HiFi-WiN: Hybrid Integrated Fiber-Wireless Networking for Broadband Metropolitan Area Access

Vinaykumar Muralidharan Weichao Wang Alexander M. Wyglinski
Information Technology and Telecommunication Center
The University of Kansas, Lawrence, KS, USA 66045-7612
Email: {vinaym,weichaow,alexw}@ittc.ku.edu

***Abstract*— In this paper, we propose a novel HiFi-WiN architecture designed to enhance the error robustness and security of first/last-mile broadband wireless access links within a metropolitan service area. The proposed architecture is capable of employing multi-hop routing for link range extension when attempting to access a mobile user that is not within direct wireless range of any WAP unit. Furthermore, path diversity techniques are employed by the proposed HiFi-WiN architecture in order to enhance the error robustness of the first/last-mile wireless links. Each of these paths could also be multi-hop links. Finally, an authentication mechanism for the HiFi-WiN architecture, based on an extensible authentication protocol (EAP), is proposed in order to secure the network from Denial of Services attacks that could potentially bring down the entire network. Computer simulations have been generated using Network-Simulator (NS) with the results showing the proposed architecture achieving better performance with respect to wireless link error robustness and security when compared to other architectures that do not employ these enhancements, e.g., 30% throughput increase during DOS attacks**

I. Introduction

Wireless frequency reuse is one solution in order to satisfy the growing demand for additional bandwidth from new and existing wireless services. Although often employed in cellular telephony networks, where the data rates between the central office (CO) and the wireless access point (WAP) units are relatively low, applying wireless frequency reuse strategies to broadband wireless networks poses new engineering challenges with respect to the movement of substantial amounts of information over large distances within the network.

One technology that can help support wireless frequency reuse within a broadband wireless access network is hybrid integrated fiber-wireless networking (HiFi-WiN), where the transfer of a large amount of information between the CO and the WAP units, which when compared be separated by distances on the order of kilometers. In this configuration, the fiber optic cables act as "extension cords" between the CO and WAP units, where the conversion between the digital and analog signals is conducted at the CO. As a result, an analog optic transmission format is used for the exchange of information between the CO and the WAP units.

The advantages of an HiFi-WiN are: (i) complex digital processing and network management can be performed at the CO, (ii) WAP unit complexity is kept low due to the simple conversion between optical and wireless transmission, and (iii) the fiber capacity is increased due to the use of an analog optical transmission format. Despite these advantages, there still exist several issues with this architecture. First, most HiFi-WiN architectures only employ a simple (i.e. single-hop) wireless access scheme for reaching the mobile users within the service area, yielding a decrease in wireless link performance the further the mobile user is from the nearest WAP unit. Second, most architectures do not exploit the spatial diversity offered by multiple WAP units, which can be used to counteract the effects of path loss, multi-path propagation, and multi-user interference. Third, methods of enhancing the security of HiFi-WiN architectures with respect to denial-of-service (DOS) attacks have not been fully investigated within the literature.

The rest of the paper is organised as follows, Section II we outline the proposed HiFi-WiN architectural framework that consists of the channel assignment stratergies, Multihop transmissions, Path diversity techniques. In Section III we explain the authenticatin process in the HiFi-WiN network. In Section IV we present the Routing protocol implementations in NS simulator. Section V and Section VI provides a description of the simulation setup and throughput measurements of the network comparing them with the traditional protocols. In section VII we provide some concluding remarks.

II. Proposed HiFi-WiN Architectural Framework

The general layout of the proposed HiFi-WiN architecture is shown in Fig. 1. The network contains several WAP units connected sequentially along a fiber optic cable that runs throughout a service area. Unlike Reference [1], the WAPs in this implementation are attached on a single loop of fiber optic cable to facilitate network/service scalability. The WAP units of the network provide wireless access to the mobile users within the service area, which could be operating one of several services at different center frequencies. The two ends of the fiber optic cable are connected to a CO, which is responsible for managing the transmission of information between mobile users and WAP units, as well as acting as a gateway to other networks. To illustrate the difference

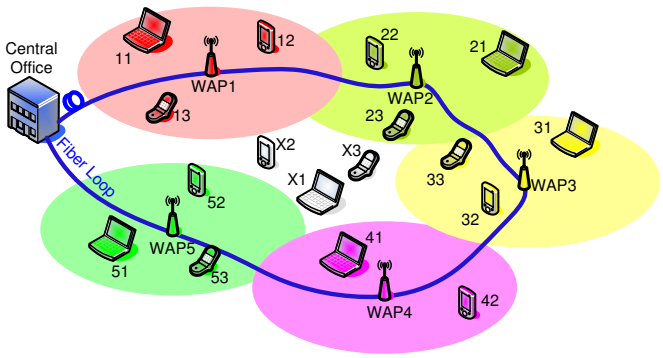

Fig. 1. Schematic of a HiFiWiN architecture for a metropolitan service area.

between current HiFi-WiN implementations and the proposed implementations, we present the following examples:

1) Example 1 - Conventional HiFi-WiN approach: In a conventional approach, wireless links are formed directly between the mobile user and a WAP unit. With reference to the Fig. 1, suppose that WAP1 received information from the CO destined for mobile 12, since it is the closest WAP to this mobile. In order for WAP1 to communicate the received information to the mobile, it must first establish a wireless link with a reasonable level of link reliability. To achieve this, WAP1 would adjust its transmit power level such that the signal strength of the link is sufficient for communications. Once the transmit power level has been adjusted, WAP1 transmits the information to mobile user 12.

Although this approach is straightforward, it has the disadvantage of decreasing the level of spectral reuse throughout the network. For instance, if WAP1 was suppose to communicate with mobile X2, the transmit power required to reliably reach this user will result in a very large transmit radius. As a result, the spectrum used to transmit the information to mobile X2 cannot be used by any other device within this radius.

2) Example 2 - HiFi-WiN employing multi-hop relaying: One of the proposed enhancements to the HiFi-WiN architecture is multi-hop relaying, where the two ends of a wireless link are connected via several intermediate relaying mobiles. Suppose we refer back to our example in Fig. 1 with respect to WAP1 transmitting information to mobile X2. Instead of WAP1 increasing its transmission radius, which results in a reduction of spectral reuse, it can employ multi-hop relaying between itself and mobile X2, with mobile 13 relaying the signal. With the CO coordinating the multi-hop relaying using radio control channels, WAP1 transmits to mobile 13, which in turn retransmits that same signal to mobile X2. As a result, the signal is received by mobile X2 and the spectral reuse of the network is relatively unaffected.

Although the coverage of a network, including the HiFi-WiN implementation, is greatly enhanced by multi-hop relaying, this technique suffers from two problems. The first problem is power consumption, where the cooperating mobiles must expend power in order to assist the relaying operation. This is particularly important if the mobile uses a limited power supply, e.g., battery pack. The second problem is latency, where a delay penalty is incurred every time relaying is performed. For information that is time sensitive, such as multimedia traffic, this is a particularly serious problem. On the other hand, if the relaying operation is restricted to performing long hops, the impact of latency should be reduced [2].

3) Example 3 - HiFi-WiN employing Multiple Services: Another proposed enhancement of the HiFi-WiN architecture is the support of multiple services by the same infrastructure. For example, suppose that the HiFi-WiN implementation supports both wireless local area network (WLAN) as well as the cellular telephony traffic, such as the implementation proposed in [1]. However, unlike [1], all network traffic is handled by a single fiber optic cable to support network scalability. Suppose that mobile 31 is a laptop requiring WLAN service while mobile 31 is a cellular telephone. The CO would transmit both signals simultaneously down the fiber optic cable to WAP3, where two wavelength division multiplexing (WDM) demultiplexers extract the signals. Note that each WAP employs enough WDM units to handle all the services supported by the network. The extracted signals are each transmitted by WAP3 using a dedicated RF chain that is designed to support a specific service. If either mobile is out of range of WAP3, multi-hop relaying can be performed. Otherwise, both mobiles receive the corresponding signals.

4) Example 4 - HiFi-WiN employing path diversity techniques: Considering that the HiFi-WiN architecture can be employed in a metropolitan area, such an environment can potentially lead to poor channel conditions between the WAP unit and a mobile due to multipath propagation, shadowing, and other impairments. To mitigate the effects of distortion introduced to an HiFi-WiN implementation by the wireless channel, several researchers have proposed the use of a simple path diversity scheme called macro-diversity [3–5]. For instance, suppose that mobile 33 does not have LOS conditions with either WAP2 or WAP3 even though it is within range of both WAP units. To enhance the reliability of the wireless link between mobile 33 and the network, the CO can send the same signal to both WAP2 and WAP3 for transmission to mobile 33. As a result, mobile 33 can use the resulting spatial diversity to improve the link reliability.

However, macro-diversity depends on the mobile being within range of two or more WAP units. Building upon the idea of an HiFi-WiN architecture employing multi-hop relaying, the proposed implementation is designed to support more advanced path diversity techniques that use a combination of transmission via several WAP units and multi-hop relaying, such as cooperative diversity or multi-hop diversity. For example,in order to communicate with X3, WAP2 would transmit the signal to mobile 23, which would in turn relay the signal to X3. Similarly, WAP3 would transmit to mobile 33, which would relay the signal to mobile X3. As a result, both wireless paths would experience different amounts of distortion, providing the necessary diversity to enhance the link reliability.

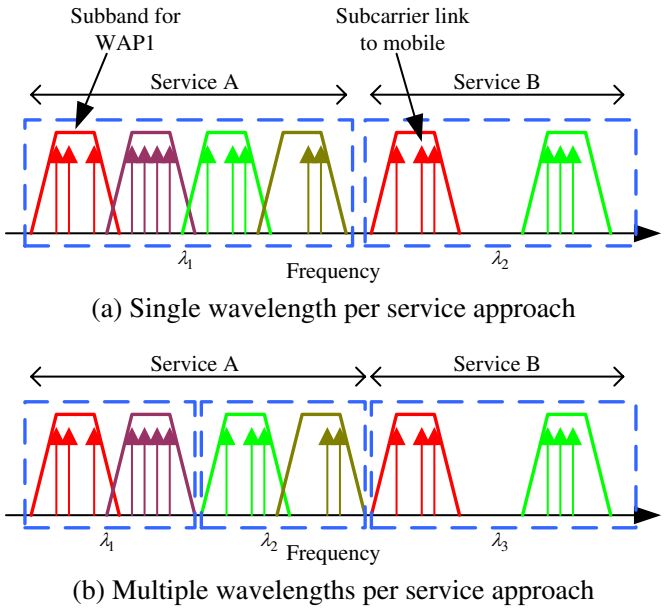

Fig. 2. Frequency domain schematic of channel assignment within proposed HiFi-WiN architecture.

To incorporate these proposed enhancements into the HiFi-WiN architecture, the CO must be capable of assigning channels quickly and efficiently.

A. Channel Assignment Strategies for Multiple Service HiFi-WiN Architectures

Channel assignment strategies [6–15]are designed to efficiently allocate communication links to available portions of spectrum within the network as well as the appropriate WAP units. Within the context of an HiFi-WiN architecture, the channel assignment strategy is performed at the CO. A strategy employed within a HiFi-WiN architecture will potentially use the following information for deciding a channel assignment: (1) the total number of mobile users, (2) the total number of WAP units, (3) the number of supported services, (4) the amount of available optical bandwidth, (5) the bandwidth constraints of the WAP units, and (6) the mapping of mobile users to WAP units based on some metric, e.g., received signal strength. Given these six inputs, the channel assignment strategy must decide on an allocation that supports low complexity implementations of WAP units, makes efficient use of optical bandwidth, and yields a computationally efficient assignment process.

The channel assignment strategy employed in the proposed architecture is based on the principle of grouping. Fig. 2 shows a frequency domain example of the proposed strategy. First, communication links belonging to the same service are grouped together in the same bandwidth, and are assigned a dedicated wavelength known throughout the network. For example, in Fig. 2(a), Service A is supported by λ_1 while Service B is assigned λ_2. By assigning each service to a wavelength, the WDM process for each WAP unit is greatly simplified. Second, with the supported bandwidth of the RF section of each WAP unit being much smaller than the service bandwidth, the service bandwidth is subdivided into subbands. Each subband has a bandwidth that is supported by the WAP RF section, and each subband per service bandwidth is dedicated per WAP unit. As a result, all the WAP unit needs to do is filter out its subband and transmit it. Finally, within each subband is a collection of subcarriers, which correspond to each communication link between the network and a mobile user. Thus, if the channel assignment strategy needs to allocate a signal to a mobile, it simply assigns that signal to the WAP unit(s) closest to that mobile.

Note that the proposed channel assignment support strategy can also assign multiple wavelengths to a service if its bandwidth is heavily populated. For example, in Fig. 2(a), Service A has several subbands allocated to its single wavelength. To balance the spectral occupancy and make WDM extraction/coupling simpler, the proposed channel assignment algorithm allocates two wavelengths to Service A, as shown in Fig. 2(b).

B. Multi-Hop Relaying Transmission

With the channel assignment strategy implemented, the network has the potential to increase its coverage throughout the service area using *multi-hop relaying*. To reduce the setup time of the relaying paths, only the CO decides on and sets up the communication multi-hop paths, implementing those decisions via radio control channels. The algorithm which decides on these paths would need the location information of all the mobiles within the network, their supported service type, and the channel conditions between pair of wireless transceivers, i.e., WAP units and mobiles.

In the proposed architecture, all mobile hosts (MHs) in a WAP service area take part in the topology discovery, wherein each MH regularly sends to the WAP unit information about the beacon power received from its neighbors. This information is used by the WAP unit to estimate distances between MHs. For best-effort communications, all transmissions share a single data channel and a single control channel. An on demand approach is used in the routing protocol. When a source A has a packet to send to the destination B to which a path is not known, it sends a route request packet to the WAP unit over the control channel. The WAP unit responds with a route reply packet containing the route, which is sent back to node A over the control channel. The route is computed using an ad-hoc routing protocol approach. The source A upon the reception of the route reply packet transmits the data packet with the entire route information contained in it, to the next node on the path. The WAP unit also chooses the data channel on which the transmission can take place.

C. Path Diversity Techniques for Enhanced Wireless Link Reliability

With the proposed HiFi-WiN implementation supporting multi-hop relaying, the next step is to devise techniques that would enhance link reliability between the network and a

mobile by employing the principle of diversity. With several mobiles out of range from the WAP units, the only way to reach them is using multi-hop relaying. Suppose that several hops in a relaying path experience poor channel conditions. Thus, some distortion has been introduced to the relayed signal. To correct for this, if the same mobile receives several copies of the same relayed signal transmitted through different paths, it could improve the received signal. This process is called *path diversity*. To employ path diversity within the proposed HiFi-WiN framework, the process requires the same information that is used to perform multi-hop relaying.

To perform path diversity [16], the proposed architecture needs to determine the closest WAP units to the target mobile. Once these WAP units have been determined, the multi-hop relaying algorithm is applied between the target mobile and each of the WAP units to determine the best relaying paths between the network and the mobile. To keep the complexity of the mobile to a minimum, the CO can pre-distort the signal prior to transmission such that the mobile would not need to employ complicated signal processing techniques in order to recover the information. As a result, channel estimation techniques are needed to extract the transmission conditions over the relaying paths.

D. Physical HiFi-WiN Implementation

1) Optical Transmission Format: Analog transmission has stringent requirements on the carrier-to-noise-ratio (CNR), and the signal quality is susceptive to nonlinear transfer characteristics of the system [17]. In general, digital data format is preferred for long distance optical transmission systems for their high tolerance to channel degradations and their ability to be regenerated, analog optical systems are often used in local and metro area networks because of their simplicity and low bandwidth requirement. Although both digital and analog transmission formats can be used in the proposed fiber-wireless network, we only consider analog transmission in this work, thus avoiding the requirement of ultra high capacity DWDM systems and the complications due to high-speed data multiplexing and demultiplexing. As a result, this system will be able to support multiple WAP units and mobile users employing different services with only a few wavelength channels.

In order to minimize the impact of fiber chromatic dispersion and increase optical bandwidth efficiency, optical single-sideband (OSSB) modulation can be employed in the optical transmitter of each WAP unit [18]. Since an OE-EO conversion is needed at each WAP unit, modulation nonlinearity of optical transmitters will be accumulated along the system. Pre-distortion can be applied in the RF domain to minimize inter-modulation distortion [19, 20]

2) Optical-Wireless Interface: Referring to Fig. 3, the WDM module extracts a service wavelength of bandwidth B_{service} and undergoes optical-to-electrical (O/E) conversion. Following the conversion, the subband at frequency f_n that corresponds to this WAP unit is extracted by a bandpass filter and sent to the RF chain for transmission. The same output

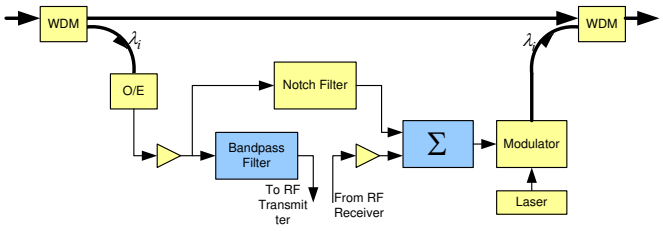

Fig. 3. Schematic of an HiFi-WiN fiber-wireless interface.

of O/E converter is also passed through a notch filter, with the rejection band located at f_n. This signal is then spliced together with the received signal from the RF chain. Once the RF combiner has merged the signals together, the signal is converted back into an optical signal through an electro-optical conversion (E/O) and fed into the fiber optic cable through a WDM multiplexer. The signal then passes through each of the remaining WAP units attached to the fiber optic cable prior to returning to the CO for processing.

III. HiFi-WiN Authentication Process

In a network employing multihop communications [21], malicious nodes can bring down the network in one of several ways, e.g., blackholes, impersonation attacks, denial-of-service attacks, passive attacks, battery exhaustion attacks. In such a case, an authentication and encryption mechanism should be in place to eliminate these malicious nodes from the network.

The routing protocol employed in the proposed architecture uses an *enhanced authentication protocol* (EAP) authentication mechanism [22–24], where the supplicant negotiates with the type of security protocol to be used using the EAP Protocol. It provides credentials using the agreed security mechanism to the WAP unit or undergoing the authentication phase. The WAP units servicing the source and destination nodes negotiate the session keys to be used with the encrypted data. Here, each device in the hybrid network is connected to its corresponding WAP unit within range and employs the authentication mechanism of the WAP unit to reach its neighboring WAP unit. The EAP protocol is used within the WAP unit service area to identify the security mechanism that is used within that area. If the WAP unit servicing the source node is different from that of the destination node, the source node might agree on its own security protocol and the destination node may agree on a different protocol. The WAP unit will make the changes in transmission of the packets in such a network.

A. Generic Authentication Process

When implementing secure integration of a heterogeneous network [25–28], such as the proposed architecture, three tasks needed to be considered: (1) *developing a generic security management protocol that can span the network clouds*, (2) *developing an efficient resource monitoring and planning mechanism*, and (3) *creating techniques to defend against collusive attacks*.

A generic authentication process has six major phases. *Bootstrapping* is the first phase, where a supplicant is securely provided, either offline or online, with something that it should have (a key) or something that it should know (a password) those authenticators would trust as a proof of the supplicant's eligibility to access protected resources or offer service. Once the bootstrapping phase is completed, the supplicant is ready to participate in the network. The *pre-authentication* process is where a supplicant presents its credentials to an authenticator in an attempt to prove its eligibility to access protected resources or offer services. Once the supplicant's credentials are verified, a *credential establishment* process is invoked to establish the supplicant's new credentials, which it will use as a proof of its identity and as a verification of its authorized state thereafter.

A credential could be a symmetric key, a public/private key pair, a commitment of a hash key chain, or some contextual information. The established credentials might be tagged with an expiry date after which the supplicant has to re-negotiate a new "certificate" of credentials. Upon success of all of the steps above, a supplicant is considered authenticated, which means that it is authorized to access resources protected by the authenticator. Within the authentication state, all communications between the supplicant and the authenticator is authenticated by the source and validated at the destination using the established credentials. While authenticated, a supplicant's behavior is *monitored* for fear of it being compromised or misbehaving. A compromised supplicant may get its credentials *revoked* or its *re-establishment* of credentials request denied when its credentials *expire*. In both cases, the supplicant is isolated from the network. In this paper, we will focus on node-to-node authentication.

B. Node Authentication Phase

There are several states that a supplicant can assume during the authentication process. The first state *initializes* the supplicant. In this state, the supplicant is usually supplied with necessary tools to carry on an authentication function. These tools could be supported authentication protocols (e.g., TESLA, 802.1x), authentication credentials (e.g., signed certificates), or identities of trusted entities. At the end of the initialization state, a supplicant has all necessary tools to authenticate to an authenticator [24].

Once a supplicant is initialized, it is ready to move on to the next state, which is *discovery*. During the discovery state, a supplicant scans for reachable services of interest. Each available service is expected to advertise its presence and list service-access requirements. A reachable service is one that is capable of directly making the supplicant aware of its presence (e.g., through periodic advertisements). At the end of the discovery state, a supplicant has a list of reachable services and the service-access requirements for each.

The following state is the *selection* state. Based on the list of reachable services and the service-access requirements of each, a supplicant filters accessible services of interest. The supplicant matches the tools it was supplied with during the initialization state to the service-access requirements advertised by each service. If none of the services match, the supplicant goes back to the discovery state. At the end of the selection state, a supplicant has a list of matching accessible services that are of interest to it.

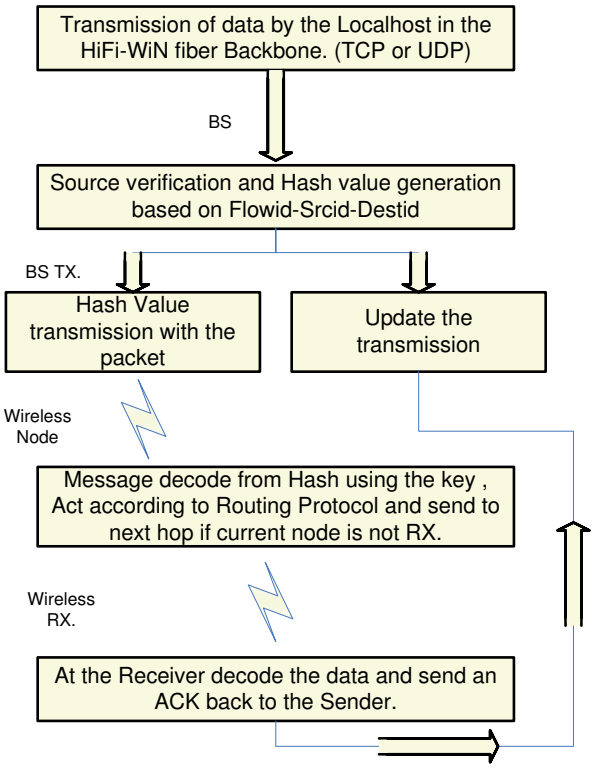

Fig. 4. Authentication process employed in proposed HiFi-WiN architecture.

The next state is the *authenticating* state. The supplicant uses the tools it was supplied with during the initialization state to attempt to authenticate to the authenticator. If the authentication process was successful, the supplicant moves to the authenticated state; if it fails the supplicant goes back to the discovery state. Within the authenticated state, the supplicant is considered *trusted* and is given appropriate access privileges to resources protected by the authenticator. The supplicant is bootstrapped with credentials that can be used to prove its access rights from there after.

Following the authenticated state, the supplicant frequently enters an *evaluation* state where its behavior is examined. Based on the outcome of the evaluation process the supplicant could either return back to the *authenticated* state (i.e. well behaving) or is put under *probation* (i.e. selfish or malicious). The probation state comes next, in which the supplicant enters as a penalty if it was determined to have behaved inappropriately. Eventually, the supplicant would be re-evaluated and given a chance to recover.

IV. Routing Protocol Design

The routing protocol used is similar to the base station-assisted routing (BAAR) protocol. This protocol is imple-

mented by integrating the EAP with BAAR protocol shown in Fig. 4. The source agrees with the WAP unit on the authentication mechanism using the EAP protocol and transmits to the WAP unit on a random access channel (RACH) for establishing a connection to the network. The authentication server present in the WAP unit authenticates the node [29]. Upon authentication, the node will send a request on the destination it wants to communicate if the destination is present within the service area which is checked by the WAP unit using its HLR and VLR then obtains a route on demand. Then, the route is sent to the source node. If the destination node is present in the same service area, the packet is directly encrypted and transmitted in an ad-hoc mode. If the destination node is in another service area, the packet is transmitted to the WAP unit, which transmits to the WAP unit servicing the destination node. The transmission is then communicated to the destination node from the WAP unit using multihop communications.

The routing protocol uses Heirarchial Addressing, scheme of addressing structure is used in the network by which the nodes are registered to a single BTS or multiple BTS using the addressing struc- ture. The routing information for wired nodes are based on connectivity of the topology, i.e how are nodes connected to one another through links. However wireless nodes have no concept of links. Packets are routed in a wireless topology using their adhoc routing protocols which build forwarding tables by exchanging routing queries among its neighbours. So in order to exchange pkts among these wired and wireless nodes base-stations are used which act as gateways between the two domains. The addressing provides different levels of hierarchy for data exchange between nodes in the same cluster and are in the format similar to IP addressing.

V. Simulation Setup

Simulations were performed in ns-2.31, employing the CMU wireless models for simulating multi-hop wireless networks with physical, data link, and MAC layer models. The distributed coordination function (DCF) from the IEEE 802.11 standard was used in the MAC layer. The radii model employed characteristics based on Lucent WaveLAN product.

The network possessed an overall service area of 2000×2000m, with a simulation runtime ranging from 100 to 300 seconds. The simulation investigated a HiFi-WiN architecture consisting of eight WAP units connected via a single fiber loop. The network supported up to 300 wireless nodes that were randomly placed throughout the service area. Note that all of the wireless nodes were assumed to be stationary. During each simulation runtime, 100 TCP/UDP connections were generated at random between a pair of wireless nodes within the network. An example of our simulation network layout is shown in Fig. 5.

The hierarchical addressing was employed in the network to help with integrating the wireless nodes with the WAP units, which follows the `Domain.Cluster.Node` pattern of generating the addresses. These addresses are generated

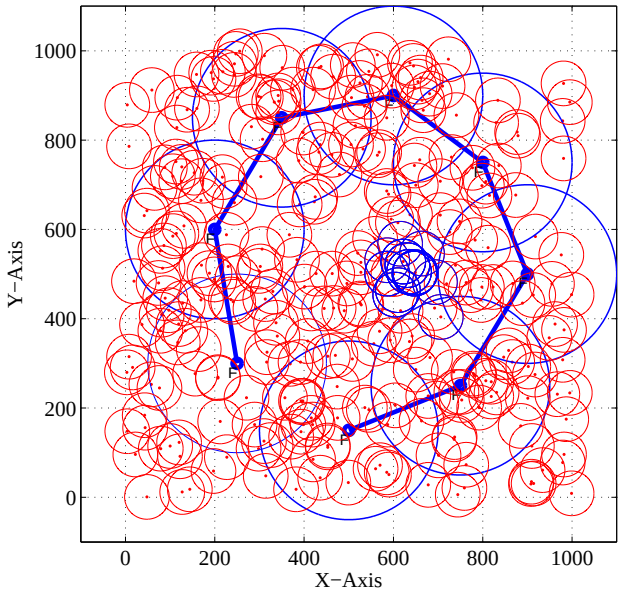

Fig. 5. Example layout of a metropolitan area-based HiFi-WiN architecture employing 8 WAP units (blue) connected with fiber links and 300 mobile nodes (red) with transmission ranges indicated.

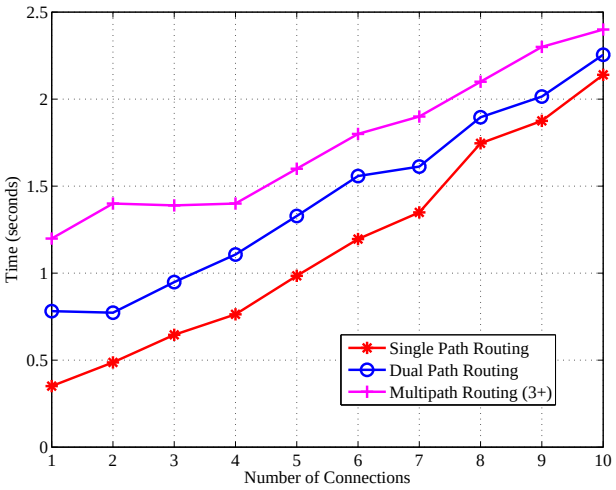

Fig. 6. Route computation time graph shows convergence of multipath routing to the single path routing with increase in the number of connections.

using the network discovery protocol (NDP) implemented in C++. AODV routing protocol [30] is used for routing the data packets to the mobile nodes from the WAP units.

VI. Simulation Results

A. Route Computation Time

The route computation time between the routing protocols was measured using the number of simultaneous connections that were generated. The protocol employed by the proposed architecture is compared with a simple OSPF route computation. From Fig. 6, we can see that the routing protocol converges to the same approximate time when the number of connections are high which are expected in a network across

TABLE I

THROUGHPUT COMPARISION FOR DATA PACKETS WITH AUTHENTICATION AND WITHOUT AUTHENTICATION ENTERING ON TO THE NETWORK.

Num Malicious Nodes	Sim No Auth	Sim with Auth
5	0.9176	0.9614
10	0.8913	0.7574
20	0.8467	0.9354
30	0.7832	0.926
40	0.6743	0.9148

boundaries.

The protocol initially took more time to compute the routing path since its design involves more route discoveries and route maintenance relative to simple OSPF. However, when the number of connections increases the time taken for route discovery and maintenance gets averaged out. The route computation times shown in the graphs are average times over 100 simulation runs.

B. Throughput Measurements

The trace files are then analyzed for throughput by analyzing the number of packets that are reaching the destination with and without the authenticator. Table I clearly shows that the authenticator in place increases the throughput of the system.

Since the malicious nodes are generated at random the seed in the generator is such that the nodes get generated in the middle of the network where the back bone is located. Hence, when the number of malicious nodes increases we see a significant packet loss. If the malicious nodes are located at the farther end, its impact will be much lesser than what we see in Table I. Also the authenticator increases the throughput significantly as the malicious nodes are eliminated from the system. The error we see in the authenticator is due to the use of wireless physical channel of the ns-2 simulation model which implements a default channel error model for dropping the packets. Hence we see that the authenticated BAAR protocol will provide a high amount of throughput which is a necessary requirement for any service.

Fig. 7 clearly shows the performance of the authenticator in the system to the degradation of the system due to the malicious node attacks without the authentication mechanism. We can see that the throughput increases as the number of dropped gets reduced. In the case of malicious nodes making TCP SYN attacks the authenticator in place reduces the throughput. Also, the goodput (i.e., amount of correct transmissions without any retransmission) using the TCP connection increases. The communication overhead is more but is required for the safety of data transmission.

C. Path Diversity Results

Fig. 8 presents the network throughput when the proposed architecture employs a path diversity routing approach. Also shown is the result of the network performing a single path ad-hoc routing approach. Ad-hoc on demand distance vector (AODV) routing is chosen to be the traditional protocol for this comparison. The trace file obtained through the ns-2 simulation model is analyzed for throughput at a particular receiving node which employs an error model that is varying over time to simulate the characteristics of channel fading.

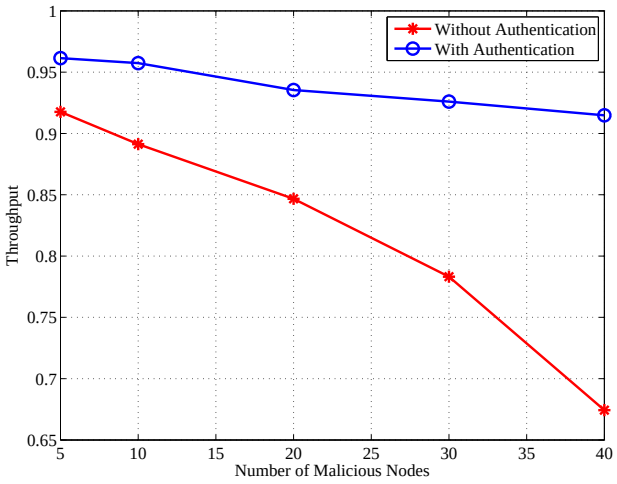

Fig. 7. Throughput graph showing the percentage quality of data with and with out authentication of nodes arriving at the receiving nodes.

From Fig. 8, we observe that the single path routing protocol does not perform well in the time-varying conditions as it can provide only a single route to the destination node from the source node. The protocol only reaches maximum throughput at only a few time instances when the amount of error is at a minimum. Conversely, the path diversity-based protocol maintains nearly a maximum throughput level due to the transmission of same packets from different neighboring nodes which provides additional redundancy to the communications between two nodes, increasing the data quality at the destination nodes. When the error-rate is high, the single hop performs very badly which is understandable due to the excess fade in the channel. However, this does not influence the multi-path routing approach as the packet gets received from some other route to the destined node and the destined node gets its data.

VII. CONCLUSION

The proposed HiFi-WiN architecture is capable of enabling ubiquitous broadband wireless coverage throughout a metropolitan service area that can support a large number of mobile users. Combined with multi-hop routing and path diversity, the first/last mile of the communications links with these mobiles can be made more reliable as well as extend their overall transmission range.

ACKNOWLEDGEMENTS

The authors would like to thank Dr. Rongqing Hui for his insights on the physical implementation of the fiber optic component for the proposed HiFi-WiN architecture.

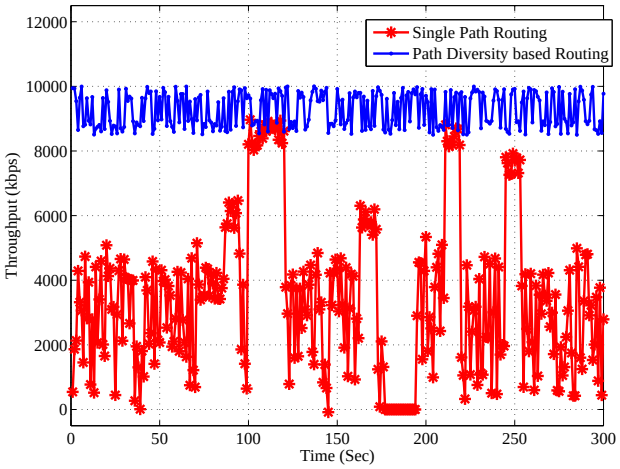

Fig. 8. Throughput graph showing the performance of path diversity based authenticated HiFi-WiN network comparing with traditional AODV protocol.

REFERENCES

[1] R. Yuen and X. N. Fernando, "Analysis of sub-carrier multiplexed radio over fiber link for the simultaneous support of WLAN and WCDMA systems," *Wireless Personal Communications*, vol. 33, pp. 1–20, Apr. 2005.

[2] M. Haenggi and D. Puccinelli, "Routing in ad hoc networks: A case for long hops," *IEEE Communications Magazine*, pp. 93–105, Oct. 2005.

[3] N. Khashjori, H. S. Al-Raweshidy, and A. Bajwa, "Macrodiversity performance in the uplink of WCDMA with radio over fibre access network," in *13th IEEE International Symposium on Personal, Indoor, and Mobile Radio Communications*, vol. 3, pp. 1367–1371, Sept. 2002.

[4] N. Khashjori, H. S. Al-Raweshidy, and A. Bajwa, "The performance of macrodiversity in the downlink of WCDMA with radio over fibre access network.," in *5th International Symposium on Wireless Personal Multimedia Communications*, vol. 2, pp. 362–366, Oct. 2002.

[5] L. Smoczynski and M. Marciniak, "A comparison of different radio over fibre system concepts with regard to applications in mobile internet and multimedia," in *4th International Conference on Transparent Optical Networks*, vol. 1, pp. 211–213, Apr. 2002.

[6] D. C. Cox and D. O. Reudink, "Some effects on channel occupancy of limiting the number of available servers in small cell mobile radio systems using dynamic channel assignment," *IEEE Transactions on Communications*, vol. COM-27, pp. 1224–1226, Aug. 1979.

[7] D. C. Cox and D. O. Reudink, "Increasing channel occupancy in large-scale mobile radio systems: Dynamic channel reassignment," *IEEE Transactions on Communications*, vol. COM-21, pp. 1302–1306, Nov. 1973.

[8] D. C. Cox and D. O. Reudink, "A comparison of some channel assignment strategies in large scale mobile communication systems," *IEEE Transactions on Communications*, vol. COM-20, pp. 190–195, Apr. 1972.

[9] J. C. I. Chuang, "Performance issues and algorithms for dynamic channel assignment," *IEEE Journal on Selected Areas in Communications*, vol. 11, pp. 955–963, Aug. 1993.

[10] G. Vidyarthi, A. Ngom, and I. Stojmenovic, "A hybrid channel assignment approach using an efficient evolutionary strategy in wireless mobile networks," *IEEE Transactions on Vehicular Technology*, vol. 54, pp. 1887–1895, Sept. 2005.

[11] K. Smith and M. Palaniswami, "Static and dynamic channel assignment using neural networks," *IEEE Journal on Selected Areas in Communications*, vol. 15, pp. 238–249, Feb. 1997.

[12] S. K. S. S. K. Das and R. Jayaram., "A dynamic load balancing strategy for channel assignment using selective borrowing in cellular mobile environment.," *ACM Wireless Networks*, vol. 3, no. 5, pp. 333–347, 1997.

[13] S. S. Kuek and W. C. Wong, "Approximate analysis of a dynamic-channel-assignment scheme with handoffs," *IEEE Proceedings on Communications*, vol. 141, pp. 89–92, Apr. 1994.

[14] D. Hong and S. S. Rappaport., "Traffic model and performance analysis for cellular mobile radio telephone systems with prioritized and non-prioritized handoff procedures.," *IEEE Transactions on Vehicular Technology*, vol. VT035, no. 3, pp. 77–91, 1986.

[15] D. Everitt and D. Manfield, "Performance analysis of cellular mobile communications systems with dynamic channel assignment," *IEEE Journal on Selected Areas in Communications*, vol. SAC-7, no. 10, pp. 1172–1180, 1989.

[16] R. Teixeira, K. Marzullo, S. Savage, and G. M. Voelker, "In search of path diversity in ISP networks," in *3rd ACM SIGCOMM Conference on Internet Measurement*, (New York, NY, USA), pp. 313–318, ACM Press, 2003.

[17] M. R. Phillips and T. E. Darcie, "Lightwave analog video transmission," in *Optical Fiber Telecommunications IIIA* (I. P. Kaminow and T. L. Koch, eds.), 1997.

[18] R. Hui, B. Zhu, R. Huang, and C. Allen, "10gb/s scm system using optical ssb modulation," *IEEE Photonics Technol. Lett.*, vol. 13, no. 8, 2001.

[19] S. Betti, E. Bravi, and M. Giaconi, "Effects of intermodulation distortions due to the joint action of dynamic chirping and dispersive transmission of scm optical signals," *IEEE Photonics Technol. Lett.*, vol. 11, no. 6, pp. 680–682, 1999.

[20] H. Gysel and M. Ramachandran, "Electrical predistortion to compensate for combined effect of laser chirp and fibre dispersion," *Electronics Letters*, vol. 27, no. 5, pp. 421–423, 1991.

[21] M. Marina and S. Das, "On-demand multipath distance vector routing in ad hoc networks," in *IEEE International Conference on Network Protocols*, pp. 14–23, 2001.

[22] D. Park, C. Boyd, and E. Dawson, "Classification of authentication protocols: A practical approach," in *Third International Workshop on Information Security*, (London, UK), pp. 194–208, Springer-Verlag, 2000.

[23] L. Venkatraman and D. Agrawal, "A novel authentication scheme for ad hoc networks," in *IEEE Wireless Communications and Networking Conference*, vol. 3, 2000.

[24] A. A. Pirzada and C. McDonald, "Kerberos assisted authentication in mobile ad-hoc networks," in *27th Australasian Conference on Computer Science*, pp. 41–46, 2004.

[25] J. B. Evans, W. Wang, and B. J. Ewy, "Wireless networking security: open issues in trust, management, interoperation, and measurement," *International Journal of Security and Networks*, vol. 1, no. 1/2, pp. 84–94, 2006.

[26] B. Bhargava, X. Wu, Y. Lu, and W. Wang, "Integrating heterogeneous wireless technologies: a cellular aided mobile ad hoc network (CAMA)," *Mob. Netw. Appl.*, vol. 9, no. 4, pp. 393–408, 2004.

[27] M. Danzeisen, T. Braun, D. Rodellar, and S. Winiker, "Heterogeneous network establishment assisted by cellular operators," in *5th IFIP TC6 International Conference on Mobile and Wireless Communication Networks*, (Singapore), 2003.

[28] N. Aboudagga, M. T. Refaei, M. Eltoweissy, L. A. DaSilva, and J.-J. Quisquater, "Authentication protocols for ad hoc networks: taxonomy and research issues," in *1st ACM International Workshop on Quality of Service & Security in Wireless and Mobile Networks*, (New York, NY, USA), pp. 96–104, ACM Press, 2005.

[29] P. Traynor, W. Enck, P. McDaniel, and T. L. Porta, "Mitigating attacks on open functionality in sms-capable cellular networks," in *12th Annual International Conference on Mobile Computing and Networking*, (New York, NY, USA), pp. 182–193, ACM Press, 2006.

[30] C. E. Perkins, E. M. Belding-Royer, and S. Das, "Ad hoc on demand distance vector (aodv) routing.," in *IETF RFC 3561*, July 2003.