International Journal On Engineering Technology and Sciences – IJETS™
ISSN (P): 2349-3968, ISSN (O): 2349-3976
Volume 2 - Issue 5, May 2015

INFERENCE AWARE DISTRIBUTED ROUTING PROTOCOL USING OUTAGE PROBABILITY

V.Nithya Kalyani[1] Prof.Shuriya B[2]
[1]PG Scholar, [2]Assistant Professor
Department of Computer Science and Engineering
RVS Technical Campus, Coimbatore RVS Technical Campus, Coimbatore.
Email ID: s.kalyaniramanan@gmail.com, shuriya1987@yahoo.co.in

Abstract -Using hybrid network for data transmission gathered a significant research in the QoS constraint which is devoted to real time applications. Many research solutions has been derived to mitigate the QoS problem, among them QoS oriented distributed routing protocol for scheduling and segment resizing are predominant. Invalid reservation problem occurswhen the reserved resources become useless if the data transmission path between a source node and a destination node disrupts. Race condition problem occurswhenthe same resource is double allocated to two different QoS paths.Theproblems in the hybrid networks rise due to denial of service attacks,node correlation, channel fluctuations, node fadingand collision. In order to minimize the interference as well as correlation losses this work proposesan Inference Aware Distributed Routing Protocol (IADRP). Inference Aware Distributed Routing Protocol monitors the transmission log and using passion theory the Node correlation over outage probability considered as self behaving has been rescheduled and utilized for further transmission .Experimental results proves that outage probability estimation mitigates the overhead of the network due to interference, transmission delay , scalability and node collision for improved QoS of the network.

Keywords: Hybrid Wireless network, quality of service, Routing Protocol, Interference Handling

I. INTRODUCTION

A hybrid network [1][2] refers to any computer network that contains two or more different communications standards. Hybrid wireless networks help to tackle the critical end-to-end quality of service (QoS) requirements pertaining to different applications and are proven to be a superior network structure for the next generation wireless networks. Hybrid networks combine infrastructure networks and MANETs [4] to complementeach other performance. In detail, the scalability of a MANET is improved by infrastructure networks, while spontaneousself-organizing networks are established by MANETs, thus leveragingthe infrastructure networks. It is important to improve the data transmissionefficiency with high throughput. Thereare several causes like node collision, race condition, denial of service and channel fading which degrades the performance of the network. Interference is an important factor in system design, becausethe performance of a network is frequentlyaffected by users competing for the same resources. There are four major sources of randomness that leads to interference in huge networks. The first is multipath fading [3][5], which is the time variation of the channel strengths due to small-scale effects. The second is node placement. Mobile networksrequire a random model of spatial locations to facilitate the network analysis. A homogeneous poisson point process [7] is a authentic model for the node distribution in wireless networks. The third is power control, which helps in the interference management, energy optimization, and connectivity. The fourth is channel access. This can be achieved by two classes of well-accepted random and distributed medium access control protocols(MAC) viz., ALOHA and CSMA. Microscopic mobility induces multipath fading. Randomness in channel gain is induced by minor change of a node position. On the other hand, when distance is weighted in a wireless transmission, a major change in the transmission distance or macroscopic mobility, leads to path-loss uncertainty [6]. Multipath fading denoted as fading and large-scale path loss are both induced by mobility. The temporal and spatial correlations are both affected by mobility. The locations of a node show a certain unit of correlation in several time slots since the speed of the node is finite. The quantification of such correlation becomesessential, since it has a higher impact on the network performance. Providing QoS guarantees becomes more challenging withtheadditionalcomplexities of a hybrid network. The challenges in providing service guarantees are many, but the foremost challenge in a traditional networkiscongestion. On the other hand, wireless and mobile networks face more challenges apart from those of a traditional network.

Service guarantees are typically made for one or more of the following four characteristics. 1) A guarantee of delay ensuresboth the sender and receiver that it will consume no more than a specified period of time for a packet of data to travel from sender to receiver. 2) A guarantee of loss ensuresboth the sender and receiver that no more than a specified fraction of packets will be lost during transmission. 3) A guarantee of jitter ensuresboth the sender and receiver that the delay will not vary more than a specified time. 4) A guarantee of throughput assures both the sender and receiver that within a specified unit of time, no

less than specified amount of data can be sent from sender to receiver.

There are many hindrancesin guarantying the quality of servicein a network; some of the challenges in wired and wireless networksare as below. The principal challengeis network congestion. In a congested network, the packet stays longer in the queue for each hop and eventually increases the delay. When the queue is full, it automatically starts to drop the incoming packets. This will also tend the additional packets to be dropped thereby limiting the throughput.

One moreproblem is the multi-path routing. When two packets travel, it is notguaranteed that they en-route the same path to the targeted destination. If one of thepathsis more congested or perhaps has more number of hops then the packets may not reach the destination in parallel time.

This paper proposes an Inference Aware Distributed Routing Protocol (IADRP) to minimize the interference and correlation losses. Inference Aware Distributed Routing Protocol using poisson theory the node correlation over outage probability is considered as self-behavingand is rescheduled and utilized for further transmission. The remainder of the paper is organized as follows: Related work in Section 2. Description and formulation of optimal path for mobile sink propagation and collection in Section 3. In Section 4, Simulations are reported with performance evaluation graph and tables. Finally, Section 5 concludes the paper.

II. RELATED WORK

A. QoS oriented Distributed Routing Protocol (QOD)

QoS-Oriented Distributed routing protocol (QOD) enhance the QoS support capability of a hybridnetwork. With the advantage of lesser transmission hops and anycast transmission features of the hybrid networks, QOD convertsthe packet routing problem to a resource scheduling problem. QOD includes five algorithms: 1) a QoS-guaranteed neighbourselection algorithm to meet the transmission delay requirement[10], 2) a distributed packet scheduling algorithm to further reducetransmission delay, 3) a mobility-based segment resizing algorithm that adaptively adjusts segment size according to node mobility inorder to reduce transmission time, 4) a traffic redundant elimination algorithm[9] to increase the transmission throughput, and 5) a dataredundancy elimination-based transmission algorithm to eliminate the redundant data to improvise the transmission QoS.

B. Disruption Tolerant Networking for Efficient path selection

Disruption tolerant networking (DTN) technology is designed to deal with the intermittent connectivity among mobile nodes due to mobility, intermittent connectivity and frequent partitions e.g. earthquake and disaster recovery scenarios and short range radios or terrain obstacles. DTN network become efficient communication technology for critical network environment. Some of the most challenging issues in this are the enforcement of authorization policies and the policies update for secure data retrieval.This survey analyse the cipher textpolicy attribute based encryption (CP-ABE) which is a promising cryptographic solution to the access control issues. Conversely, the problem inusingthistoa decentralized DTN prompts to security and privacy challenges pertaining to coordination of attributes,key escrow andattribute revocation. A secure data retrieval scheme using CP-ABE for decentralized DTNs is used as current research with multiple key authorities managing their attributes independently.

III. PROPOSED MODEL

A. HybridWireless Network Architecture

In this Process, for efficient data transmission a hybrid network is modelled usinga wireless infrastructure network and a MANET (Mobile AdHoc Network). Nodes are designed with capabilities of data transmission among them within a network. The mobility of the nodes is independent with respect to each other and every node updatesits position at the beginning of each time slot.

B .Interference characteristics

Interference in hybrid network is modelled with reference to latency and delay in data transmission. Interference is the possibility of packet loss or delay in transmission due to environment or node fault conditions. It refers to the additionof noise or unwanted signals to a intended signal. Following are conditionsthat explain the attack evolution.

Multipath fading -Multipath fading is induced by node location changes which lead to large scale path losses. Multipath fading, which is the time variation of the channel strengths due to small-scale effects.

Node Correlation -Attenuation in a wireless channel is modelled as a product of a large-scale path-loss component based on node correlation. The packet observesa number of realizations because the node covers a number of wavelengths.

C. Interference Aware Distributed Routing Protocol

The outage probability is one of the fundamental performance metrics in wireless networks. In channels limited by interference, outage happens if the signal-to interference ratio (SIR) is lower than the thresholdat the receiver. The mean interference in a network is calculated using either uniform mobility model (UMM) or random waypoint (RWP) mobility. The location of a node in

UMM assumes a distribution within a radius $a_o$from base location.

$$f_w(x) = \begin{cases} \frac{1}{\pi a_0^2} & \|x\| \leqslant a_0 \\ 0 & \text{otherwise,} \end{cases}$$

Where || - || is the Euclidean distance.

Investigating the interference in a single time slot is insufficient to design the transmission and routing schemes in wireless networks, since the interference is temporallyand spatially correlated. Such correlation, which is caused by the locations of mobile nodes, affects retransmission and routing strategies greatly. A link in outage at a given time indicates a higher outage probability in the next several time slots. Such correlation affects retransmission and routing schemes greatly and thus needs to be quantified.

Outage Probability -

T(a, b) = outage consumed in transmitting and receiving by node in specified time with respect to packet over one hop from a to b

$e_j = \Sigma^{k-1}_{i=1} T(n_i, n_{i+1})$ = total outage energy spent for packet j

Traffic redundancy elimination uses a chunking scheme to determine the boundary of the chunks in a data stream. The data sent out by the source node is cached by the source node. Likewise the data received by the receiver node is cached by the receiver.

Node replication Prediction -Node replication is termed for DOS attack or Sybil attack in the network for mitigating the high latency in the network and its elimination can be modelled with Poisson equation.

Some nodes behave greedy, these greedy nodeseither extend only partial cooperationwith other nodes or do not co-operate at all (that is, non-cooperative or misbehaviour actions are usually

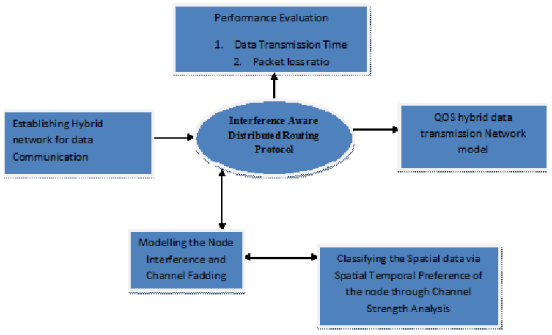

Figure3.1: Framework of Inference Aware Distributed Routing Protocol

termed as selfish, this is remarkably different from malicious behaviour).A selfish node will not contribute its memory to store a replica for the reference of other nodes. The need is to develop an algorithm that detectsselfish nodesand considers selfishness to any degree and allocation of replicas to handle the selfish allocations. Selfish replica allocation denotes a node's non-cooperative behaviour.

Inference Aware Distributed routing Protocol against Node correlation

- Packet Request from source for data Transmission
- Estimate the Node density of intermediate nodes

Based on satisfying the below conditions.

Node Density > Threshold

Where,Node density = $\frac{\text{Node Processing Speed}}{\text{Number of source connected}}$

And, Threshold is a limit for Node ability for data processing (packet)

Predict the node request from the source node against the DOS attack. DOS Attack can be calculated through Multivariate analysis.

Multivariate analysis process

a. It analysis request
b. No. of times in the network / Threshold count
c. No. of load given per time through various constraints.

IV. EXPERIMENTAL RESULTS

The experimental part demonstrates the distinguishing properties of the Inference Aware Distributed Routing Protocol, this protocol extends Ad hoc On-Demand Distance Vector (AODV) by adding information of the maximum delay and minimum available bandwidth of each neighbour in a node's routing table. Mobility causes higher rate of linkage breaks, which leads to more number of packet drops. In a dynamic wireless network, heavy node density seems to break the transmission link amid two nodes. Further, in a dynamic network, a node has more likelihood to encounter other nodes and wireless access points.This is very much advantageous for scheduling the resource.

Channel fading and node correlation can be considered as distributed denial of service (DDOS) attack in the IADR protocol as scenario resembles the same, this attacks can be incurred with the help of the routing table used to log the transaction of the nodes for packet transfer. Interference caused due to node correlation can be defined as periodic communication between the nodes more specified thresholds.

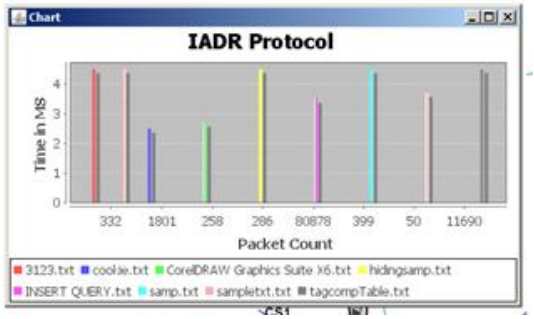

Figure 4.1 Performance analysis of the execution time against the proposed framework

Evaluation of the performance of IADR protocol is done against the QOD protocol with respect todetection time and transmission efficiency as shown in figure 4.1.These two aspects are compared in relation to the packet size of the data transferered and number of hops for the communication.

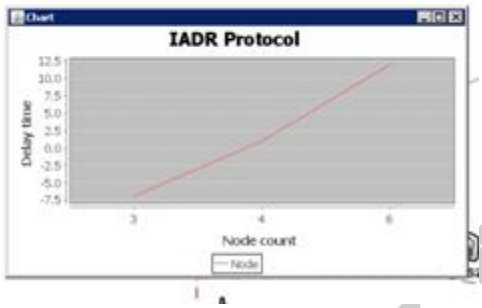

Figure4.2. Performance delay against the node creation in IADR

In figure 4.2, the derived transmission capacity results are evaluated in this section for some typical parameters in order to show how ad hoc network capacity can be expected to scale with path loss and spreading, and to compare frequency hopping and direct sequence spread spectrum. Additionally, a simulated ad hoc network where nodes are spatially distributed according to a Poisson point process is used to show how the derived bounds perform relative to simulated performance.

V. CONCLUSION AND FUTURE WORK

Hybrid wireless networks that integrate MANETs and Infrastructure wireless networks have proven to be a better network structure for the next generation networks. An Inference Aware Distributed Routing Protocol (IADRP) is modelled and implementedto minimize the interference and correlation losses. Inference Aware Distributed Routing Protocol monitors the transmission log and using passion theory the node correlation over outage probability considered as self behaving has been rescheduled and utilized for further transmission by taking advantage of the unique features of hybrid networks, i.e., anycast transmission and short transmission hops.Experimental results prove that outage probability estimation mitigates the overhead of the network due to interference, transmission delay, scalability and node collision for improved QoS of the network.In futurethe performance of IADRP can be leveraged by evaluating the performance against various network topologies and network conditions.

REFERENCES

[1] I. Jawhar and J. Wu, "Quality of Service Routing in Mobile Ad Hoc Networks," Network Theory and Applications, Springer, 2004.
[2] M. Haenggi and R.K. Ganti, "Interference in Large Wireless Networks," Foundations and Trends in Networking, vol. 3, no. 2, pp. 127-248, 2009.
[3] X. Zhang and M. Haenggi, "Random Power Control in Poisson Networks," IEEE Trans. Comm., vol. 60, no. 9, pp. 2602-2611, Sept. 2012.
[3] R.M. Metcalfe and D.R. Boggs, "Ethernet: Distributed Packet Switching for Local Computer Networks," Comm. ACM, vol. 19, no. 7, pp. 395-404, 1976.
[4] L. Kleinrock and F. Tobagi, "Packet Switching in Radio Channels: Part I-Carrier Sense Multiple-Access Modes and Their Throughput- Delay Characteristics," IEEE Trans. Comm., vol. 23, no. 12, pp. 1400-1416, Dec. 1975.
[5] E. Sousa and J. Silvester, "Optimum Transmission Ranges in a Direct Sequence Spread-Spectrum Multihop Packet Radio Network," IEEE J. Selected Areas in Comm., vol. 8, no. 5, pp. 762-771, June 1990.
[6] E. Sousa, "Interference Modeling in a Direct-Sequence Spread- Spectrum Packet Radio Network," IEEE Trans. Comm., vol. 38, no. 9, pp. 1475-1482, Sept. 1992.
[7] F. Baccelli, B. Blaszczyszyn, and P. Muhlethaler, "An Aloha Protocol for Multihop Mobile Wireless Networks," IEEE Trans. Information Theory, vol. 52, no. 2, pp. 421-436, Feb. 2006.
[8] S. Srinivasa and M. Haenggi, "Distance Distributions in Finite Uniformly Random Networks: Theory and Applications," IEEE Trans. Vehicular Technology, vol. 59, no. 2, pp. 940-949, Feb. 2010.
[9] R.K. Ganti and M. Haenggi, "Interference and Outage in Clustered Wireless Ad Hoc Networks," IEEE Trans. Information Theory, vol. 55, no. 9, pp. 4067-4086, Sept. 2009.
[10] R.K. Ganti, J.G. Andrews, and M. Haenggi, "High-SIR Transmission Capacity of Wireless Networks with General Fading and Node Distribution," IEEE Trans. Information Theory, vol. 57, no. 5, pp. 3100-3116, May 2011.