A Novel Routing Strategy for Cognitive Radio Ad-hoc Network

[1]Malleswari.Y and 2Shavali. V

[1]Department of ECE, Sri Venkateswara Institute of Science and Technology, kadapa, JNTUA, India, yallaturumalleswari20@gmail.com

[2]HOD and Assistant Professor Department of ECE, Sri Venkateswara Institute of Science and Technology, kadapa, India,,v.shavali@gmail.com

ABSTRACT

The paper presents the novel routing strategy for cognitive radio ad hoc network. The ad hoc network is termed as Cognitive Radio Ad Hoc Networks (CRAHN). The CRAHN consists of communicating nodes that can move from one node to other node. In this work, we evaluate the performance metrics of the routing strategy protocols in mobile network environment. The main objective of this work is to access the various routing strategies protocols have been proposed based on performance metrics like delay, power, hop count and spectrum awareness. Performance metrics such as packet delivery ratio, throughput, and end-to-end delay are evaluated using MATLAB TOOL. Simulation results shows the proposed method has gives better performance than existing routing protocols.

Index Term: - CRAHN (Cognitive Radio Ad Hoc Networks) CR (Cognitive Radios) ,MTPR (Minimum Total Power Routing), AODV (Ad hoc On Demand Distance Vector), EED (End to End Delay)

1. INTRODUCTION

Automatic key establishment between two devices in a network is generally performed either by publickey- based algorithms (like Diffie and Hellman [1]), or by encrypting the newly-generated key with a special key wrapping key [2]. However, in addition to the well-established, well-investigated keying information exchange, one additional aspect of key establishment is often understated: to ensure the security of the application it serves, the newly generated secret key has to be truly random. While minimum standards for software-based randomness quality are generally being enforced [3], many applications rely on often costly hardwarebased true random generators [4]. Sources of randomness employed by true random number generators vary from wireless receivers and simple resistors to ring oscillators and SRAM memory.

In general, tree topology inference assumes single-path routing, where the routing path between any two end-hosts remains unique. Notice that in a tree topology, every two end-to-end paths construct an inverted “Y” structure. Then through end-to-end measurements, e.g., the “back-to-back” probing, the delay covariances between paths can be used to determine where their branching nodes are [5]. Abstracting the delay covariance as a length metric for the shared paths, [6] generally shows that the tree topology is identifiable from the shared path lengths of every two of its end-to-end paths. Moreover, the multi-source topology (having the “Y" structures) has also been proved as identifiable by [7] when the lengths of both the end-to-end paths and their shared paths are known. The multisource topology is shown reconstructable via merging the tree sub-topologies.

2. MOBILE AD-HOC NETWORK TOPOLGY

The communicating Nodes in ad hoc networks may be mobile resulting in a dynamic, weakly connected topology. In our topology management scheme, NFPQR (Node Failure prediction for query routing) nodes are selected in such a way that link nodes have the maximum power level among their on hop neighbors and all non-link nodes are within the transmission range of link nodes. These adhoc link nodes have the routing protocal i.e. they make all decisions nodes related to routing. The gateway nodes having minimum of power levels are selected so that they can forward packets one node to other node. A gateway node does not associated to routing intelligence. These link as well as gateway nodes are awake to route the packets of other other nodes. The member nodes wake up a number of times in a particular period T, and they goes to sleep mode again when if they hadn’t to transmit or receive data. The wake up time for each node is calculated from a pseudo-random number, such that link node as well as neighbor nodes know the wake up of that ad-hoc node time. Thus the member node can remain in power saving sleep mode most of the time, if it is not actively sending or receiving packets. The packets are routed over the virtual backbone consisting of link nodes and gateways. The routes are found with the help of mobile agents.

The ad-hoc topology management scheme runs above the MAC layer and interacts with the routing protocol. If a communicating node has been asleep for a while, packets destined for it are not lost but are buffered at a neighboring link node. It can retrieve these packets from the buffering link node When the node awakens. This topology management schemes makes the routing simple, as only those entries in a node’s

routing table that correspond to currently active link nodes can be used as valid next-hops (unless the next hop is the destination itself).

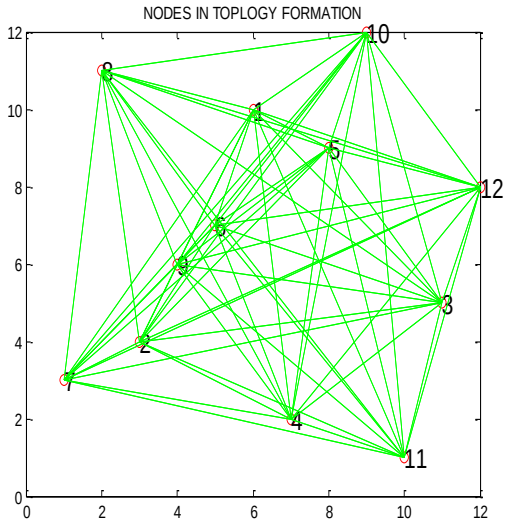

Fig.1. ad-hoc network topology

The algorithm of proposed method is given by

Deploy Secondary Nodes (N)

Hop Count =0;

PDR =0;

Reachability =0;

End to End Delay=0;

TPL=0;

for (source (S) =1:1:N)

for (destination (D)= i+1: 1: N)

If (path exists (S-D))

PDR= PDR + Send data();

Hop Count = Hop Count + size(path);

End to End Delay = End to End Delay+ path delay() + switching delay() + back off delay();

End

End

End

PDR=(PDR)/Reachability;

Hop Count Hop count/ Reachability;

pt= pt/Reachability;

End to End Delay = End to End Delay/ Reachability

3. PERFOMANCE METRICS

In the work, performance metrics are delay, power, hop count, packet delivery ratio, throughput, and end-to-end delay.

a) Energy

Time to send or receive one bit = 1 / 1 Mbps = 1 μsec

The energy used in transmitting or receiving packets from nodes is given by .

Energy = Power * Time (2.1)

where Power is in Watts and Time is in seconds

$$Energy_{Txonebit} = 1040 * 1 * 10^{-3} W * 1 * 10^{-6} sec$$

$$Energy_{Txonebit} = 1.04 \mu J/bit$$

b) Power loss

Power loss is depends on frequency, antenna height and receive terminal location relative to obstacles. Power loss is given by

Lfs = 32.45 + 20Log10(dkm) +20Log10(fMHz)

Where dkm is the distance between one to other node and f is the frequency.

c) Packet delivery ratio (PDF)

Packet delivery ratio is the ratio of data packets received by the source node to destination node. Mathematically, it can be defined as:

PDR= S1÷ S2

Where, S1 is the sum of data packets received by the each destination and S2 is the sum of data packets generated by the each source.

d) Power

The Energy is calculated by using this formula.

Energy = Power * Time (1)

The energy consumption is measured by the transmitting power or receiving power multiply the transmitted time.

$Pt = 8 * Packet\ Size / Bandwidt$

e) **Hopcount**

The **hop count** is defined to the number of intermediate nodes between source and destination node.

f) **delay**

Network delay is an important design and performance characteristic of a mobile ad-hoc network as well as telecommunications network. The delay of a network

specifies how much of time to travel from one node or endpoint to another. It is given by the following formula:

Dt=N/R seconds

where

Dt is the transmission delay in seconds

N is the number of bits, and

R is the rate of transmission (say in bits per second)

4. RESULTS

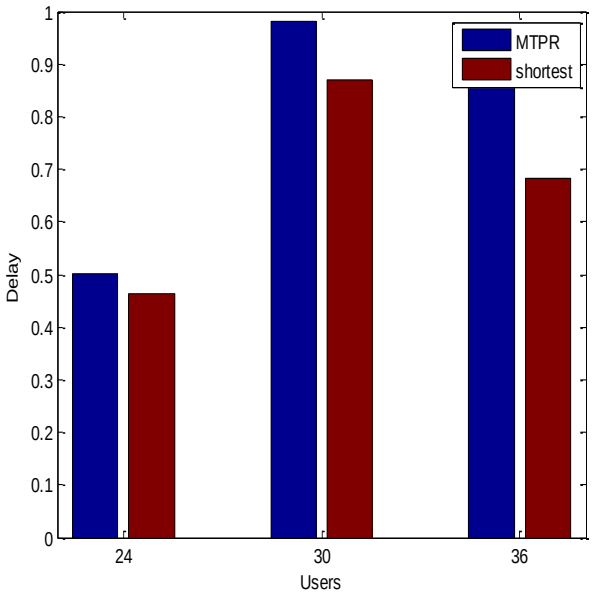

Fig 2. Impact on End to End Delay

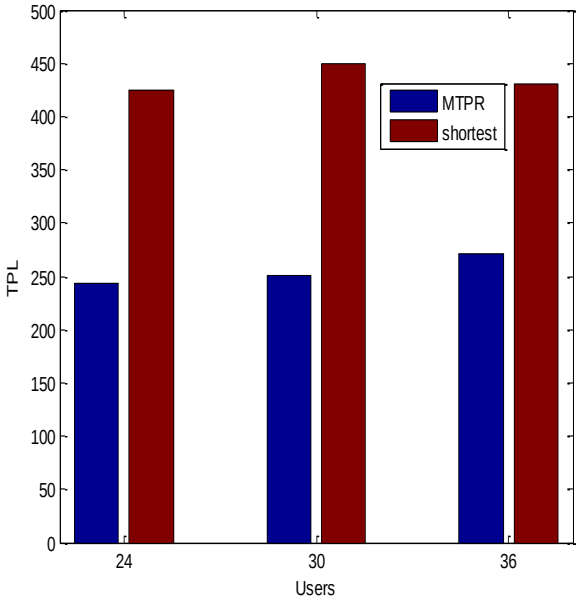

Fig3. Impact on Transmission Power Loss

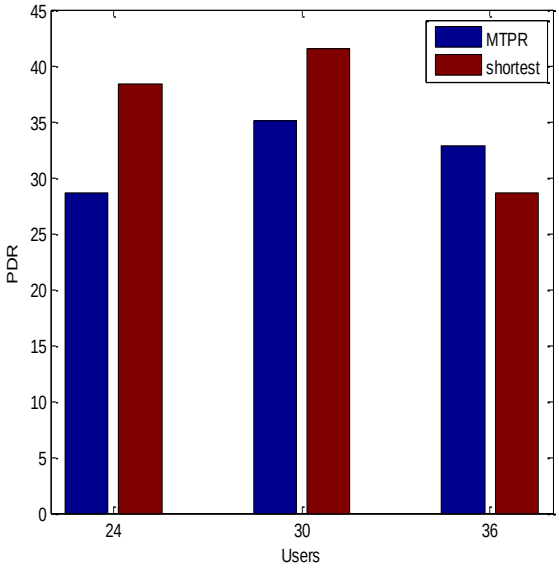

Fig 4. Impact on PDR

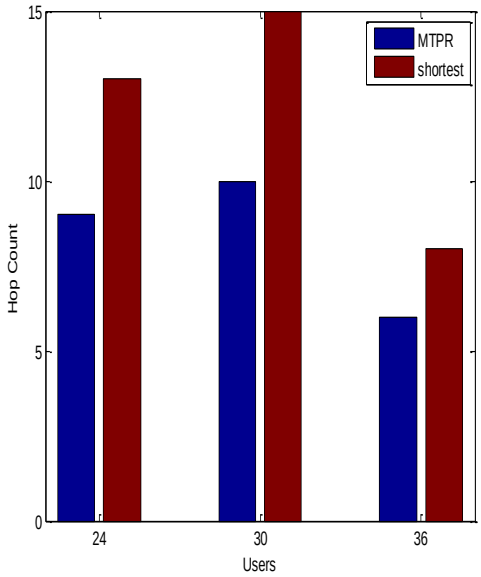

Fig 5. Impact on Hop Count

5. CONCLUSION

In this paper we have introduced the notion of performance metrics within the context of wireless ad-hoc networks. The objective was to investigate the impact of using transmit powers, packet delivery ratio successfully reaching destinations, which we define as end-to-end network throughput. Thus, a network with a power management scheme implemented will have better performance than a network without such a scheme. It has gives better performance than existing routing protocols.

REFERENCES

[1] W. Diffie and M. E. Hellman, "New directions in cryptography," IEEE Trans. Inf. Theory, vol. 22, no. 6, pp. 644–654, Nov. 1976.

[2] M. Bellare and C. Namprempre, "Authenticated encryption: Relations among notions and analysis of the generic composition paradigm," in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2000, pp. 531–545.

[3] S. K. Park and K. W. Miller, "Random number generators: Good ones are hard to find," Commun. ACM, vol. 31, pp. 1192–1201, Oct. 1988.

[4] B. Sunar, "True random number generators for cryptography," in Cryptographic Engineering. New York, NY, USA: Springer, 2009, pp. 55–73.

[5] Y. Tsang, M. Yildiz, P. Barford, and R. Nowak, "Network radar: Tomography from round trip time measurements," in Proc. 4th ACM SIGCOMM Conf. Internet Meas., 2004, pp. 175–180.

[7] J. Ni and S. Tatikonda, "Network tomography based on additive metrics," IEEE Trans. Inf. Theory, vol. 57, no. 12, pp. 7798–7809, Dec. 2011.

[12] M. G. Rabbat, M. J. Coates, and R. D. Nowak, "Multiple-source Internet tomography," IEEE J. Sel. Areas Commun., vol. 24, no. 12, pp. 2221–2234, Dec. 2006.

