INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

DESIGN AND IMPLEMENTATION OF ROUTING PROTOCOLS TO DEAL WITH SELFISH NODES IN MANET

Shephy[1], Dr. Sukhvir Singh[2]

[1]N.C. College of Engineering, Kurukshetra University,
Israna, Panipat-132107, India
shephybatra87@gmail.com

[2]N.C. College of Engineering, Kurukshetra University,
Israna, Panipat-132107, India
boora_s@yahoo.com

Abstract: *Routing protocol is used to find out the path without any selfish node i.e. the nodes whose energy is low may not be the part of the route from source to destination. After having the following information a neighbor list is generated. First source node send the hello request packets to all its neighbors, then all the nodes who received the hello request packets send the unicast hello reply packets to the source node by using this neighbor list source address checks whether the destination node is in its vicinity or not, if the destination node is in its vicinity then it directly unicast the packet to the destination node otherwise we apply the Roulette wheel mechanism to find out the destination node by using the neighbor list. The process goes on until the hop count maximum limit exceeds or the packet reaches to the destination.*

Keywords: *ARAN, ARIDANE, SEAD, SAODV, SRP*

1. INTRODUCTION

Wireless networks use some sort of radio frequencies in air to transmit and receive data instead of using some physical cables. Wireless networks are formed of routers and hosts. In a wireless network, the routers are responsible for forwarding packets in the network and hosts may be sources or sinks of data flows. The fundamental difference between wired and wireless networks is the way that the network components communicate. A wired network relies on physical cables to transfer data. In a wireless network, the communication between different network components can be either wired or wireless. Since wireless communication does not have the constraint of physical cables, it allows a certain freedom for the hosts and/or routers in the wireless network to move. This is one of the advantages of a wireless network.[1]

Network components in a wireless network communicate with each others using wireless channels. The use of wireless networks has become more and more popular. There exist two types of mobile wireless networks.[2][3]

- Infra structured Networks
- Infra structure less Networks

2. LITERATURE REVIEW

MANET consists of mobile nodes interconnected by multi hop communications paths or radio links.[4] A MANET consists of mobile platforms, known as nodes, which are free to move at any speed in any direction and organize themselves randomly. The nodes in the network function as routers, clients, and servers. These nodes are constrained in power consumption, bandwidth, and computational power. MANET lack central administration and prior organization, so the security concerns are different than those that exist in conventional networks. Wireless links make MANET more susceptible to attacks. It is easier for hackers to eavesdrop and gain access to confidential information. It is also easier for them to enter or leave a wireless network because no physical connection is required. They can also directly attack the network to delete messages, inject false packets, or impersonate a node. This violates the network's goals of availability, integrity, authentication, and non-repudiation. Compromised nodes can also launch attacks from within a network. Security issues have been emphasized when mobile ad hoc networks (MANET) are employed into military and aerospace fields.[5]There exist several proposals that attempt to architect a secure routing protocol for ad hoc networks, in order to offer protection against the attacks. These proposed solutions are either completely new stand-alone protocols, or in some cases incorporations of security mechanisms into existing ones (like DSR and AODV). The design of these solutions focuses on providing countermeasures against specific attacks, or sets of attacks. Furthermore, a common design principle in all the examined proposals is the performance-security trade-off balance. The existing

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

routing protocols based on the cryptographic techniques and digital signatures. In this chapter the following secure routing protocols for MANET are described.[6][7]

- Authenticated Routing for Ad hoc Networks (ARAN)
- ARIADNE
- Secure ad hoc on demand routing protocol (SAODV)
- *Secure Efficient Ad hoc Distance Vector Routing (SEAD)*
- Secure routing protocol (SRP)

ARAN

The Authenticated Routing for Ad hoc Networks (ARAN) protocol, proposed in [8], is a stand-alone solution for securing routing in ad hoc networking environments. ARAN use cryptographic certificates in order to achieve the security goals of authentication and non-repudiation. [9]

ARAN is consisting of three operational stages: -certification, route discovers process and shortens path assurance, first two are compulsory and the last one is optional.
Preliminary certification process: it requires the existence of a trusted certification authority (CA). Each node, before attempting to connect to the ad hoc network, must contact the certification authority and request a certificate for its address and public key. The protocol assumes that each node knows a priori the public key of the certification authority. Each node receives exactly one certificate after securely authenticating their identity to T.[10]
Route discovery process: It provides an end-to-end authentication. This ensures that the intended destination was indeed reached. Each node must maintain a routing table with entries that correspond to the source-destination pairs that are currently active. The route discovery packet (RDP) includes the certificate of the initiating node, a nonce, a timestamp and the address of the destination node. The initiating `node signs the RDP packet with its private key. Each node validates the signature with the certificate, updates its routing table with the neighbor from whom it received the RDP, signs it, and forwards it to its neighbors after removing the certificate and the signature of the previous node (but not the initiator's signature and certificate). The signature prevents malicious nodes from injecting arbitrary route discovery packets that alter routes or form loops [11].

3. NEW PROPOSED SCHEME

The Communication in an ad hoc network is a multi hop communication wherein a source node communicates with a distant node using intermediate nodes in order to save the power. Thus the major activity in an ad hoc network environment is to find a suitable route such that the delivery of the message is ensured beyond doubt. The route should be so chosen that all the nodes in the path are trustworthy, non malicious, unselfish and the hop count is minimum.

The first receiver of the message to a distant node is some immediate neighbor of the source node. Therefore, it is necessary that every node in the ad hoc network must be aware of its immediate neighbors at every moment. To remain aware about its neighbor nodes, a node in the network keeps on broadcasting hello requests on the periodic basis and keeps on receiving the hello replies as well. Using these hello request and replies a node in the ad hoc network constructs and maintains a table of its neighbors known as neighbor table. Since the nodes in the ad hoc networks are mobile the neighbor table keeps on changing with time. Our proposal begins with the format for hello request packet as shown in Fig. 4.1. [12]

Packet Type	Source Address	Power Status

Figure 4.1: Hello Request Packet

The hello request packet has three fields, namely packet type, source address and power status. The packet type field denotes that it's a hello request packet, source address field is the identifier of the node in the network which generated the hello request and power status field indicates the current status of the power of the node issuing the hello request. There is no destination address in this packet as hello request is a broadcast mechanism.
Hello reply is multiple unicast mechanism wherein a node responds to the node from whom it has received a hello request. The format of hello reply packet is shown in the Fig. 4.2.

Packet Type	Source Address	Destination Address	Power Status

Figure 4.2: Hello Reply Packet

It has four fields: packet type, source address, destination address and power status. The packet type field here is hello reply, source address field contains the identification of the node from which the reply packet originated, destination address field is the identification of the node to which the packet has to be sent and the power status field provides the current power status of the sender node.[13]
The proposed routing mechanism in this paper has modified the conventional hello request and reply mechanism to include a new feature called power status. This feature keeps a node aware about the power status of neighboring nodes. Thus the neighbor table of a node, in the proposed routing protocol, will have an additional entry in form of power status of the neighboring node.
The knowledge about the power status of the neighbors helps a node in avoiding a node which is very low in power and may drop the packet in selfish manner to save the energy. A node in the ad hoc network can have five power statuses: very low, low, medium, high, very high with their ordinal values as 0, 1, 2, 3, 4 respectively.

Vol. 1, Issue VIII, Sep. 2013
ISSN 2320-6802

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

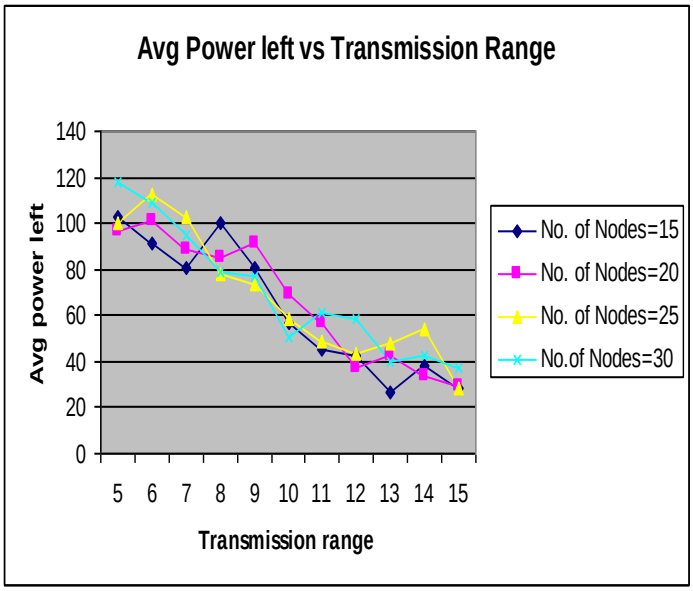
WINGS TO YOUR THOUGHTS.....

4. IMPLEMENTATION RESULTS

Average Power left per node in Normal Routing Protocol

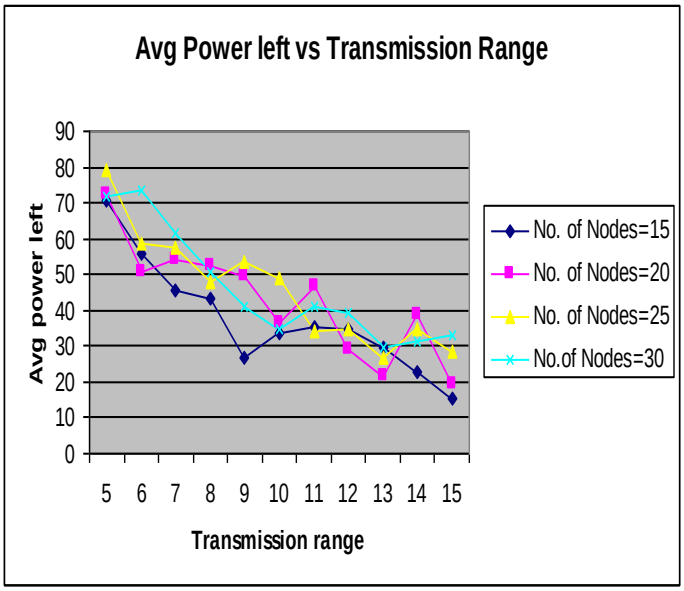
	Average Power left per node			
Transmission range	No. of Nodes=15	No. of Nodes=20	No. of Nodes=25	No. of Nodes=30
5	102.59	96.3	100.16	117.86
6	91.26	100.94	112.4	108.7
7	80.67	89	102.59	94.73
8	100.33	85.05	78.08	78.53
9	80.33	91.34	73.5	77.16
10	56.33	69.4	58.36	50.7
11	45.53	56.45	48.84	60.93
12	42.34	37.1	43.84	58.1
13	26.67	42.55	47.56	40.17
14	37.94	33.95	54.48	42.64
15	28.6	29.05	28.16	37.3

Old Graphs:



Average Power left per node in proposed Routing Protocol

	Average Power left per node			
Transmission range	No. of Nodes =15	No. of Nodes =20	No. of Nodes =25	No. of Nodes=30
5	70.8	72.19	79.44	71.63
6	55.86	50.9	58.44	73.76
7	45.46	53.95	57.68	61.57
8	43.4	52.25	48.08	50.87
9	26.87	49.3	53.56	41.16
10	33.8	36.35	48.95	34.7
11	35.34	46.78	34.16	41.2
12	34.8	29.15	34.52	39.1
13	29.8	21.4	26.92	29.4
14	22.8	38.8	34.68	31.5
15	15.33	19.35	28.2	33.06

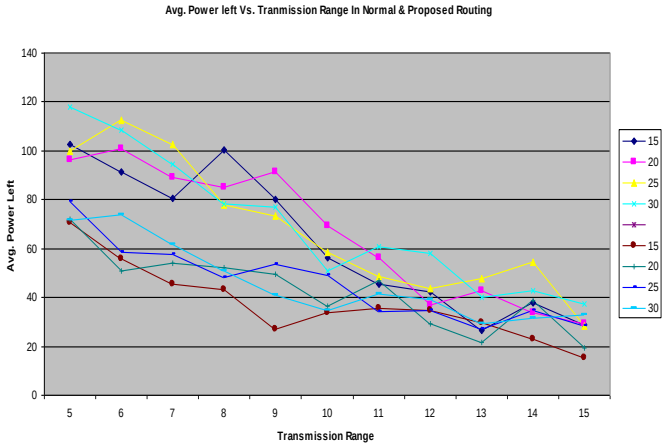


Vol. 1, Issue VIII, Sep. 2013
ISSN 2320-6802

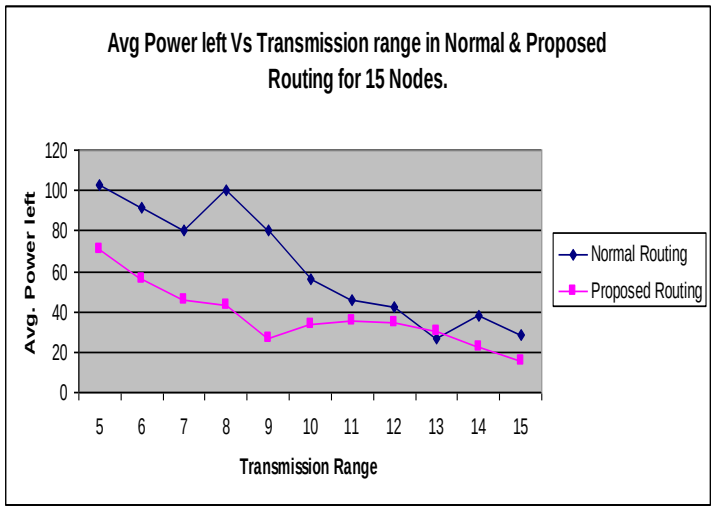
INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

New Graphs:



OR



This graph is showing only the Comparison between normal & proposed routing for avg . power left when Nodes =15

4. CONCLUSION AND FUTURE SCOPE

In this work a new routing protocol has been implementing for ad hoc network. The proposed protocol is power aware keeping in view the power constraint of nodes being used in ad hoc network.[14]

To test the performance of the protocol a program has been designed in C++. This implementation in C++ used to check the performance of the protocol under various conditions. This performance has been illustrated in the forms of the graphs and tables in the previous chapter of dissertation. The results are quite satisfactory indicating that the proposed protocol has feasible implementation.

The testing of the protocol in the present work has been done in isolated environment where conditions are not standard. However to check the actual applicability of protocol it is mandatory to check this protocol under an industrial standard environment. So that actual rating of a proposal can be made. Such an environment can be provided by standard software's like NS2 and Qualnet. However to test a protocol in NS2 and Qualnet the C++ code of the protocol has to be physical augmented. The implementation of the protocol in C++ has accomplished this task.[15]

Now, the future work is to customize this implementation so as to create it augmentation compatibility with NS2 or Qualnet. Then the proposed protocol can be actually tested in the standard condition and its performance can be compared with the other existing routing protocols.

REFERENCES

[1] Dimitri Butsekas & Robert Gallager, "Data Networks 2nd edition". Prentice Hall, New Jersy, ISBN 0-13-200916-1.

[2] Chim Yuen Chong, Raymond Seah Kwang Wee, Sim Soon Lian, Tan Jia Hui, "Moblie Ad hoc Networking", http://www.dsta.gov.sg/DSTA_horizons/2006/Chapter_7. htm"

[3] Humayun Bakht "Application of mobile ad hoc networks" http://www.computingunplugged.com/issues/issue2004/00001371001.html

[4] A Trust Model Based Routing Protocol for Secure Ad Hoc Networks www.cse.cuhk.edu.hk/~lyu/paper_pdf/Aero04_TAODV.pdf

[5] Saab NetDefence, Available on-line 2002-05-06.

[6] Y.-C. Hu, A. Perrig, and D.B. Johnson, "Packet Leashes: A Defense Against Wormhole Attacks in Wireless Ad hoc Networks," Proc. 22nd Annual Joint Conf. IEEE Computer and Communications Societies (Infocom'03), San Francisco, CA, April 2003.

[7] Y.-C. Hu, A. Perrig, and D.B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad hoc Networks," Proc. 22nd Ann. Joint Conf. IEEE Computer and Communications Societies (INFOCOM 2003), IEEE Press, 2003, pp. 1976-1986.

[8]http://www.telenor.com/rd/pub/rep03/R_41_2003.pdf

[9] Cisco. Cisco Internetworking. Cisco Press, 2002.

[10] P. Papadimitratos, and Z.J. Haas, "Securing the Internet Routing Infrastructure," IEEE Communications, vol. 10, no. 40, October 2002, pp. 60-68.

[11] S. Murphy, "Routing Protocol Threat Analysis," Internet Draft, draft-murphy-threat-00.txt, October 2002.

[12] M. Gerla, Fisheye state routing protocol (FSR) for ad hoc networks, Internet Draft, draft-ietf-manet-aodv-03.txt, work in progress, 2002.

[13] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields and E.M. Royer, "A Secure Routing Protocol for Ad hoc Networks", Proc. 10th IEEE Int'l. Conf. Network Protocols (ICNP'02), IEEE Press, 2002, pp. 78-87.

[14] Y.-C. Hu, A. Perrig, and D.B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad hoc Networks," Proc. 8th ACM Int'l. Conf. Mobile Computing and Networking (Mobicom'02), Atlanta, Georgia, September 2002, pp. 12-23.

[15] M.G. Zapata, and N. Asokan, "Secure Ad hoc On-Demand Distance Vector Routing," ACM Mobile Computing and Communications Review, vol. 3, no. 6, July 2002, pp. 106-107