang *et al*, 2010, Y. (Michael) Fang *et al*, 2010) author J. Sun explained the detail architecture of VANET. This network is very useful for the vehicles and misuse of this causes very serious consequences. To avoid and make secure vehicular system author proposed the new Identity based privacy preserving approach. This identity card contains private and public components. Public components contain name, photograph and email address and key. This Identity card approach we are using in our project to form a trust between users.

In (J. Lopez *et al*, 2000, R. Dahab *et al*, 2000) J. Lopez explained performance of ECC algorithm. Performance of ECDSA over RSA and DA. Author taken some test and calculated time taken to execute the algorithms. Performance of ECC over other public key cryptography algorithms.

In (E. Perkins *et al*, 1998) C. Perkins present Ad hoc on demand distance vector routing algorithm (AODV) new routing algorithm for ad hoc network. In AODV each mobile node act as a router and routes request on demand means it is not reliance on periodic advertisement. This is algorithm useful for network which is self configured. It is loop free route algorithm

and repairs all broken links. It is scalable for large mobile nodes to form ad hoc network.

In (Manjeet Singh *et al*, 2013, Gaganpreet Kaur *et al*, 2013) author surveyed some attacks which are faced in MANET network. As MANET have some advantages of not to having central administration it also have some disadvantages. Network without central administration is vulnerable to attacks. In this paper author have listed some attacks in MANET.

In (S. Gallo *et al*, 2004, L. Galluccio *et al*, 2004, G.Morabito *et al*, 2004) author S. Gallo explains about service discovery. In order to communicate in spontaneous network node will have to discover neighbor. Velocity of discovery is paid in energy consumption. Here they achieve high velocity within less energy. They explained the haunting process. Haunting process type are as follow:

- Inquiry
- Inquiry scan
- Doze

These 3 types of haunting process are explained.

One author describes Spontnet, our prototype implementation of a simple ad hoc network configuration utility based on these ideas. Spontn *et* allows users to distribute a group session key without previous shared context and to establish s h a d namespace. Two applications, a simple web server and a shared whiteboard, are provided as examples of collaborative applications that could be useful in a spontaneous networking environment.

3. Implementation Details

A. Problem Statement

In existing system they do not give a security against attacks. We are targeting one of the attack to secure our Spontaneous wireless ad hoc system designing Intrusion Detection System. We are focusing following points to make system performance better.

1) Use of ECC over RSA algorithm to increase performance.
2) Design IDS to detect the selfish node in the spontaneous Network to enhance the security.

B. Mathematical Modeling

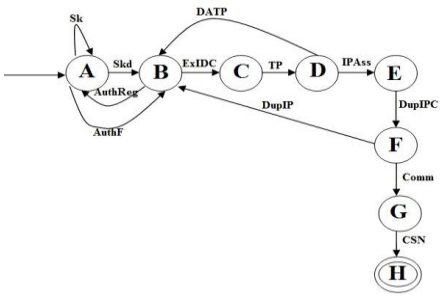


Figure 2: System Modeling

A deterministic finite automaton M is a 5-tuple, (Q, ∑, δ, qo, F) consisting of

- A finite set of states (Q)={A, B, C, D, E, F,G,H}
- A finite set of input symbols called the alphabet(∑)={Sk, Skd, AuthReg, AuthF, ExIDC, TP, DupIPC, DupIP, Comm, CSN}
- A transition function (δ: Qx∑→Q)={ }
- A start state (qo € Q)={q0}
- A set of accept states (F ⊆ Q)={q7}

Where,
Sk = Session key generation
Skd = Session key Distribution
AuthReg = authentication and registration
AuthF = Authentication fail
ExIDC = IDC Exchange
TP= Transmission protocol Agree
DNTP = do not agree TP
IPAss = IP assignment
DupIPC = IP Duplication Check
DupIP = Duplicate IP Exit
Comm = Start Communication
CSN = Check for selfish Node.

Table 1 Delta Representation

State/ δ	Sk	Skd	AuthReg	AuthF	ExIDC	TP	DNTP	IPAss	DupIPC	DupIP	Comm	CSN
A	A	B	Ø	B	Ø	Ø	Ø	Ø	Ø	Ø	Ø	Ø
B	Ø	Ø	A	Ø	C	Ø	Ø	Ø	Ø	Ø	Ø	Ø
C	Ø	Ø	Ø	Ø	Ø	D	Ø	Ø	Ø	Ø	Ø	Ø
D	Ø	Ø	Ø	Ø	Ø	Ø	B	E	Ø	Ø	Ø	Ø
E	Ø	Ø	Ø	Ø	Ø	Ø	Ø	Ø	F	Ø	Ø	Ø
F	Ø	Ø	Ø	Ø	Ø	Ø	Ø	Ø	Ø	B	G	Ø
	Ø	Ø	Ø	Ø	Ø	Ø	Ø	Ø	Ø	Ø	Ø	H
H	Ø	Ø	Ø	Ø	Ø	Ø	Ø	Ø	Ø	Ø	Ø	Ø

C. System Architecture

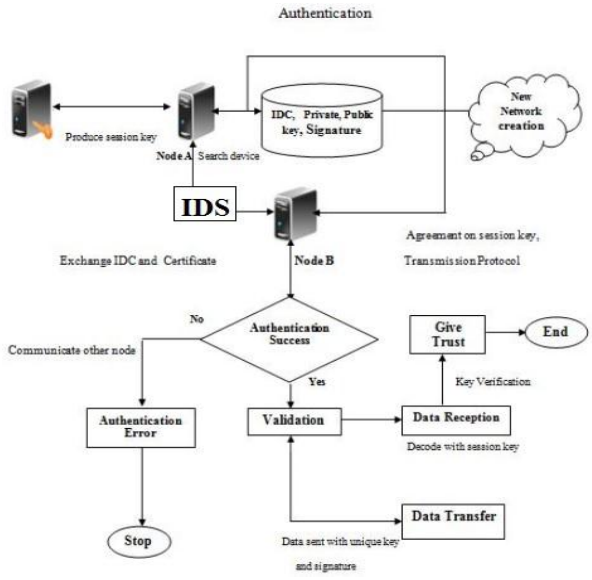


Figure (a)

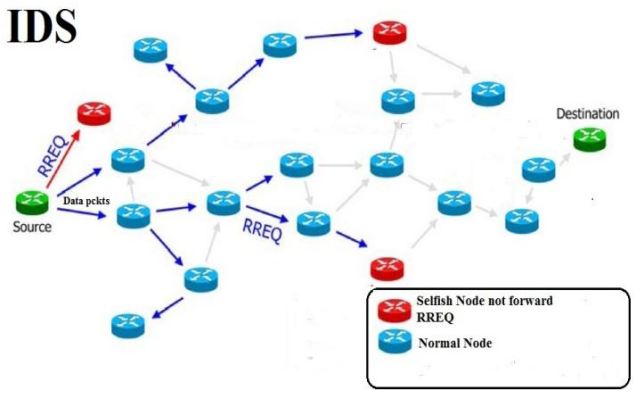


Figure (b)

Figure 3: System Architecture

1) AODV Protocol

In AODV protocol every node in the network will send four types of messages in network.

- Hello message
- Route Request (RREQ)
- Route Replay (RREP)
- Route Error (RERR)

Hello message is send by the each node in the network to all the node in the network to tell them that I Am alive. Whenever source sends packets to destination. Source will send RREQ to neighbor and these neighbor will forward RREQ to their neighbor till destination will not reach and entry will be made every time in Router table. When destination reach RREP message will be send in reverse order till source will not reach. Whenever some error occurred at any stage RERR message will be sent.

2) Selfish Node Behavior

Node is selfish node when it gets all the benefits from network and do not cooperate in network to save resources and battery power and bandwidth. The selfish node will not cooperate with neighboring node. Selfish node will not forward the packets or only sends some packets in which it interested. Referring this behavior selfish node is classified as follows:

• Do Not Forward RREQ Messages:
Selfish node will not forward the incoming route request messages from the neighbor.
• Do not send Hello messages:
Selfish node will not send hello message and hide itself from being part of routing path.
• Do not forward data packets:
Selfish node will not forward the information packets an act as a selfish.
• Do not forward route replay (RREP) messages:
The messages coming from destination node to intermediate node the selfish node will not forward these messages to neighbors.

In this paper we are focusing to detect two types of behavior of selfish nodes. Do not forward RREQ messages and do not forward Data packets. Algorithms for these are as follow.

D. Algorithms

1) Algorithm for new node connection

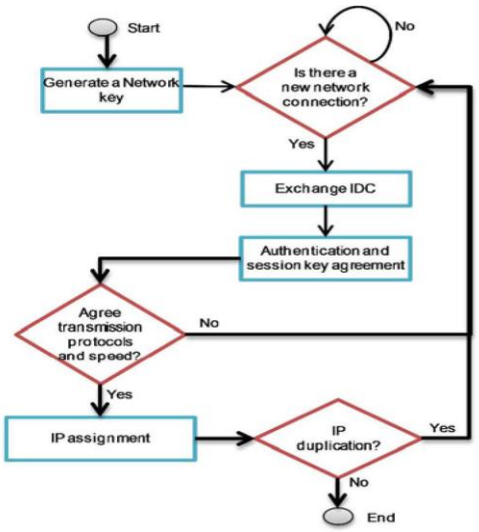


Figure 4: Algorithm for new node connection

2) Algorithm for new network creation

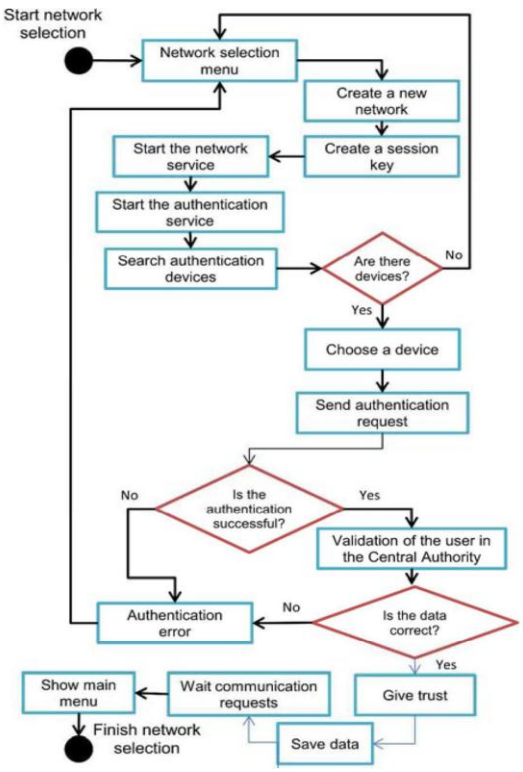


Figure 5: Algorithm for new network Creation

3) Algorithm for RREQ Checking Node

Step 1 Broadcast the RREQ messages to its neighbors
Step 2 Record the information of the neighbors who has
rebroadcast the same RREQ message
Step 3 After waiting for a period of time, it checks it's the neighbors recorded in routing table.
Step 3.1 IF
A neighbor has rebroadcast the same RREQ message
THEN
This neighbor is identified to a normal node
ELSE
The neighbor is identified to a selfish node who does not forward RREQ messages.

1. The algorithm for RREQ checked node:

STEP 1 If the RREQ checked node receives a RREQ messages sent by the RREQ checking node.

STEP 2 Record the source address and the identification
of this RREQ message and rebroadcast the RREQ message.

STEP 3 Change the role to be a RREQ checking node and perform the works of the RREQ checking node.

2. The algorithm for data checking node:

Step 1. Create a Data checking packet and fill its address
into the destination field in this packet.
Step 2. Transmit the Data checking packet to the data checked node.
Step 3. After waiting for a period of time, it must check whether the data checked node sends back the data checking packet to the data checking node or not.
Step 3.1. IF
The data checking packet has been sent back by the data checked node to the data checking node.
THEN
The data checked node is identified to a normal node.
ELSE
The data checked node is identified to a selfish node who does not forward data messages.

3. The algorithm for data checked node:

Step 1. After received a data packet, the data checked node will check this data packet whether the data
packet is a data checking packet or not.
Step 2. IF
The address of the destination field in this data packet is the same as the data checking node's address.
THEN
This data packet is a data checking packet and the checked node must send it back to the data checking node.
Change its role to be a data checking node and perform the checking works of the data checking node.
ELSE
Forward the data packet to next node in the reverse transmission path.

4. Experimental Evaluation

We have developed this system in java technology. We firstly search the node in the network then list of the node will be there. We create on hotspot network so that everyone can see us. By forming trust we can start communication between node securely. All the data sent will be in encrypted form and receiver has to decrypted the data using key sent by user.

We are also providing security to the system by detecting selfish node in the network. Suppose any node may behave selfish in the network our system will detect that node. This part we done one single machine as simulation.

We have used java platform to develop this system we requite net bins to run the program an jdk 1.7 or more to run this program.

System Requirements:

1) Software requirement

- JDK 1.7 above.
- Net Bins
- SQL SERVER 2008
- Connectivity.

2) Hardware requirements

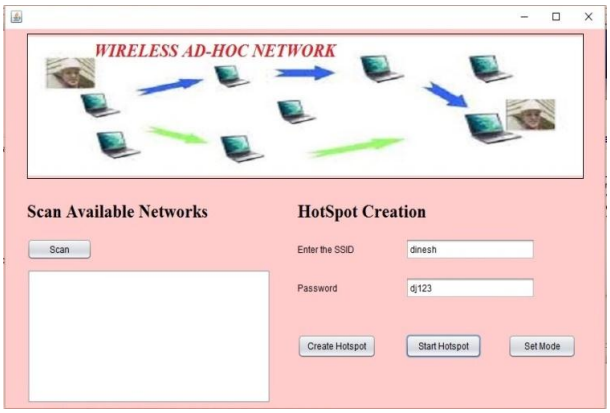
- Two or PC with suitable configuration.

3) Operating System

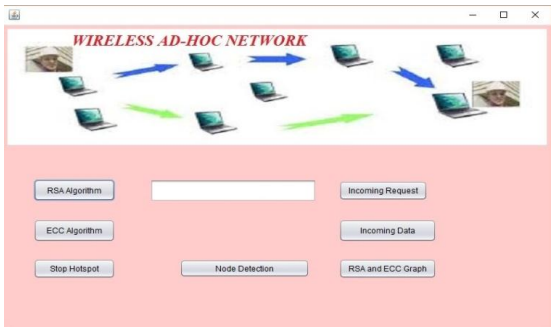
- Windows 7 or higher.

E. Results

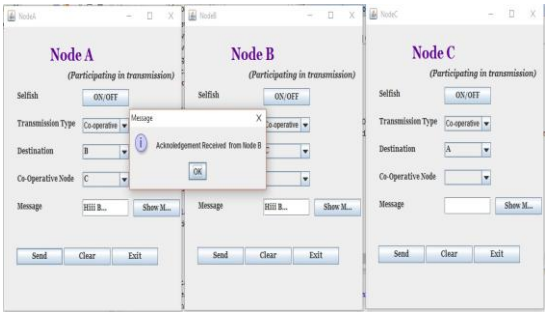
Following table and snapshots shows the result for time taken for generation of key and time taken to encrypt a message. We have shown comparison between ECC and RSA. Table gives the ECC gives less time than RSA and small key size of ECC gives similar security as RSA.



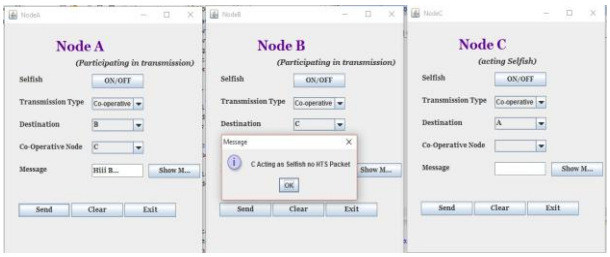
Snapshot No1: Network formation



Snapshot No 2: RSA vs ECC



Snapshot No 3: Message sent acknowledgment



Snapshot No 4 Selfish Node detected

Table 2 Comparison of ECC and RSA

Public Key Algorithms	Key Size	Time (millisecond)
RSA key generation	512	11.03
RSA key generation	1024	152.14
ECC key generation	192	8.34
RSA Encryption	512	192.4
ECC Encryption	192	187.47

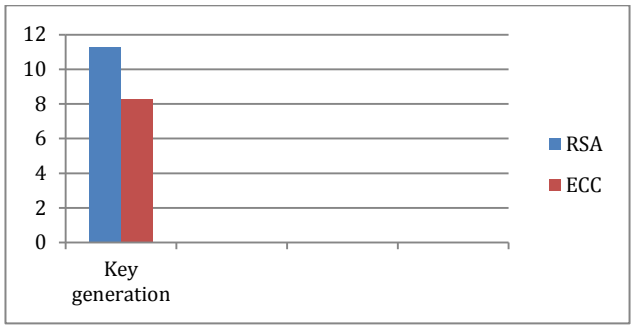


Figure 6: Comparison of RSA and ECC for key generation

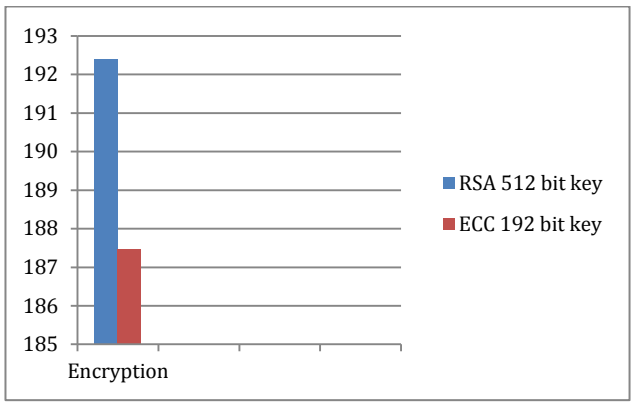


Figure 7: Comparison Of RSA and ECC to Encrypt data

Expected values for memory utilization

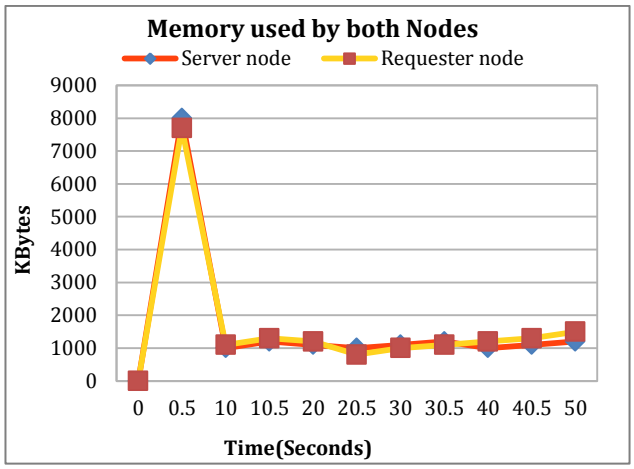


Figure 8: Expected result for memory utilization by nodes

Conclusion

Spontaneous wireless ad hoc network have some advantages like it is self configure it does not require any central authority and central server. As advantages it has some disadvantages such as security issues. I have taken it as problem and solved the one of the vulnerable attack of selfish node. Using proposed algorithm we can detect the selfish node in the network.

We have implemented system successfully and we are getting 30% of performance better than existing system. We have implemented selfish node detection using AODV protocol. The selfish node can be detected very successfully.

In security as well as in performance we have made system very secure and fast.

References

L.M. Feeney, B. Ahlgren, and A. Westerlund (June 2001), Spontaneous Networking: An Application-Oriented Approach to Ad-hoc networking, IEEE Comm. Magazine, vol. 39, no. 6, pp. 176-181.

Y. Xiao, V.K. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway (Sept. 2007), A Survey of Key Management Schemes in Wireless Sensor Networks, Computer Comm., vol. 30, nos. 11/12, pp. 2314-2341.

R. Lacuesta and L. Pen˜ aver (July 2005), IP Addresses Configuration in Spontaneous Networks, Proc. Ninth WSEAS Int'l Conf. Computers (ICCOMP '05).

J. Sun, C. Zhang, Y. Zhang, and Y. (Michael) Fang (Sept. 2010), An Identity- Based Security System for User Privacy in Vehicular Ad Hoc Networks, IEEE Trans. Parallel and Distributed Systems, vol. 21, no. 9, pp. 1227-1239.

J. Lo´pez and R. Dahab (May 2000.), Performance of Elliptic Curve Cryptosystems, Technical Report IC-00-08

C. E. Perkins (1998), Ad hoc On-Demand Distance Vector (AODV) Routing, RFC 3561, IETF Network Working Group.

Manjeet Singh, Gaganpreet Kaur (June 2013) A Surveys of Attacks in MANET, RFC 3561, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 6.

R. Lacuesta, J. Lloret, M. Garcia, and L. Penalver (2010), A Spontaneous Ad-Hoc Network to Share WWW Access, EURASIP J. Wireless Comm. and Networking, vol. 2010, article 18.

FIPS 180-1 - Secure Hash Standard, SHA-1 (2012), National Institute of Standards and Technology, http://www.itl.nist.gov/fipspubs/fip180-1.htm, Feb. 27.

S. Gallo, L. Galluccio, G.Morabito, S. Palazzo (October 4-6, 2004),Rapid and Energy Efficient Neighbor Discovery for Spontaneous Networks,MSWiM'04, Venezia, Italy

M. Feeney, B. Ahlgren, A. Westerlund, and A. Dunkels (Oct. 2002), Spontnet: Experiences in Configuring and Securing Small Ad Hoc Networks, Proc. Fifth Int'l Workshop Network Appliances.

R Lacuesta, J Lloret, Miguel Garcia (April 2013),A Secure Protocol for Spontaneous Wireless Ad Hoc Networks Creation, IEEE transactions on parallel and distributed systems, Vol. 24, No. 4