RTOS BASED SECURE SHORTEST PATH ROUTING ALGORITHM IN MOBILE AD- HOC NETWORKS

R. Ramesh[1] and S. Gayathri[2]
[1] Department of Electrical and Electronics Engineering, Anna University, India
rramesh@annauniv.edu
[2] Department of Electrical and Electronics Engineering, Anna University, India
gayathri.in50@gmail.com

ABSTRACT

Increase of number of the nodes in the wireless computing environment leads to different issues like power, data rate, QoS, simulators and security. Among these the security is the peak issue faced by most of the wireless networks. Especially networks without having a centralized system (MANETS) is facing severe security issues. One of the major security issues is the wormhole attack while finding the shortest path. The aim of this paper is to propose an algorithm to find a secure shortest path against wormhole attack. Existing algorithms are mainly concentrated on detecting the malicious node but they are hardware specific like directional antennas and synchronized clocks. But the proposed algorithm is both software and hardware specific. RTOS is included to make the ad hoc network a real time application.

KEYWORDS

Mobile ad hoc networking, routing, security, wormhole, shortest path, RTOS, Real time application

1. INTRODUCTION

Mobile ad hoc networks (MANETS) have a wide range of applications, especially in military operations, emergency, e-commerce and entertainment. Mobile ad hoc networks are self configuring network sometimes called mesh networks which form link by themselves. It forwards the traffic also establishes a route by route request within its transmission range. Hence it acts like a transmitter as well as a router. The route establishment is not static it is done by dynamic ways. Hence these types of systems don't have a centralized system. This leads to the evolution of protocols bounded within a mobility range usually nodes which are placed only few hops of each other. Different protocols are then evaluated based on packet drop rate, overhead introduced by routing protocol, security etc. In this paper the security issue faced by the routing protocol is taken into consideration. The routing protocol of mobile ad hoc networks faces different security issues described in [2]. This paper concentrates on wormhole attack described in [1]. The effect of wormhole attack creates a malicious node thereby deleting the legitimate path. Many *secure routing* protocols against wormhole have been proposed in [3, 5, 6, 8, and 9] for an efficient routing on a general purpose routing environment. This paper focus on local monitoring and isolation through cryptographic methods in a real time operating system *(RTOS)* environment.

2. MANETS ROUTING PROTOCOL

Routing is an activity or a function that connects a call from origin to destination in telecommunication networks and also plays an important role in architecture, design and operation of networks. Ad-hoc networks are wireless networks where nodes communicate with each other using multi-hop links. There is no stationary infrastructure or base station for communication. Each node itself acts as a router for forwarding and receiving packets to/from

DOI : 10.5121/ijnsa.2011.3412

other nodes. Routing in ad-hoc networks has been a challenging task ever since the wireless networks came into existence. The major reason for this is the constant change in network topology because of high degree of node mobility. A number of protocols have been developed to accomplish this task.

Classification of routing protocols in MANET's can be done in many ways, but most of these are done depending on routing strategy and network structure. According to the routing strategy the routing protocols can be categorized as Table-driven (Proactive) and source Initiated (Reactive), while depending on the network structure these are classified as flat routing, hierarchical routing and geographic position assisted routing. Both the Table-driven and source initiated protocols come under the Flat routing.

2.1. Proactive Protocol

Each node maintains routing information to other nodes. The routing information is normally kept in table. These table are updated whenever the network topology changes. Most flat routed global routing protocols do not scale very well. The increase in scalability can be achieved by reducing the number of rebroadcasting nodes. Some of the types of proactive routing protocols are DSDV (Destination sequenced distance vector), WRP (Wireless Routing Protocol).

2.2. Reactive Protocol

In this case the topology information is transmitted by nodes on demand. Whichever node wants to transmit will flood a route request in the network. A route establishment is created if the request is received by the destination or through the intermediate route. The most popular reactive algorithm is AODV (Ad-hoc On Distance Vector). As long as the route lasts it is in active state when- ever it loses it path again RREQ is sent.

3. SECURITY THREATS TO ROUTING PROTOCOLS

3.1. Modification

The attack tries to modify the data by doing packet misrouting. The attack will do impersonation and spoofing.

3.2. Fabrication

Sleep deprivation is one of the attacks in mobile ad hoc networks which put the battery in exhaust condition. The attacker tries to consume the batteries of a node.

3.3. Interruption

An intruder tries to drop packets during forwarding of packets. One more attack is flooding of packets.

3.4. Interception

Black hole attacks and worm hole attacks. Out of these attacks this paper evaluate wormhole attack scenario.

4. WORM WHOLE ATTACK

Wormhole attack is the most severe attack in MANET routing. Figure 1 depicts a small wormhole scenario. In this type two or more nodes collaborates each other thereby creating a

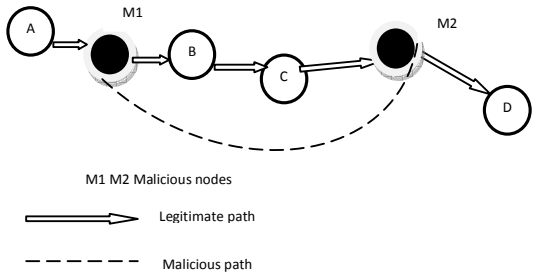

Figure 1. Wormhole Scenario

shortcut between the packets through that link. The packets are forwarded between the malicious nodes by encapsulation. Also forwarding the packets through additional hardware like wired link and directional antenna. It can be launched in two modes hidden mode and participation mode. Wormhole attacks can be used to drop packets. They are extremely difficult to detect. Encryption or authentication cannot able to protect against hidden- mode worm holes because malicious node won't read or modify the packets it simply forwards. Participation modes are very difficult to launch once they are launched.

5. RELATED WORK

In [1] wormhole scenario is explained. A wormhole is created in the mobile ad-hoc network which can able to defend against any type of countermeasures. This attack can create a malicious path even if the attacker has not malpractice the other host that is even if the other hosts path is good. Similarly the attack can happen even if there is a good encryption and decryption is happening.

In [2] surveys the types of complex wormhole attack in wireless Ad-hoc networks. This paper refers attacks like spoofing, eaves dropping and packet leashes. In this paper the wormhole is identified as two phase process launched by one or several malicious nodes, called wormhole nodes, try to lure legitimate nodes to send data to other nodes via them. In the second phase, wormhole nodes could exploit the data in variety of ways. The wormhole attack mode and classes, and point to its impact and threat on ad hoc networks.

In [3] two algorithms were proposed which will eliminate the wormhole attack faced when the ad-hoc network is in mobility state called MOBIWORP. In this paper there is a special node called Central Authority (CA) which monitors the node locally and if any malicious activity occurs it isolates the node globally.

In [4] the wormhole attack is detected using the topology changes. This paper does not concentrate on special hardware or artefacts for finding the attacks. The algorithm is independent on wireless communication models. The proposed algorithm detects the wormhole by using the information collected in the upper layer like routing layer. The detection algorithm looks for forbidden structures which are not present in the legal connectivity.

Work [5] introduces a light weight counter measure for mobile ad-hoc networks (LITEWORP). This algorithm listens to the neighbour node. In this algorithm every malicious node is detected and isolated and it's specially concentrates on resource constraints.

Work [6] examines the wormhole attack in WAHAS (Wireless Ad-Hoc and Sensor networks). This paper introduces a protocol called SECOS which provides a secure route between any two

nodes despite of compromise of any number of other nodes. The algorithm uses a low key-management and authentication technique

Work [7] mainly concentrates on a specific local monitoring when the ad-hoc network is vulnerable to stealthy packet dropping. The stealthy packet dropping do a packet dropping by intermediate node by avoiding the packets to reach the destination. This creates as if the malicious node is performing a legitimate action thereby creating a suspicious to the legitimate path. Here there is a protocol called DISA (Detection and Isolation of sneaky attackers in locally-Monitored Multi-hop wireless networks).

Paper [8] proposed an efficient algorithm called (Wormhole attack prevention algorithm) WAP. This algorithm avoids the use of specialized hardware. It first monitors the neighbour nodes by using timer and by maintaining a neighbour node table. The next phase of work is to detect the wormhole route by flooding the RREQ and getting the false route reply.

Paper [9] runs the AODV in a secure way. The AODV is made to run against wormhole attack. A mechanism called Wormhole Attack Detection Reaction (WADR) is made to run with conventional AODV. This paper reduces overhead and the packet loss caused by malicious nodes.

Paper [10] proposed a concept of monitoring nodes only as end - to -end instead of monitoring each corresponding neighbour node in a multi-hop environment. Hence the proposal will only look after the source and destination path and it reduces overhead mechanism. The proposed algorithm is cell based open tunnel avoidance (COTA) to manage the information. COTA achieves an equal space for each node between the source and destination through geographic information. The proposed algorithm can be combined with existing routing algorithm to protect the MANETS against wormhole attacks.

Paper [11] analyzes the obstacle faced in the conventional cryptographic methods because the wormhole attack cannot be defeated as the malicious nodes do not send separate packets. In this paper, we present a cluster based counter-measure for the wormhole attack which alleviates these drawbacks and efficiently mitigates the wormhole attack in MANET.

6. RTOS (Real Time Operating System) BASED SECURITY ALGORITHM

Already existing routing algorithm is made to run on a geographical area of few kilometres. Since the area is small the nodes assumed to be less.

A wormhole scenario will be created. The malicious activity created by the wormhole attack will be monitored and the malicious node will be isolated

The idea of shortest path algorithm will be studied. A probabilistic method of analysis will be studied

The cryptographic analysis will be made to run in a real time environment using a real time operating system.

7. PROPOSED WORK

i) Traditional AODV is made to run on the system.
ii) Wormhole scenario is created and monitored.
iii) Node Isolation.

8. WORK COMPLETED

The following code describes the traditional AODV. This program deals with 20 nodes. The nodes are placed by using a random number generator and the nodes are assumed to be transmitting randomly. Node 1 is taken in to consideration and is distributing the signal to the nodes whose minimum distance is 1.

8.1. MATLAB SIMULATION

8.1.1. Node Distribution

```
A=randint (20);
% Making matrix all diagonals=0 and A(i,j)=A(j,i),i.e. A(1,4)=a(4,1),
% A(6,7)=A(7,6)
for i=1:20
for j=1:20
if i==j
A(i,j)=0;
else
A(j,i)=A(i,j);
end
end
end

disp(A);
t=1:20;
%disp( ' a   b ' )
disp(t);
disp(A);
status(1)='!';
dist(1)=0;
next(1)=0;
```

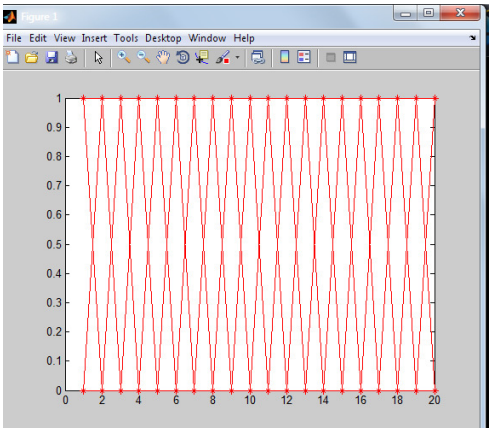

Figure 2. Node Distribution

Figure 2 explains the random integer matrix which contains matrix elements whose values consists of only 1's and zeros generated randomly for every t seconds of simulation. In order to make the nodes to be distributed uniformly the diagonal elements are assumed to be 0. At time t1 node 1 is assumed to distribute randomly to the corresponding nodes whose minimum distance is 1 for the above Figure 2 the corresponding nodes are 2, 4, 8, 9, 10, 11, and 18. The following code explains the node 1 transmission.

```
for i=2:20
status(i)='?';
dist(i)=A(i,1);
next(i)=1;
disp(['i== ' num2str(i) ' A(i,1)=' num2str(A(i,1)) ' status:=' status(i) ' dist(i)=' num2str(dist(i))]);
for i=4
plot(i,A(i,1),'-mo')
end
flag=0;
for i=2:20
if A(i,1) == 1
disp([' node 1 sends RREQ to node ' num2str(i)
end
end
```

The above code explains the transmission of route request to the corresponding nodes whose minimum distance A (i, 1) = 1. Hence the simulated output is as shown in Figure 3.

Output

```
node 1 sends RREQ to node 2
node 1 sends RREQ to node 4
node 1 sends RREQ to node 8
node 1 sends RREQ to node 9
node 1 sends RREQ to node 10
node 1 sends RREQ to node 11
node 1 sends RREQ to node 18
```

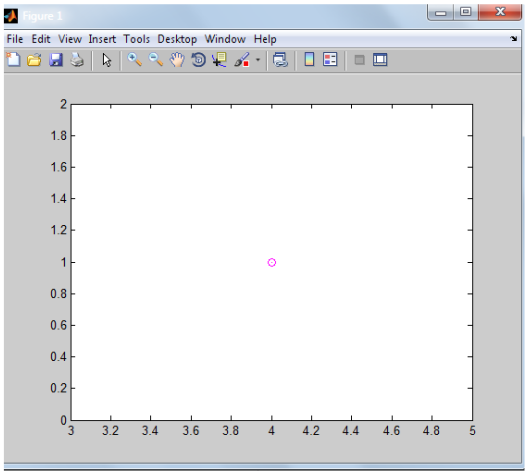

Figure 3. Node 1 Transmission

8.1.2. Creation of Wormhole

Output

Our agenda is to create a wormhole so that the corresponding node which is going to act as a wormhole will transmit the route request. Wormhole can be created in different methods we have created the malicious node by increasing the power factor. Hence the modified code is

```
for j = 0:1:3
 power = power+1;
   if power>1
flag = 0;
for i=2:20
   if A(i,1) == 1
disp([' node 1 sends RREQ to node ' num2str(i)])
   end
end
   else if power>3
for i = 2:20
status(i)='?';
dist(i)=A(i,2);
next(i)=1;
disp(['i== ' num2str(i) ' A(i,2)=' num2str(A(i,2)) ' status:=' status(i) ' dist(i)=' num2str(dist(i))]);
end
      end
   end
end
 for i = 2: 20
if A(i,2) == 1
disp([' node 2 sends RREQ to node ' num2str(i)])
end
end
```

Here an additional parameter power is included whose value is fixed to 3. Whenever the node trying to transmit is going to have a power factor of more than 3 that corresponding node is made to act as a malicious node and is going to perform malicious activity. In our case we have made node 2 to be a malicious node. Hence the output will show node 1 activity till the power factor becomes greater than 3. Also node will send the packets to its own destinations that got their own minimum distance.

Output

```
 node 1 sends RREQ to node 2
 node 1 sends RREQ to node 4
 node 1 sends RREQ to node 8
 node 1 sends RREQ to node 9
 node 1 sends RREQ to node 10
 node 1 sends RREQ to node 11
 node 1 sends RREQ to node 18
 node 2 sends RREQ to node 5
 node 2 sends RREQ to node 6
 node 2 sends RREQ to node 7
 node 2 sends RREQ to node 8
 node 2 sends RREQ to node 12
 node 2 sends RREQ to node 14
 node 2 sends RREQ to node 15
 node 2 sends RREQ to node 16
 node 2 sends RREQ to node 18
 node 2 sends RREQ to node 19
```

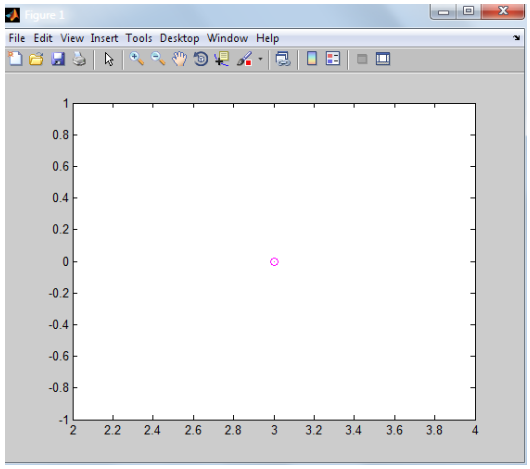

Figure 4. Wormhole Creation

Hence the above Figure 4 shows the malicious activity of node 2 when its i value is 3 since the minimum distance is 0 for i = 3 node 2 is not transmitting to 3. But for i = 5 node 2 will transmit because the minimum distance is 1 and the graph is as shown below in Figure 5.

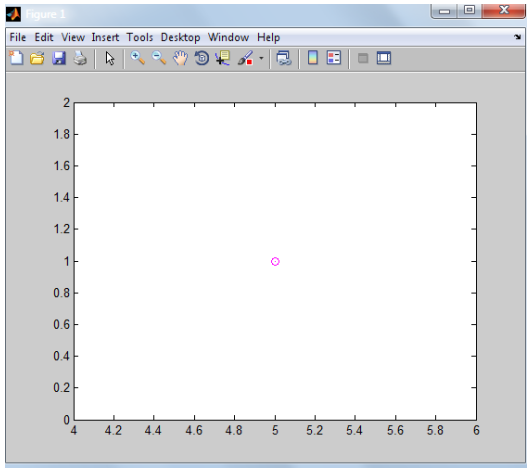

Figure 5. Node 2 Transmission

9. NODE MONITORING

The next important issue is once the wormhole is created it needs to be monitored. This operation is done using the combination of hardware and software. A counter is made to run at a specific clock period while the nodes start transmitting. Whenever a malicious activity happens at any clock period the counter starts incrementing and whenever its value exceeds the maximum count the counter will set an alarm so that the malicious activity can be predicted explicitly.

```
for k=0:1:5
counter = counter + 1;
if counter >3
for i = 2: 20
```

```
if A(i,2) == 1
   disp(['couter value exceeds maximum hence malicious activity starts'])
 plot(k, counter, '-mo')
disp([' node 2 sends RREQ to node ' num2str(i)])
%for i = 5
%plot(i,A(i,2),'-mo')
end
end
end
end
```

Output

```
node 1 sends RREQ to node 2
node 1 sends RREQ to node 4
 node 1 sends RREQ to node 8
 node 1 sends RREQ to node 9
 node 1 sends RREQ to node 10
 node 1 sends RREQ to node 11
 node 1 sends RREQ to node  18
 counter value exceeds maximum hence malicious activity starts
 node 2 sends RREQ to node 5
 counter value exceeds maximum hence malicious activity starts
 node 2 sends RREQ to node 6
 counter value exceeds maximum hence malicious activity starts
 node 2 sends RREQ to node 7
 counter value exceeds maximum hence malicious activity starts
 node 2 sends RREQ to node 8
 counter value exceeds maximum hence malicious activity starts
 node 2 sends RREQ to node 12
 counter value exceeds maximum hence malicious activity starts
 node 2 sends RREQ to node 14
 counter value exceeds maximum hence malicious activity starts
 node 2 sends RREQ to node 15
 counter value exceeds maximum hence malicious activity starts
 node 2 sends RREQ to node 16
 counter value exceeds maximum hence malicious activity starts
 node 2 sends RREQ to node 18
 counter value exceeds maximum hence malicious activity starts
 node 2 sends RREQ to node 19
```

10. NODE ISOLATION

The next step is once the wormhole is created and monitored we need to check how the communication is taking place. It is well known that node should be permanently cut off from the communication link at the time instant say t1. In the same time we are creating a path between the malicious node and its corresponding receiving nodes. Hence only node 2 should come in picture. Hence the above code has been modified and the node 1 communication is stopped and node 2 only transmitting.

```
next(i) = 2
for newi= next(i)
count = count + 1;
 if count >1
     disp ([num2str(newi) 'sends RREP to ' num2str(i)])
     %disp([ num2str(i) 'Sends message to node ' num2str(newi)]) end
end
end
end
end
end
```

Output

```
node 1 sends RREQ to node 2
 node 1 sends RREQ to node 4
 node 1 sends RREQ to node 8
 node 1 sends RREQ to node 9
 node 1 sends RREQ to node 10
 node 1 sends RREQ to node 11
 node 1 sends RREQ to node 18
 node 1 sends RREQ to node 2
 node 1 sends RREQ to node 4
 node 1 sends RREQ to node 8
 node 1 sends RREQ to node 9
 node 1 sends RREQ to node 10
 node 1 sends RREQ to node 11
 node 1 sends RREQ to node 18
 node 1 sends RREQ to node 2
 node 1 sends RREQ to node 4
 node 1 sends RREQ to node 8
 node 1 sends RREQ to node 9
 node 1 sends RREQ to node 10
 node 1 sends RREQ to node 11
 node 1 sends RREQ to node 18

node 2 sends RREQ to node 5
next =
    0    1    1    1    2    1    1    1    1    1    1    1    1    1    1    1    1    1    1
counter value exceeds maximum hence malicious activity starts
 node 2 sends RREQ to node 6

next =
    0    1    1    1    2    2    1    1    1    1    1    1    1    1    1    1    1    1    1
6sends rep to node2
counter value exceeds maximum hence malicious activity starts
 node 2 sends RREQ to node 7
next =
```

0 1 1 1 2 2 2 1 1 1 1 1 1 1 1 1 1 1 1 1
7sends rep to node2
counter value exceeds maximum hence malicious activity starts
node 2 sends RREQ to node 8
next =
0 1 1 1 2 2 2 2 1 1 1 1 1 1 1 1 1 1 1 1
8sends rep to node2
counter value exceeds maximum hence malicious activity starts
node 2 sends RREQ to node 12
next =
0 1 1 1 2 2 2 2 1 1 1 2 1 1 1 1 1 1 1 1
12sends rep to node2
counter value exceeds maximum hence malicious activity starts
node 2 sends RREQ to node 14
next =
0 1 1 1 2 2 2 2 1 1 1 2 1 2 1 1 1 1 1 1
14sends rep to node2
counter value exceeds maximum hence malicious activity starts
node 2 sends RREQ to node 15
next =
0 1 1 1 2 2 2 2 1 1 1 2 1 2 2 1 1 1 1 1
15sends rep to node2
counter value exceeds maximum hence malicious activity starts
node 2 sends RREQ to node 16
next =

0 1 1 1 2 2 2 2 1 1 1 2 1 2 2 2 1 1 1 1
6sends rep to node2
counter value exceeds maximum hence malicious activity starts
node 2 sends RREQ to node 18
next =
0 1 1 1 2 2 2 2 1 1 1 2 1 2 2 2 1 2 1 1
18sends rep to node2
counter value exceeds maximum hence malicious activity starts
node 2 sends RREQ to node 19
next =
0 1 1 1 2 2 2 2 1 1 1 2 1 2 2 2 1 2 2 1
19sends rep to node2

CONCLUSION AND FUTURE WORK

The work will be formulated to an advanced mathematical concept. This can be extended to a Wide area Network. This can be applicable to any wireless application. We can extend this project to connect group of classroom, places and buildings apart from the calculated geographical area.

ACKNOWLEDGEMENTS

The authors would like to acknowledge financial support of Council of Scientific & Industrial Research (CSIR), Govt. of India.

REFERENCES

[1] Yih-Chun Hu, Adrian Perrig, Member, & David B. Johnson, (2006) "Wormhole Attacks in Wireless Networks" IEEE *Journal on selected areas in Communications,* Vol. 24, No. 2.

[2] Mohit Jain &Himanshu Kandwal, (2009)"A Survey on Complex Wormhole Attack in Wireless Ad Hoc Networks". *International Conference on Advances in Computing, Control, and Telecommunication Technologies.*

[3] Issa Khalil, Saurabh Bagchi & Ness B. Shroff, "MOBIWORP: Mitigation of the Wormhole Attack in Mobile Multihop Wireless Networks". http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4198824

[4] Ritesh Maheshwari, Jie Gao &Samir R Das," Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information".http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=04068262

[5] Issa Khalil, Saurabh Bagchi& Ness B. Shroff,(2007) "LITEWORP: Detection and Isolation of the Wormhole Attack in Static Multihop Wireless Networks". *The International Journal of Computer and Telecommunications Networking*, Vol. 51, Issue 13, pp 3750- 3772.

[6] Issah Khalil,(2008)"Mitigation of Control and data traffic attacks in wireless ad-hoc and sensor networks" IEEE Vol. 6, Issue 3, pp 344-362.

[7] Issa Khalil, Saurabh Bagchi, Najah AbuAli & M. Hayajneh, "DISA: Detection and Isolation of Sneaky Attackers in Locally-Monitored Multi-hop Wireless Networks" http://onlinelibrary.wiley.com/doi/10.1002/sec.152/abstract

[8] Sun Choi, Doo-young Kim, Do-hyeon Lee &Jae-il Jung(2008) **"**WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks" IEEE *International* Conference on Sensor Networks, *Ubiquitous, and Trustworthy Computing SUTC'08*. pp 343- 348

[9] Emmanouil A. Panaousis, Levon Nazaryan & Christos Politis(2009) "Securing AODV Against Wormhole Attacks in MANET" *Proceedings of the 5th International ICST Mobile Multimedia Communications Conference***,** Article 34.

[10] Weichao Wang ,Bharat Bhargava & Yi XiaoxinWu(2006) "Defending against Wormhole Attacks in Mobile Ad Hoc Networks" *Wireless Communications & Mobile Computing,* Vol. 6, Issue 4,pp 483-503

[11] Debdutta Barman Roy, Rituparna Chaki, &Nabendu Chaki (2009) "A new `cluster-based wormhole intrusion detection algorithm for mobile ad-hoc networks" *International Journal of Network Security & Its Application* , Vol. 1, No.1.

Authors

Dr Ramesh pursued his B.E. Degree in Electrical and Electronics Engineering at University of Madras, Chennai, and completed his M.E degree in power systems Engineering at Annamalai University Chidambaram. He received Ph.D degree at Anna University Chennai, and has been a faculty of Electrical and Electronics Engineering Department Of College of Engineering , Guindy, Anna University, Chennai since 2003. His areas of interest are Real –Time Distributed Embedded Control, On-line Power System Analysis and solar power system.

Ms Gayathri pursued her B.E. Degree in Electrical and Electronics Engineering at University of Madras, Chennai, and completed her M.E degree in Embedded System Technologies at Anna University Chennai. She is currently pursuing Ph.D at Anna University Chennai, and has been a Teaching Research Associate of Electrical and Electronics Engineering Department of College of Engineering, Guindy, Anna University, Chennai since 2008. Her areas of interest are Real Time Operating Systems, Cryptography and Network Security, and Nanotechnology.