FraNtiC : A Fractal Geometric Framework For Mesh-Based Wireless Access Networks

Samik Ghosh, Kalyan Basu, Sajal K. Das
Center for Research in Wireless Mobility and Networking (CReWMaN)
Department of Computer Science and Engineering
The University of Texas at Arlington
{sghosh, basu, das}@cse.uta.edu

Abstract

The design of the access networks of next generation broadband wireless systems requires special attention in the light of changing network characteristics. In this paper, we present a mesh-based distributed radio access network (RAN) framework for future wireless systems. Using short, high bandwidth optical wireless links to interconnect the various network elements, we identify a generic fractal or self-similar structure in the network. A mathematical model for the framework is presented and the benefits of its scale-invariant properties on robustness, reliability and flexibility analyzed. We focus on three design parameters - carrier-class network reliability, network exposure due to failure conditions and system cost. The dynamics of these parameters on our proposed architecture are studied and compared against existing access network topologies like tree/ring and square-grid. The generality and recursive nature of our framework lends itself to be applied in interconnecting various heterogeneous broadband wireless access networks of the future.

1 Introduction

Next generation wireless systems are envisioned to provide high-speed Internet access to home and mobile users, multimedia document browsing, high quality video-conferencing, high resolution image or CAD file transfer over hand-held devices. The first steps towards this direction have already been taken in the realization of third generation (3G) mobile systems such as IMT-2000/3GPP standards, IEEE broadband access standards (802.16a, 802.20) etc. However, providing a high-performance, scalable and cost-effective wireless infrastructure requires new system and network architectures.

One of the fundamental areas where a major change is envisioned is the *radio access network*. The access network provides the vital link for backhauling user traffic and control signals to the backbone network. Existing access topologies, typically hierarchical tree/ring based networks using Time Division Multiplexing (TDM) circuits over T1/E1 links(1.5 $-$ 2.048 Mbps) (Fig. 1) to connect the base stations and radio controllers, will not be able to support the variability of next generation systems, the general view of which is captured in Fig. 2.

Next generation access networks will be based on “Open-RAN Architecture”$-$ primarily IP-based, providing high-capacity backhaul transport without incurring huge system operational costs. Future access networks will be characterized by *increased data rates and traffic, small coverage footprints, leading to a large number of base stations* and *highly scalable and easily deployable network elements* providing *carrier-class network reliability*.

In order to provide the above-mentioned characteristics, researchers have recently started re-looking into access network design and transmission technologies. While TDM-based T1/E1 links will not be able to sustain the high bandwidth demands, fiber-optics based systems will be economically infeasible for wide-spread deployments. In this context, “wireless backhaul”, based on Free Space Optical links (optical wireless) and $10-60$ GHz systems [2], emerges as a strong candidate for backhaul transmission. These technologies, either as stand-alone or as hybrid systems, will provide short high-bandwidth access links for future RANs. In this paper, we have focussed on optical wireless technology as a case in point to analyze the new generation of radio access networks.

Recent work has also focussed on redesigning the RAN architecture. In [5], a proximity graph based algorithm has been proposed for clustering base-stations (known as nodeBs in 3G) into RNC areas together with network topology optimization within the clusters so formed. In [3], a ring-based cluster-cellular horizontal topology has been

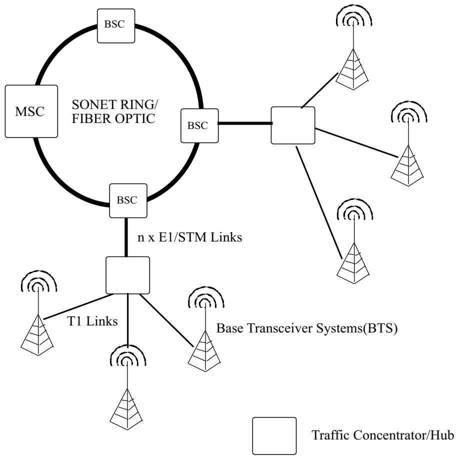


Figure 1. Existing RAN Topology

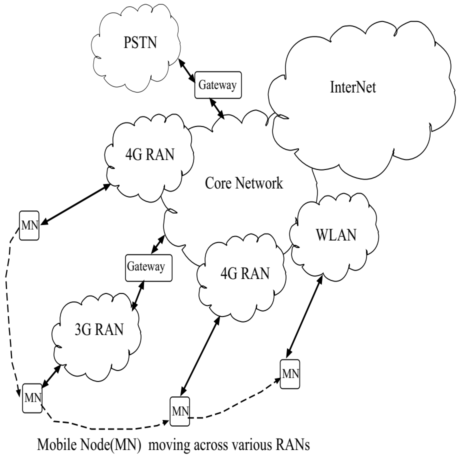


Figure 2. Next Generation Access Networks

suggested for interconnecting the nodeBs, using distributed BS control and short, high-speed wireless links. However, these works have not analyzed the impact of the topology on access networks. Acampora et.al [1] also proposed a mesh-based grid (UniNet) using short FSO links for the “last-mile” in access networks. In [8], a general overview of a wireless mesh architecture has been given for large-scale broadband access.

All these factors motivate a new approach to the design philosophy of future access networks. We believe that as the radio access network is moving into an all IP domain, we should look back at the Internet, the flagship of large IP-based public networks, to remodel existing RANs. We focus our attention to the connectivity issues in a RAN, i.e, the most effective way of interconnecting the RAN network elements. The challenge is to find a topology in the access network which is able to cater to the dynamics of future RANs without compromising on carrier-grade characteristics in a cost-efficient manner. By using a simple rule for interconnecting the base station(BS)/nodeB elements - each BS is connected only to its neighboring BS, we show that it is possible to construct a self-evolving Fractal Network topology, called FraNtiC, which displays natural self-similar properties. The main contributions of this paper are:

- Proposing a distributed fractal geometric framework(FraNtiC) for the topological design of mesh-based access networks.
- Identifying the self-evolving and generic nature of the FraNtiC framework, which allows it to be applied in various hierarchies of the access network across heterogeneous domains.
- Analyzing the new framework, its topological properties - resiliency and robustness; its performance in terms of the key issues - carrier-class network reliability (99.999%), network exposure (total traffic “exposed” on node or link failures) and system deployment costs.
- Providing a comparative platform which evaluates the performance of our framework vis-a-vis existing topologies, like the tree/star and square grid network, showing its efficacy as a next generation access network architecture.

The rest of the paper is organized as follows. Section 2 motivates the philosophy of a mesh-based access network and describes in details the FraNtiC framework. The mathematical analysis of the salient features of FraNtiC is also given in this section. Section 3 delineates the robustness and reliability analysis of the framework and the mathematical model for network exposure calculations. Section 4 presents the comparative results on the basis of optical wireless technology. We conclude the paper with a discussion of future research in Section 5.

2 Mesh Based Radio Access Network

In this section, we layout our proposed framework for the design of future access networks. As elucidated in Section 1, next generation access networks will be essentially IP-centric, supporting high-speed packet-oriented services. In the backdrop of these requirements, mesh networks are a case in point. The advantages of a mesh network, which has been exploited in the fixed line Internet domain for many years, include high coverage levels, multipath routing, flexibility in network deployment and expansion.

The topology of the underlying network can play a crucial role in extracting the advantages of a mesh architecture. While a full mesh connectivity can provide high reliability, it may not be a cost-effective solution, considering link costs as well as scalability issues. Moreover, network dynamics, which include existing traffic distribution, estimated traffic growth, etc., may not support the deployment of a regular mesh topology with well-known properties. Researchers have analyzed the topological nature of router/AS (Autonomous Systems) network in the Internet and studied its scale-free properties. [6] have also analyzed the effect of this Internet topology on error and attack tolerance issues. The natural topological evolution of the Internet motivate our design of the radio access network. Before presenting the proposed fractal geometric topological framework (FraNtiC) we enlist some basic assumptions made in our analysis:

- We assume a cellular service area with regular hexagonal cell sites and omni-directional antennas covering the entire geographical region. However, the framework can be easily extended to other cell patterns or public broadband access networks.
- The interconnection links are all optical wireless based. Other backhaul technologies like fiber optics, microwave, TDM links can also be supported in the framework.
- The radio network controllers are assumed to be co-located with the base-station sites.

2.1 The FraNtiC Framework

Based on the above assumptions, we propose to connect every base-station to all the base-station in its adjacent cells. In this way, the entire interconnection network of base-stations is formed as shown in Fig. 3.

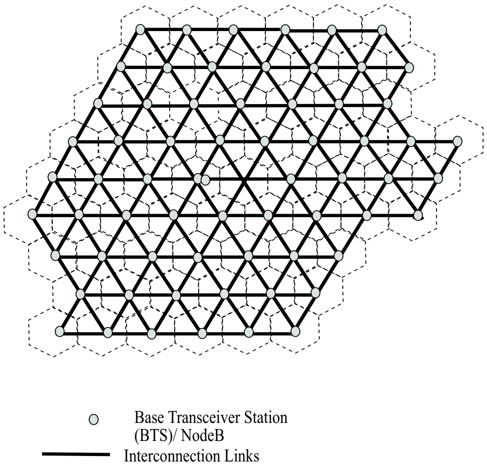


Figure 3. The RAN Interconnection Topology

As seen from this figure, the interconnection network can be viewed as a graph with nodeBs representing the vertices and the physical links between them representing the edges (links and edges are used interchangeable in the paper). The graph structure so formed is planar in nature with girth (i.e, the length of the smallest cycle) 3. Also, every edge in this graph belongs to a cycle. The hexagonal cell site assumption forces the maximum degree (number of edges incident on a vertex) of the graph to be 6. Now, we consider a deterministic fractal structure, which is a variant of the well-known Sierpinski Gasket (SG) [7], called Mod_{SG} (Modified SG). Although various triangular geometries can be taken as the initial state or initiator of the structure, we consider the equilateral triangle. The deterministic generating algorithm is to triangulate each triangle (i.e join the mid-points of each of the three sides of a triangle) at each iteration (generation) of the recursive procedure, thereby generating four smaller triangles at every generation.

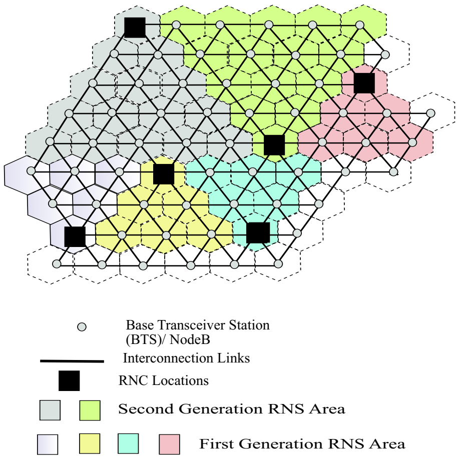

○ Base Transceiver Station (BTS)/ NodeB
Interconnection Links
■ RNC Locations
Second Generation RNS Area
First Generation RNS Area

Figure 4. An Illustrative FraNtiC Framework

Now, given the interconnection network of the RAN, it is possible to map Radio Network Sub-system (RNS) (a group of base stations under a radio network controller (RNC)) areas defined by the Mod_{SG} structure at some generation of its evolution. The radio network controller is placed at some position in the cluster (co-located with a base-station) and the nodeBs under it communicate via short multi-hop multiple paths. The mapping process can be visualized as finding a gth generation Mod_{SG} in the underlying RAN topology depicted in Fig. 3. The same area can be covered by various Mod_{SG} RNSs depending on factors like traffic distribution, RNC/gateway capacity, required network characteristics and so on. The FraNtiC structure is illustrated in Fig. 4, with the rectangular objects represent the RNCs and the shaded areas denote the generation of the RNS they are serving. As can be seen, RNS at various generations can co-exist. The placement of the RNC/gateway may not be necessarily bound to a particular position in the structure, but can be chosen on the basis of other factors without affecting our framework. Another important observation is the fact that every nodeB can be potentially under the control of multiple controllers belonging to different generations. Some salient properties of the FraNtiC framework are presented below.

2.2 Mathematical Analysis

A fundamental advantage of a fractal framework is its *scale-invariance* i.e, the ability to scale up infinitely while retaining similar properties at every level of granularity. It provides a mathematical foundation for network expansion, exhibiting invariant structural properties. Before defining the properties, we define some terminology used in our analysis:

- The fractal structure can evolve in two ways. It can either grow outwards, i.e we group triangles together to generate a higher *generation* Mod_{SG} (represented by g). The initiator is taken as the *base generation* (0) and the generator as the second generation (1). The structure can also grow inwards, as happens when we iterate on any given gth generation Mod_{SG}. This causes the smallest distance between the network elements to decrease. We term this blossoming of the Mod_{SG} as *stage evolution*.

- The number of nodes(nodeB/BS) at the gth generation RNS is defined as N^g_{RNS}. It represents the number of BSs served by the RNC placed in the RNS. The number of edges in the gth generation RNS is denoted by E^g_{RNS}. It represents the number of links to interconnect the nodes in the fully-evolved RNS.

- As can be seen from the geometry of the Mod_{SG}, the nodes are arranged in *levels*, the total number of levels at any generation being represented as l_g.

Now, we present some easily verifiable properties of our framework which are pertinent here ([10]).

Property 1 *$N^g_{RNS} = \frac{1}{2}l_g.(l_g + 1)$ and $E^g_{RNS} = \frac{3}{2}l_g.(l_g - 1)$, where $l_g = 2^g + 1$.*

Property 2 *The edge density of the gth generation structure ($\xi_{Mod^g_{SG}}$), where edge density (ξ) of a graph is defined as the ratio of the number of edges in the graph to the total number of possible edges (i.e the number of edges in the complete graph), is $\frac{12}{(l_g+1)(l_g+2)}$ and lies between that of a tree and a square grid for the same number of nodes.*

From the Property 1, we find that the number of edges is of the same order as the number of vertices in the graph which is significantly less as compared to the complete graph (obtained by connecting every node to every other node in a graph). From Property 2, we conclude that the FraNtiC structure gives a good compromise between cost and reliability, compared to existing topologies as *edge density* offers a metric for trade-off between redundancy/reliability and cost.

2.3 Flexibility And Scalability

As pointed out earlier, the fractal structure at any generation is only a scaled version of any other generation. This property offers flexibility in the design of the RAN and lends it to scale seamlessly with changing system demands. Depending on RNC capacity, cell traffic and required network reliability, the number of nodeBs supported by an RNC can be changed. From the point of view of the FraNtiC framework, it means that the RNS generation has to change. Although, we have assumed uniform evolution of RNS, it is possible that the RNS evolved *partially*. i.e different nodes can be under the control of RNCs belonging to different generations.

On similar lines, the framework renders itself to scale with changing cell sites. As cell sites are added, the framework "blossoms" (evolves in*stages*) in that portion of the geographical area. The other areas are unaffected by the changing cell geometries. This *localized evolution* significantly reduces design complexities and allows the planners to configure each RNS area according to its specific characteristics. A *partially evolved* FraNtiC framework is shown in Fig. 5 with subsequent *localized evolution* due to cell-site growth shown in Fig. 6.

3 Robustness, Reliability and Network Exposure

In this section, we start with analyzing our proposed architecture in terms of its topological robustness. We use modeling concepts from social networks [9] to study the behavior of our architecture against error and attack. We move on to present the reliability model of our architecture and finally calculate the network exposure for our topology.

3.1 Robustness

Topological robustness of a network can be defined as the ability of the network to tolerate perturbations resulting from loss of edges and/or nodes. Resilience to perturbations is a key property of future access networks, particularly for wireless backhauls, which are subject to dynamically changing wireless channel conditions. We model the robustness of our *FraNtiC* architecture in terms of the size of the largest connected component [6]. Nodes/links are removed, either randomly or in an orchestrated manner, resulting in a set of nodes becoming isolated from the network. We measure the number of nodes which are able to communicate with each other under the scenario (i.e the size of the largest connected component).

Fig 7 depicts how our framework reacts to node removal under random (simulating error conditions) and orchestrated attack conditions with varying generations. In the attack

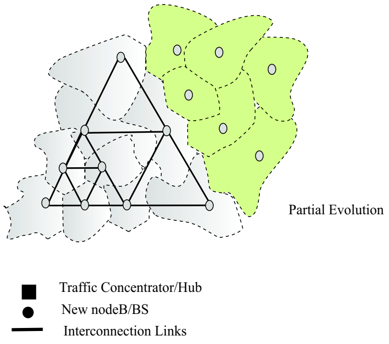


Figure 5. Partial Evolution of the FraNtiC Framework

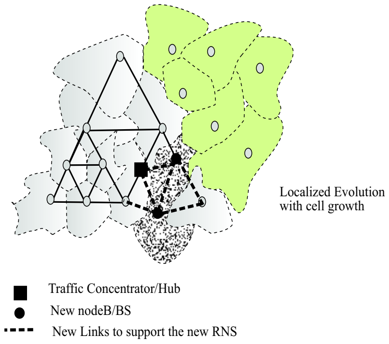

Localized Evolution with cell growth
■ Traffic Concentrator/Hub
● New nodeB/BS
---- New Links to support the new RNS

Figure 6. Localized Growth of the FraNtiC Framework

scenario, nodes were deleted starting with the one having the highest degree (number of edges incident on it). The rationale behind such an attack scenario is the fact the higher the degree of a node in a network, greater is the impact of its removal on the entire network. As can be seen from the plot, the decrease in the size of the largest component is gradual and the network becomes more resilient as we move into higher generations.

Fig 8 captures the response of the *FraNtiC* architecture to link removals. We proceed on the same lines as above, choosing links randomly and in a pre-conceived manner. In case of orchestrated link removal, links are removed based on their distance (in number of hops) from the controller node: links which are nearer to a network controller (Fig.5) and therefore more important in transmitting information to the controller, are removed first and so on. As can be seen from the above plots, the horizontal nature of the self-similar topology makes it resilient to node/edge failures. Also, the fractal structure provides flexibility in increasing generations of the network to further mitigate the effect of perturbations.

3.1.1 Centrality and Its Role In Access Topology

Till now, we have delved into the topological robustness of the *FraNtiC* architecture and studied its behavior under error and attack scenarios. Apart from these, there are several other metrices for analyzing a network. In this sub-section, we look into role of individual nodes in the fractal framework. The position of a node in a network can be crucial. For example, a network can have two highly connected components with a single node acting as a bridge between them. While the network may display robustness to link failures (in terms of size of the largest component), the bridge node makes it highly vulnerable. This analysis becomes particularly important in placement of controller nodes (RNCs or gateways) in the mesh network, which form the key traffic aggregation points [8] to the backbone network.

Centrality [9] is a fundamental property of social

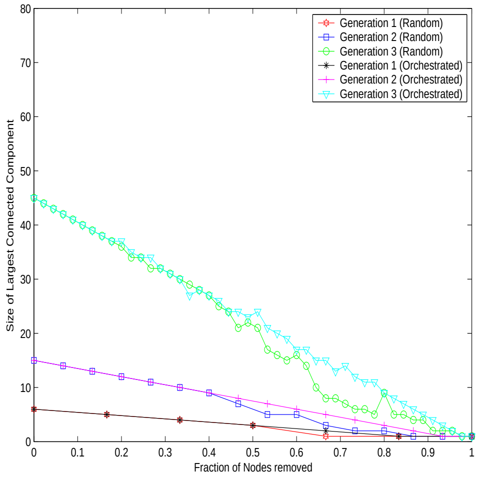


Figure 7. Size of largest Component Vs fraction of nodes removed

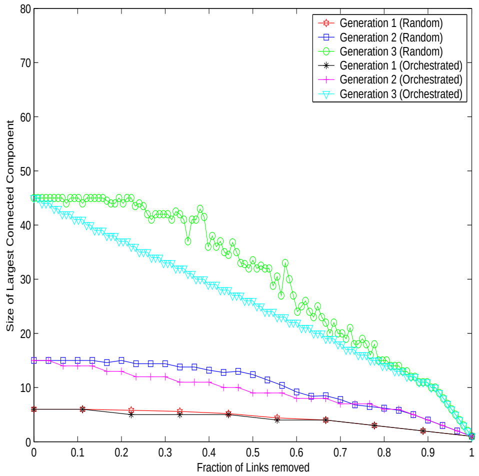


Figure 8. Size of largest Component Vs fraction of links removed

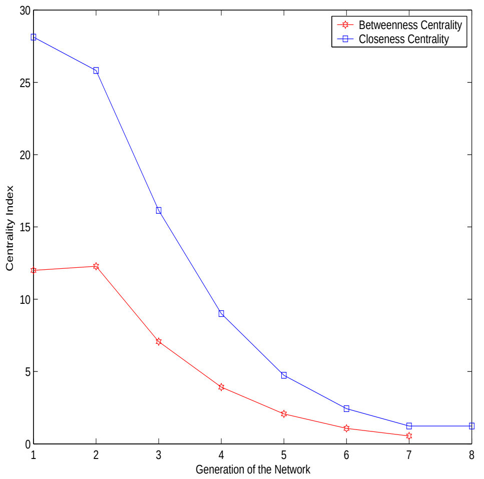


Figure 9. Centrality Network Index Vs FraNtiC generations

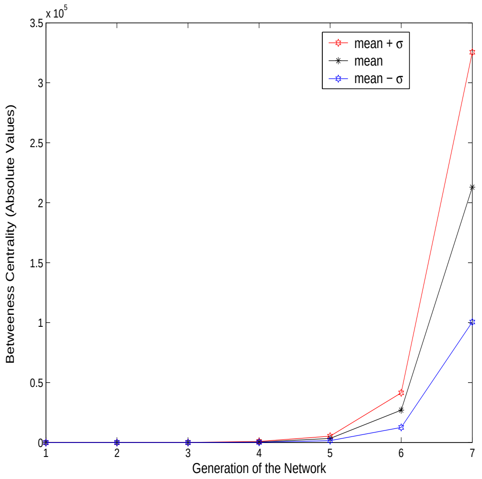


Figure 10. Variation in absolute values of betweenness centrality with generations

structures. It is used extensively in social networks to understand the power yielded by various nodes (which might be representing actors for example) on the network. There are three measures of Centrality [9]:

Degree Centrality, measured by the degree of a node, gives the ability of a node to influence its direct neighbors.

Closeness Centrality, measures the geodesic (shortest) distance of a node to all other nodes in the network. Mathematically, it is the reciprocal of the sum of the distances from a node to all other nodes in the network , i.e

$$\mathcal{C}_C(v) \quad = \quad \frac{1}{\Sigma_{w \in E}(\sigma_{vw})}$$

where σ_{vw} is the shortest distance between nodes v and w, E is the edge-set of the graph and $\mathcal{C}_C(v)$ is the closeness centrality of node v . It measures the closeness of a node with respect to all the other nodes of the network, and not only its neighbors.

Betweenness Centrality of a node is defined as the number of geodesics passing through the node. Mathematically,

$$\mathcal{C}_B(v) \quad = \quad \frac{1}{\Sigma_{u \in E \sigma_{uw}(v)} \Sigma_{w \in E \neq w}(\frac{\sigma_{uw}(v)}{\sigma_{uw}})}$$

where σ_{uw} is the number of shortest paths between u and w, $\sigma_{uw}(v)$ is the number of shortest paths between u and w that pass through v and $\mathcal{C}_B(v)$ is the betweenness centrality of node v. This metric measures the role of a node in interconnecting other nodes in the network.

These measures provide insight into choice of a controller node location in an access network. Choosing a node having high closeness or betweenness centrality as a controller will minimize delay and reduce routing costs. However, choosing a node with high centrality value can increase the potential of network failure due to error or attack. For example, compromising a node having high betweenness centrality (the root of a tree topology or the bridge-node in the previous example) can give the attacker control over most routes in the network.

In this perspective, we now analyze the centrality measures of our proposed architecture. We have used the UNICET 6.0 for Windows (V 6.59) [11] social network modeling and analysis package to calculate these metrices for our network. Fig. 9 shows the variation of centrality (Closeness and Betweenness) with generations of the fractal structure. As can be seen from the graphs, with increasing generation (i.e increasing size of the network), the centrality indices decrease, implying that the network becomes more and more de-centralized or distributed. Also, how the centrality values (absolute values) are distributed among the nodes of the network can affect its vulnerability. A network with a low betweenness centrality index, but with a skewed distribution of values among the nodes can be susceptible to attack. In Fig. 10, we plot the variation of betweenness centrality with generations for our topology. As seen from the graph the standard deviation of betweenness centrality is low and is approximately half the mean value.

All these results lead to the conclusion that the FraNtiC framework becomes more and more de-centralized with increasing generations. Even for higher centrality (lower generations), standard deviations are low, implying that most nodes of the network have equal presence in the network. As pointed out earlier, these properties make the network robust, but can cause increase in routing and delay costs. Network designers can take these and other factors into consideration while choosing the correct generation of the network.

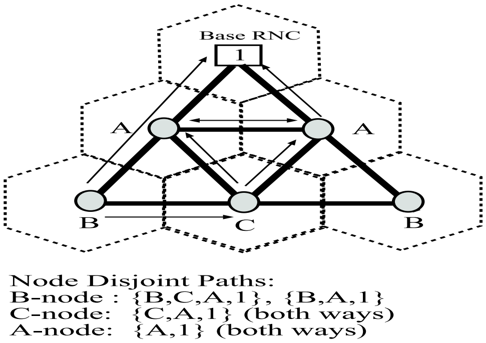

Base RNC
1
A
A
B
C
B
Node Disjoint Paths:
B-node : {B,C,A,1}, {B,A,1}
C-node: {C,A,1} (both ways)
A-node: {A,1} (both ways)

Figure 11. Base RNS and node-disjoint paths

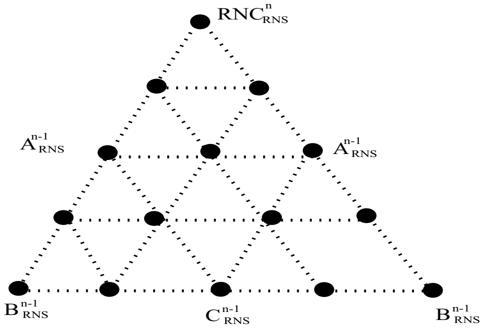


Figure 12. Generalized RNS Structure

3.2 Reliability

One of the main notions in RAN design is providing carrier-class reliability. In this section, we analyze the reliability of the FraNtiC framework. We use the link reliability formulation derived in [10] where link reliability is measured in terms of link availability ($\mathcal{A}_\mathcal{D}$), D being the link distance and represent it by r_D.

In order to calculate reliability, we define the generator structure of Mod_{SG} as the base RNS and calculate higher generation RNS reliability in terms of the base case. The base RNS is shown in Fig. 11.

In this base case, we assume the RNC to be located at node 1 as shown in the figure. We identify two shortest node-disjoint paths from any node to the corresponding RNC. Depending on the paths chosen to the RNC, we associate a type with each node. So, as depicted in Fig. 11, there are two A type, two B type and one C type node. We have concentrated on a uniform RNC location as shown in the base case. If R_t represents the reliability of a node of type t (t ={A,B,C }) i.e the probability that the node is able to communicate with its serving RNC, then,

$$R_A \quad = \quad 1 \; - \; \prod_{i=1}^{2}(\; 1 \; - \prod_{k=1}^{i} \; r_D) \qquad (1)$$

$$R_B \quad = \quad 1 \; - \; \prod_{i=1}^{2}(\; 1 \; - \prod_{k=1}^{i+1} \; r_D) \qquad (2)$$

$$R_C \quad = \quad 1 \; - \; \prod_{i=1}^{2}(\; 1 \; - \prod_{k=1}^{2} \; r_D) \qquad (3)$$

The reliability of the base RNS is defined as

$$R_{RNS}^{base} = min(R_A, R_B, R_C) \qquad (4)$$

The more general case of calculating the reliability of the gth generation RNS (R_{RNS}^g) (pictorially depicted in Fig. 12) can be expressed recursively as

$$R_{RNS}^g = 1 - (1 - min(R_A^{g-1}, R_B^{g-1}, R_C^{g-1})) * \\ (1 - R_{RNS}^{g-1}) \qquad (5)$$

where R_t^{g-1} is defined as the reliability of a t type node of the $(g-1)$th generation and can be calculated as,

$$R_A^{g-1} \quad = \quad 1 \; - \; \prod_{i=1}^{2}(\; 1 \; - \Pi_{k=1}^{i} \; r_D^{2^{g-1}}) \qquad (6)$$

$$R_B^{g-1} \quad = \quad 1 \; - \; \prod_{i=1}^{2}(\; 1 \; - \Pi_{k=1}^{i+1} \; r_D^{2^{g-1}}) \qquad (7)$$

$$R_C^{g-1} \quad = \quad 1 \; - \; \prod_{i=1}^{2}(\; 1 \; - \Pi_{k=1}^{2} \; r_D^{2^{g-1}}) \qquad (8)$$

Using the above expressions, it is possible to calculate network reliability for the FraNtiC RAN topology at various generations and stages of its evolution. The reliability analysis is unaffected by the choice of the base generation or the location of the RNC.

3.3 Network Exposure

In this section, we formally describe the other key parameter for access networks. Network exposure (χ) can be defined as the *the total traffic "exposed" due to perturbations caused by node/link failures*. Traffic is "exposed" when nodes or a group of nodes become isolated from the network (are not able to communicate with their controller node), leading to user in those cell-sites losing connectivity. It follow from the definition that the exposure will depend on the original network topology, traffic patterns and the set of links which have failed. Thus, while centrality and size of largest component measure topological robustness, network exposure is a measure of system robustness.

From the previous discussion, we have the probability of a single link failure as r_D. For the kth link,we represent it as r_k (omitting D). Let us calculate the exposure for a gth generation FraNtiC network (χ_g) having N_g nodes and E_g links (we omit the superscript RNS for simplicity). Let

f be the number of failed links. Now, f links can fail in $\binom{E_g}{f}$ ways. Depending on the f links chosen, there will be $\binom{E_g}{f}$ configurations of the network. Let us denote the jth combination of f link failures as S_j^f, where $f \in \{1 \ldots E_g\}$ and $j \in \{1 \ldots \binom{E_g}{f}\}$. For a given S_j^f, we know the exact f links which have been chosen and we can calculate the link failure probability r_k. The link failure event may not always be independent of each other, particularly in cases where the links are adjacent (have a common end-point). This is more true for optical wireless links, which as we will see later, are highly susceptible to weather conditions. Thus, we calculate the probability of the configuration S_j^f, ($P_{S_j^f}$) as follows -

$$P_{S_j^f} = \begin{cases} \Pi_{k=1}^{i}(1-r_k), \text{ if non-adjacent links fail} \\ (1-r_k^{max}), \text{ otherwise} \\ \quad \text{where } r_k^{max} = \max(r_k) \text{ for the } f \text{ adj. links} \end{cases} \tag{9}$$

Let T_g be the total traffic of nodes in the gth generation and $T^X_{S_j^f}$ be total traffic exposed at the jth configuration of f link failures (which is the sum of traffic of all exposed nodes). Then,

$$\chi_{S_j} = T_g - T^X_{S_j^f} \tag{10}$$

where χ_{S_j} is the exposed traffic at the jth configuration. It is well-known that as the number of failed links (f) increase, the network exposure will increase. However, the probability of f nodes failing will also decrease correspondingly. In order to capture this situation, we model the exposure for f link failures as a discrete random variable (χ_f) which takes a value S_j^f with probability $P_{S_j^f}$. Thus, the average exposure at f link failures is given as,

$$\bar{\chi}_f = \sum_j (S_j^f \times P_{S_j^f}) \;\; \text{j} \in \{\, 1 \ldots \binom{E_g}{f} \,\} \tag{11}$$

Knowing the average exposure, we can also calculate the maximum exposure at the gth generation (χ_g^{max}) as $\chi_g^{max} = max_f(\bar{\chi}_f)$.

The algorithm for network exposure based on the above calculations (Fig. 13(a)) takes exponential time as it does an exhaustive search on all possible combinations. This can be very costly for large-scale access network design. Taking advantage of the self-similar nature of the FraNtiC architecture, we present a linear time recursive algorithm (*NXCalcR*) which gives a lower bound on the exposure for a given generation(Fig. 13(b)). By specifying the seed generation (gBase in the figure) whose exposure we calculate by the exhaustive approach, we can evaluate the minimum exposure at a given generation. The proof of complexity of the algorithms is given in Appendix.

```
NXCalc (g) /*Traffic matrix, distance matrix and
adjacency matrix are computed*/
/* g is the generation whose
network exposure is being computed */
compute $N_g$, $E_g$
for(f=1 to $E_g$ )
for (j=1 to $\binom{E_g}{f}$)
generate new adjacency matrix
with $f$ edges deleted according to the $S_j^f$ configuration
calculate $P_{S_j^f}$ according to Eqn.10
calculate $\chi_{S_j}$ according to Eqn.11
avgExposure = avgExposure + $\chi_{S_j} \times P_{S_j^f}$
EndFor
EndFor
EndAlgo.
                  (a)
```

```
NXCalcR ( g, gBase) /* g is the generation whose
network exposure is being computed */
/* gBase is the base generation */
if ( g equals gBase) minXposure = //calculate
exposure using brute force method
else
minXposure = $min_k$(NXCalcR ( g-1, gBase)), where $k$ is
the number of $g-1$ generation fractal structures.
EndAlgo.
                  (b)
```

Figure 13. Network Exposure Calculation Algorithms

4 Performance Analysis

In this section, we provide the results of our analysis of the *FraNtiC* framework. We start with optical wireless link modeling and present the system cost parameters. Next, we present the results of reliability and network exposure calculations. Finally, we compare our architecture vis-a-vis existing topologies on these system parameters.

Optical wireless technology uses point-to-point laser operating at $785-1550$nm to provide high bandwidth channels. Optical wireless links are characterized by line-of-sight requirements, transceiver characteristics and weather conditions, like visibility, temperature, relative humidity and fog as modeled in [1]. The availability of an optical wireless link depends mainly on the distance between the optical transceivers and the atmospheric attenuation effects [4]. Link availability is expressed by the probability that atmospheric losses are less than the link margin ([4]) which is generally captured in terms of meteorological visibility data. Based on these parameters, we calculate the reliability of optical wireless links as a function of distance, plotted in Fig. 14 (detailed modeling of optical wireless link can be found in [4]).

As mentioned earlier, system deployment cost is an important metric in access network design. System cost is dependant on user traffic patterns, base-stations and con-

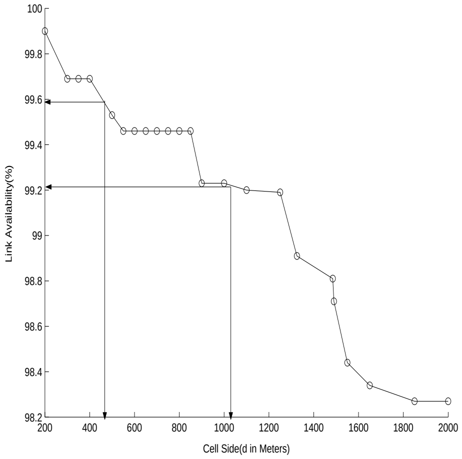


Figure 14. Max. Link Reliability Vs Cell Side

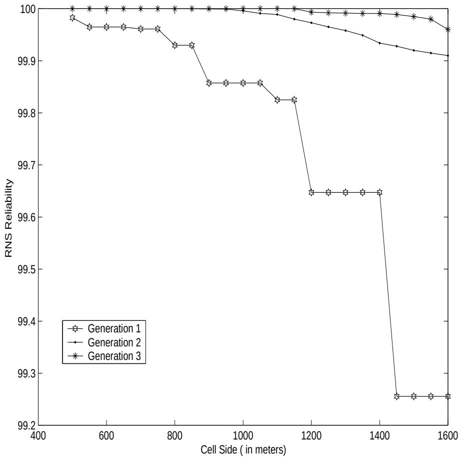


Figure 15. RNS Reliability Vs Cell-Side

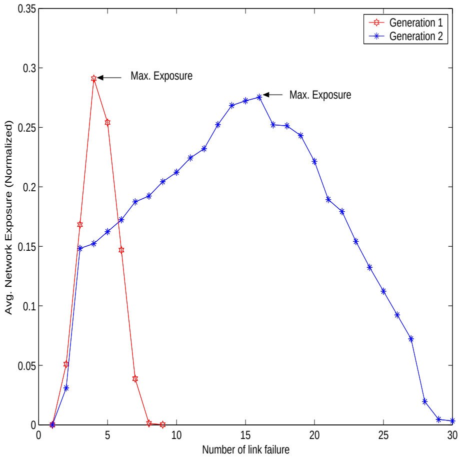
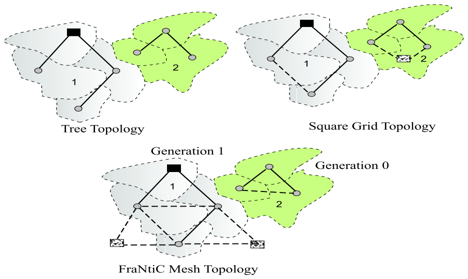


Figure 16. Avg. Network Exposure(Normalized) Vs number of link failures



Cluster No.	System Parameters	FraNtiC	Tree	Square-grid
1	reliability cost exposure (normalized)	99.9826 195700 0,02	99.90 754022 0,06	99.891 195700 0.0395
2	reliability cost exposure (normalized)	99.8936 125700 0,04	99.90 554022 0,05	99.871 125700 0.0395

■ Traffic Concentrator/Hub
▨ Proxy Nodes added in the network
● Network nodes
- - - New Links to support topology structure
—— links in the initial tree topology

Figure 17. Sample Access network (with different topologies)

troller capacities, link distance as well as link technology. We follow the approach in [4], using standard tariffs for existing tree topologies and using optical wireless link costs for square grid and FraNtiC architectures. Cell site traffic is estimated on the number of users, assuming data traffic and is calculated based on effective bandwidth as in [4].

The reliability of the framework is analyzed in terms of RNS Reliability(R^g_{RNS}) at the gth generation as explained in Section 3. RNSs can be formed by grouping various number of nodeBs under the control of a RNC, giving rise to higher generation RNSs. Fig. 15 shows the changing RNS reliability with increasing generations. As can be seen from the figure, even for cell-sides over 1 Km (i.e links with low link reliabilities), the framework is capable of providing carrier-class reliability to the RNSs.

Next, we look into variations of network exposure based on calculations explained in the previous section. Fig. 16 shows how the average network exposure changes with increasing number of link failures. As explained earlier, we find that the exposure initially increases with link failures, but is mitigated when the failure probability of a large number of links become sufficiently low. Another observation is that with increase in generation, the average exposure curve flattens out. However, increasing generations can lead to higher system costs and designers will have to trade-off between these parameters depending on system requirements.

In order to compare the dynamics of these parameters on an access network design scenario, we consider an access network with given cell-sites, their distances and traffic patterns. Now, we employ the *clustering model* proposed by Winter. et al [5] and the modification suggested in [4] to generate optimal tree-based clusters (group of cell-sites under the control of a controller). Then, we change the interconnection within the clusters with the corresponding square-grid and FraNtiC structures. We compare the above mentioned system parameters for each of the topologies

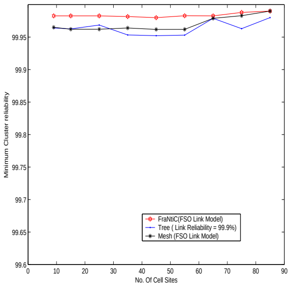


Figure 18. Network Reliability Vs No. Of Nodes

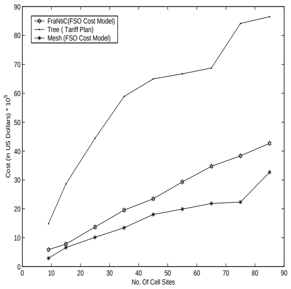


Figure 19. System Cost Vs No. Of Nodes

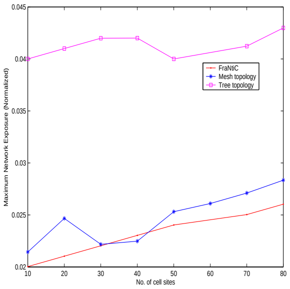


Figure 20. Maximum Network Exposure Vs No. Of Nodes

using different link costs. Fig. 17 gives an illustrative example of an access network with the values of the parameters. Fig. 18 and Fig. 19 gives a comparative study of performance on the three structures on reliability and system cost within increasing number of cell-sites. As can be seen, the system costs for tree topology which uses expensive high-reliability (99.9% and above) links increases. On the other hand, the FraNtiC structure provides carrier-class reliability at significantly lower costs using optical wireless links. Fig. 20 gives the plot of maximum network exposure with increasing cell sites, where the fractal structure performs better on account of topological properties explained earlier. On the whole *FraNtiC* scores over the others with respect to the overall system parameters and emerges as strong candidate for mesh-based access networks.

5 Conclusion

In this paper, we presented a fractal geometric framework which provides a robust, scalable, flexible high-performance system architecture for next generation wireless access network. We compared the architecture in terms of key system parameters against existing backhaul topologies. The FraNtiC architecture provides a flexible framework for incorporating various system parameters in designing future access networks. Our current work is focussed in developing routing strategies in mesh networks which take advantage of this underlying topology and issues related to it. We envision that such multi-technology based, IP-centric access network models will be the call of future wireless systems.

References

[1] A. Acampora and S. V. Krishnamurthy, *A Broadband Wireless Access Network Based on Mesh-Connected Free-Space Optical Links*, IEEE Wireless Communications, Vol. 6, No.5, October 1999.

[2] S. Bloom , W. Hartley Seth, *The Last-mile Solution: Hybrid FSO Radio*. AirFber Inc. www.airfiber.com

[3] T. Otsu, I. Okajima, N. Umeda, Y. Yamao, *Network architecture for mobile communications systems beyond IMT-2000* . IEEE Wireless Communications, Volume: 8 Issue: 5, Oct. 2001.

[4] S.Ghosh, P.De, K. Basu and S. Das, *PeterNet : An Emergent Technology Based Radio Access Network Architecture for Next Generation Cellular Wireless Systems*, in proceedings of *Broadnets*, pp.641-650, 2004.

[5] Ulrich Lauther, Thomas Winter, Mark Zeigelmann, *Proximity Graph Based Clustering Algorithms For Optimized planning of UMTS Access Network Topologies*, ICT 2003.

[6] Reka Albert, Hawoong Jeong, A. Barabasi, *Error and Attack Tolerence of complex networks* . Nature magazine, Vol.406, July 2000.

[7] S. Havlin, A. Bunde, *Fractals and Disordered Systems*, Springer, 1991.

[8] R. Karrer, A. Sabharwal, and E. Knightly, *Enabling Large-scale Wireless Broadband: The Case for TAPs*, HotNets 2003.

[9] L. C. Freeman, *Centrality in social networks: I. conceptual clarification*,Social Networks, 1979.

[10] Samik Ghosh, *Emergent Technology Based Radio Access Network (RAN) Design Framework for Next Generation Broadband Wireless Systems*, http://www.crewman.uta.edu/phdms.htm, May 2004.

[11] S.P Borgatti, M.G Everett, L.C Freeman, *Ucinet for Windows: Software for Social Network Analysis*. Harvard, Analytic Technologies.

[12] Yook Soon-Hyung,Jeong Hawoong, A. Barabasi, *Modeling the Internet's large-scale topology* . PNAS, Vol:99, no.21, Oct 2002.

5.1 Complexity of Network Exposure Algorithms

The complexity of network exposure calculation algorithm, NXCalc is O(2^N), where N is the number of nodes in the network. Its recursive counterpart, NXCalcR gives a lower bound on network exposure in O(N).

Proof: Let $T(g)$ be the running time of the non-recursive algorithm where N is related to g by Property 1. (the subscript g is omitted on N for simplicity). From Fig.14(a), it can be easily verified that,

$$\begin{aligned} T(g) &= \sum_{f}^{\binom{E}{g}} (f \times \binom{E}{f}) \\ &= 2^E \end{aligned}$$

where E is the number of edges/links in the network (subscript g has been omitted for simplicity). Now, from Property 1. E is of the order of N. Thus, T(g) ≈ O(2^N).

The complexity of the recursive algorithm can be found by solving the following recurrence relation.

$$T(g) \quad = k \times T(g-1) + \kappa$$

where κ is the constant time taken to calculate the network exposure for the base generation. Solving the recurrence gives T(g)= O(k^g), where k, which indicates the number of $g-1$ generation structures, depends on the topology. For a fully evolved FraNtiC structure, $k = 4$. Thus, T(g) = O(4^g). Now, from Property 2, we can find that N = O(2^{2g}), which leads to T(g) = O(N). ■