A FRAMEWORK FOR THE SELF-CONFIGURATION OF WIRELESS MESH NETWORKS

by

Adeolu Oluwaseun Adeoye

A thesis
presented to the University of Waterloo
in fulfilment of the
thesis requirement for the degree of
Master of Applied Science
in
Electrical and Computer Engineering

Waterloo, Ontario, Canada, 2009

AUTHOR'S DECLARATION

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

ABSTRACT

The use of wireless radio technology is well established for narrowband access systems, but its use for broadband access is relatively new. Wireless mesh architecture is a first step towards providing high-bandwidth wireless network coverage, spectral efficiency, and economic advantage.

However, the widespread adoption and use of Wireless Mesh Networks (WMN) as a backbone for large wireless access networks and for last-mile subscriber access is heavily dependent on the technology's ease of deployment. In order for WMNs to be regarded as mainstream technology, it needs to gain a competitive edge compared to wireline technologies such as DSL and cable.

To achieve this, a broadband wireless network must be self-configuring, self-healing and self-organizing. In this thesis, we address these challenges. First, we propose a four-stage scheme (power-up, bootstrapping, network registration, and network optimization). We develop algorithms for each of these stages, taking advantage of the inherent properties of WMNs to determine the network's topology.

The novel part of our scheme is in the de-coupling of the subscriber's credentials from the network hardware. This is a key part of our architecture as it helps ensure quick network enrolment, management and portability. It also helps, in our opinion, make the concept of widespread deployment using commodity hardware feasible.

ACKNOWLEDGMENTS

I wish to express my sincere gratitude and appreciation to Prof. Paul A.S. Ward for his valuable supervision and assistance in the preparation of this manuscript. Your patience and guidance throughout this process was instrumental to its successful completion.

I would like to thank Profs. Sagar Naik and Guang Gong for reviewing my thesis and providing their feedback.

I would like to thank my colleagues at the University of Waterloo for providing a wonderful academic experience and friendly environment during my Masters' program. In addition, special thanks to the wireless research group whose familiarity with the subject and critical feedbacks were essential to the development of this work.

I would like to thank God for providing the most wonderful set of parents in the world. Thank you for always encouraging me to chase my dreams. Finally, I thank Abimbola for gently prodding me whenever I was distracted and for filling my life with love and joy.

To everyone that I did not to mention by name, blame it on the head and not the heart. Thanks for your support throughout this journey.

TABLE OF CONTENTS

LIST OF FIGURES

C h a p t e r 1

INTRODUCTION

Wireless technology is well established but its use for commercial broadband access is relatively new. Wireless mesh architecture is a first step towards providing high-bandwidth network coverage. It is critical to large-scale wireless networks with no pre-existing infrastructure as it enables quick-and-easy extension of a local area network into wider area. The Mesh architecture helps sustain signal strength by breaking long distances into a series of shorter hops. Intermediate nodes not only boost the signal, but cooperatively make forwarding decisions based on their knowledge of the network. Such architecture provides high network coverage, spectral efficiency, and economic advantage.

The major incentives for the deployment of wireless mesh networks come from their envisioned advantages: extended coverage, robustness, self-configuration, easy maintenance, and low cost. In spite of the high attention and the massive efforts on research and development, wireless mesh networks have not yet widespread adoption. One of the key economic drivers of WMN is that they are quicker and cheaper to deploy than existing wireline technologies. It has been noted that without this key incentive, WMNs will not achieve acceptability in the marketplace.

Recently, interesting commercial applications of wireless mesh networks (WMN) have emerged. One example of such applications is "community wireless networks". Several vendors have recently offered WMN products. Some of the most experienced in the business are Nortel [1], Cisco Networks [2], Tropos Networks [3], and BelAir Networks [4]. There has been a lot of startup activity in this technology space as the concept of the ubiquitous wireless access holds a lot of promise. The promise is supported as well by the work of standards bodies such as the IEEE 802.11s Working Group [5]. However, much more remains to be done before WMNs realize their full potential.

One major obstacle to the widespread deployment of WMNs as a connectivity solution for large wireless access networks is the long-term operational efficiency of running such a network. In today's world of rapid technology innovation, the cost of hardware (capital expenditure or

'CapEx') is rapidly falling while the cost of running the infrastructure (operational expenditure or 'OpEx') keeps rising. Hence, even though WMNs offer the promise of quick and easy deployment (in comparison with wired access technologies), the cost of maintaining a stable level of service is still prohibitively high. As a result, over the lifetime of a network, wired access networks may actually turn out to be cheaper. As noted in [6], the large footprint of wired alternatives e.g. Cable and DSL in urban areas also poses questions concerning the suitability of wireless technology as an alternative for last-mile connectivity.

One key strategy to help make WMNs more competitive as a viable last-mile access technology is to make it possible for the network to automatically configure wireless mesh nodes in a distributed fashion while ensuring security and resource conflict resolution. While this may sound daunting at first, the inherent properties of a WMN allow us to devise interesting schemes to address the issue. The wireless backbone of mesh routers mainly relays mobile clients' traffic to and from the Internet via gateways connected to the wired network. As a result, most of the traffic is directed to and processed by a few nodes (gateways). These nodes would form bottlenecks as more and more packets contend for the channel as they are forwarded closer towards them. The network scales better when the traffic pattern is kept *local* i.e. each node sends only to nearby gateways within a fixed radius, independent of the network size. For optimal performance, the WMN should be subdivided into disjoint trees (clusters). Within each tree, the "root" would serve as the gateway, connecting the nodes to the wired backbone. Strategically placing and connecting the gateways to the wired backbone is therefore critical to the management and efficient operation of a WMN.

In this work, we seek to address this challenge by proposing a solution for the self-configuration of WMNs. We describe a feasible architecture for wireless mesh networks utilizing a practical view on the usage scenarios. We also explore critical factors influencing the performance and scalability of these networks, security issues (to ensure only authorized users are granted network access), billing/accounting that is beneficial for clients as well as providers.

I. CONTRIBUTIONS

Our contributions can be summarized as follows.

We propose an algorithm for the provisioning of wireless subscriber connectivity. This algorithm allows end-point WMN nodes to be automatically provisioned and configured in a secure, distributed and conflict-free manner. It also introduces the concept of decoupling the service from the hardware. No other work in the literature presents a similar concept.

The algorithm is both distributed and centralized. The distributed portions include neighbour discovery, topology construction and beaconing. The centralized aspects include monitoring agents deployed on nodes (used to monitor device and network metrics) and report to the central station, QoS and SLA guarantees and security. A key aspect of our architectural framework is that is readily lends itself to a service-provider based service model. We believe this is a critical feature of the system because, as we have already shown, WMNs have to pass the economic litmus test to be considered a viable technology for the future.

II. OUTLINE

The thesis is organized as follows. Chapter 2 presents WMN characteristics and motivate our work. Chapter 3 describes the architectural framework in detail and addresses the service provisioning issues in a WMN. Chapter 4 presents an analysis of the merits of the system and how it addresses the prevailing issues with WMN deployments today. Chapter 5 concludes our work.

C h a p t e r 2

THE CASE FOR WMNs

Wireless mesh networks (WMN) have emerged as a key technology for next generation wireless networks, showing rapid progress and inspiring numerous applications. WMNs seem significantly attractive to network operators for providing new applications that cannot be easily supported by other wireless technologies. The major incentives for the deployment of wireless mesh networks come from their envisioned advantages: extended coverage, robustness, self-configuration, easy maintenance, and low cost. Yet, in spite of the high attention and the massive efforts on research and development, wireless mesh networks have not yet witnessed mass market deployment. To promote the deployment of wireless mesh networks and enhance their usage, many factors have to be considered. One of the key economic drivers of WMN is that, all things being equal, they are quicker and cheaper to deploy than existing wireline technologies. It has been noted that without this key incentive, WMNs will not achieve acceptability in the marketplace.

In this work, we seek to address this challenge by proposing a solution to the self-configuration of WMNs. We describe a feasible architecture for wireless mesh networks utilizing a practical view on the usage scenarios. We also explore critical factors influencing the performance and scalability of these networks, security issues (to ensure only authorized users are granted network access), as well as billing/accounting that is beneficial for clients as well as providers.

I. INTRODUCTION

A WMN is a two-tier architecture based on wireless multi-hop transmission. A WMN is composed of Wireless Mesh Clients (WMC) and Wireless Mesh Routers (WMR). The latter offers connectivity to the former by acting like access points (APs), forming at the same time a self-organized wireless backbone. It is possible that the WMC may have clients themselves. A typical example will be a wireless home router that connects various peripherals in the home such as computers, printers, set top boxes and other

This backbone has two possible roles. It can be either a standalone network simply offering inter-client connectivity or a local extension for the wired Internet if there are available connections between one or more WMR gateways. In both cases, the WMN's backbone is in charge of relaying all the traffic from/to WMCs.

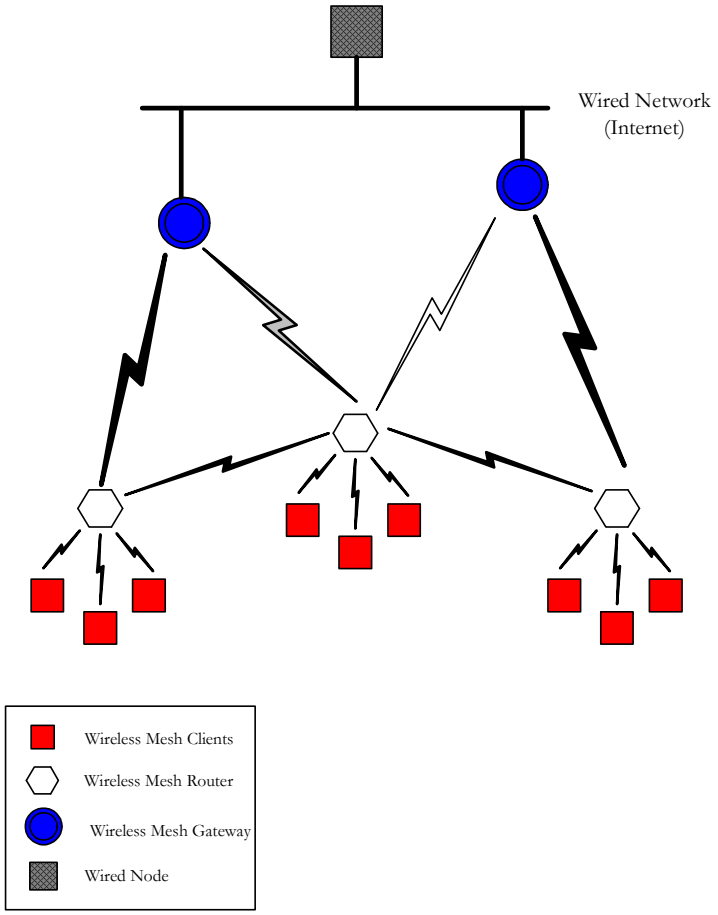

Figure 1 WMN Model

The WMRs typically have multiple radio interfaces that serve as either backhaul or access links. The backhaul links connect to other WMRs (backbone communication) while the access links (client communication) connect to the WMCs. Typically the radio transmission is low power to reduce the impact of interference in the network thereby

extending its range. Communication in a WMN is heavily reliant on multi-hop communication.
The IETF CAPWAP WG gives an architecture example of WMNs in [7] and a comprehensive survey on WMNs and related issues can be found in [8].

WMNs offer considerable advantages as an Internet broadband access technology [9] [10]:

- *Spectral efficiency:* The average link length and the average transmit power level fall as subscriber density rises. This is equivalent to moving from macro cells to micro cells, but without needing a large change in the network design.
- *Minimal risk of blind spots which means network coverage can approach 100%:* Due to its multihop routing ability, line of sight to a single base station is not required; as long as a client has connectivity to any other client, it can obtain Internet access. It was shown in [11] that a WMN can significantly improve the coverage in comparison with point-to-multipoint (e.g., IEEE 802.16) solution, especially for scenarios with significant obstructions trees or skyscrapers.
- *Economic advantage:* WMN has the advantage that customers' wireless access points (routers) make up most of the equipments needed for the system. Upfront investments are minimal because the technology can be installed incrementally, one node at a time, whenever new customers request an access to the network. In addition, omni-directional antennas are normally used, which eliminate the cost and installation time (i.e. eliminates the burden of pointing antennas). In WMNs, clients associate to a WMR without the need to run any routing feature or particular software module. This characteristic, coupled with the other advantages such as reduction in deployment cost, connecting hard-to-wire areas, resilience, self organization and self healing behaviour and the extensibility make the WMN architecture very appealing to network operators and service providers. However, practical issues, particularly relating to performance, quality of service, security, network management and monitoring, scalability etc. need to

be solved in order for WMNs to have a commercial breakthrough as a suitable technology for network operators and service providers.

- *Fast Deployment:* Adding a new client to an existing WMN can take several hours instead of several months, the typical delay for installing new wires for cable or DSL.
- *Pleasing Aesthetics:* There are many settings that can benefit from the lack of unsightly wires associated with Ethernet networks (e.g., show halls, airports, historic buildings, etc.).

II. WIRELESS MESH ARCHITECTURES

Wireless Mesh Networks (WMNs) architectures can be classified into three main groups based on the functionality of the mesh nodes: Client mesh, Infrastructure mesh and Hybrid mesh [8]. Figure 2 illustrates an example of this classification.

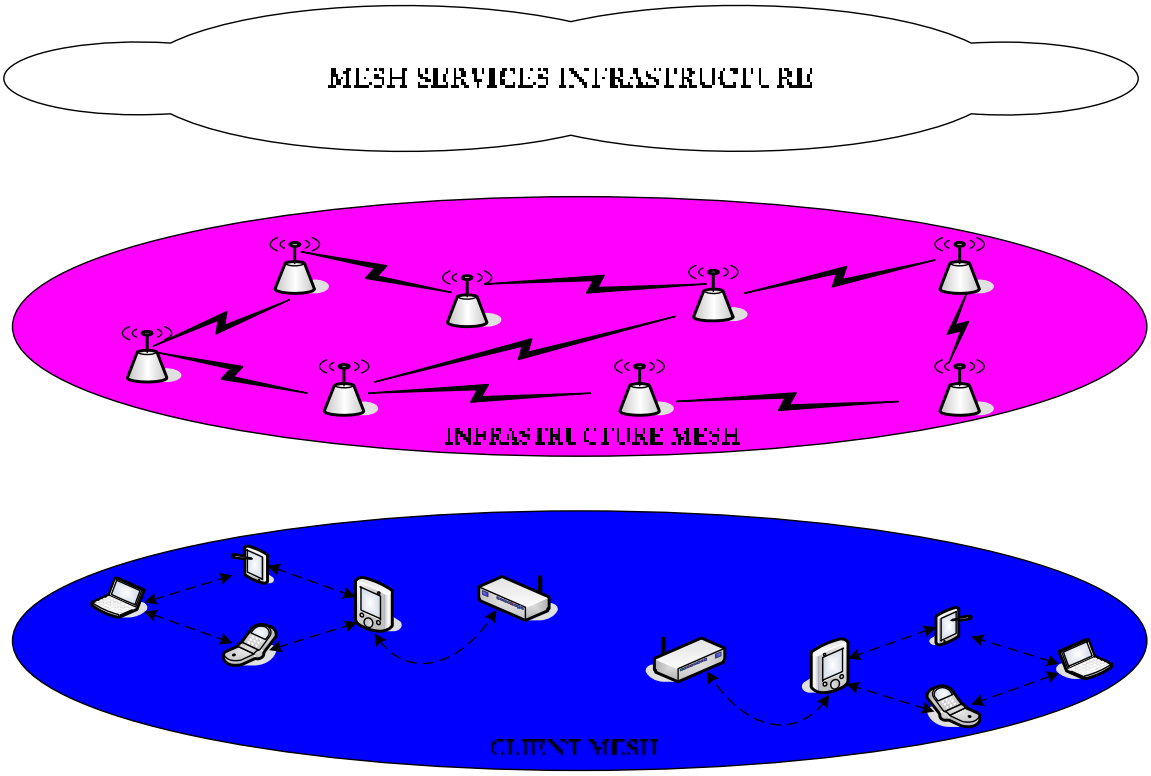

Figure 2 Mesh Network Architectures

The lower tier in the architecture diagram corresponds to the client mesh architecture which provides peer-to-peer ad-hoc connections among the mesh clients. This is also referred to as pure mesh, where most of the traffic is classified as intra-mesh traffic. In contrast, the infrastructure mesh architecture is portrayed at the middle-tier where mesh routers form a backbone infrastructure of self-healing, self-configuring links among themselves, for clients that connect to them. The top tier illustrates the services (e.g Internet) that can be accessed via the lower tiers. The hybrid mesh architecture, where mesh clients can connect to the service infrastructure through mesh routers as well as directly meshing with other mesh clients (assuming that the mesh clients can be directly connected to the service infrastructure). The traffic flows and hence the appropriate architecture depends on whether the content to be accessed is inside or outside the mesh. Thus, the type of mesh architecture required in a given situation is typically driven by the user and application needs for content [12]. This architecture is the most applicable for commercial WMN deployments.

In a WMN, customers' wireless access points make up most of the equipment needed for the rollout of the system. Each wireless access point (node) acts as a means of connecting that customer to the network and possibly forwarding neighbouring node traffic, extending the reach of the network. A dedicated radio is used for access links and remaining radios used for traffic forwarding (i.e. transit links). Also, a WMN has a relatively stable topology except for occasional nodes failure or addition. The traffic in the backbone, being aggregated from a large number of end users, changes infrequently. The wireless backbone of mesh routers mainly relays users' traffic to and from the Internet via gateways connected to the wired network.

III. APPLICATIONS AND SCENARIOS

Mesh networks have the potential to bring diverse advantages to wireless communications services, allowing clients to exchange information in a decentralized manner and also to extend coverage of cellular and other networks by allowing relay based networking at the edge terminals. Most of the technical challenges in mesh networks depend to a large extent on the environment and usage scenarios in which wireless mesh networks are used. Generally, wireless mesh networks can be classified into open and closed networks [13]. In open mesh networks, any client node may participate. These networks may belong to different operators or administrative domains constituting a mesh federation [14]. On the other hand, in closed or managed mesh networks, a certain authority exists and only known client nodes are accepted to join the mesh network. Based on these criteria, different usage scenarios are possible for both indoor and outdoor wireless mesh networks.

There is no shortage of practical usage scenarios and applications for closed and open mesh networks. These include a single meshed home network managed by the network owner for broadband home networking applications; a closed set of mesh nodes in a military environment where traffic flow must be kept confidential, thereby making the soldier-soldier communication more reliable and with a longer range; mesh APs deployed in university campuses or providing inexpensive campus-wide network coverage; an enterprise mesh network eventually eliminating the Ethernet backhaul for office WLAN based networks, which are particularly useful in office networking scenarios and also for health and medical system applications. There has also been a movement towards deploying community mesh networks (CMNs). These are typically deployed by operators in residential zones for provisioning of grass-roots communities wireless networks allowing them to share Internet connections via gateways. Most of these deployments have been proof-of-concept and experimental in nature and not commercial in nature e.g. Roofnet [15]. Metro scale mesh networks are a broader version of CMNs which covers an entire metropolitan area in order to capacitate

different city, county/municipality wide efforts for wireless broadband services, intelligent transportation services etc.

Open mesh networks also provide excellent opportunities for mission critical applications and public safety efforts, particularly for emergency operations and for vehicular communications. With the vision of future communication infrastructure often being quoted with respect to the integration of all mobile and wireless nodes with the IP core, multiple 'last-mile' connectivity options need to become a reality. WMNs can provide a viable alternate route, alongside WLAN and 3G etc., into such a core network.

IV. MESH NETWORK STANDARDIZATION

Several standardization bodies are actively working to define specifications for wireless mesh networking, targeting different types of networks. Dedicated IEEE Task Groups (TGs) have been established defining the requirements for mesh networking in Wireless Personal Area Networks (WPAN), WLANs, Wireless Metropolitan Area Networks (WMANs) and Mobile Broadband Wireless Access (MBWA) [16]. The IEEE 802.15.5 TG was formed to determine the necessary mechanisms enabling mesh networking in WPANs PHY and MAC layers. The challenge is in providing lightweight implementations for mesh networking techniques considering the limited resources in the digital devices.

Facing the throughput degradation and unfairness in IEEE 802.11 multihop networks, the IEEE 802.11s TG addresses the needs for wireless mesh in WLANs and aims to extend 802.11 architectures and protocols to provide ESS (Extended Service Set) mesh functionalities. The implementation of this specification shall be directly reflected over the existing PHY layer of IEEE 802.11a/b/g/n operating in the unlicensed spectrum of 2.4 and 5 GHz.

On the other hand, IEEE 802.16 standard targets WMANs and comprises some TGs related to mesh networking. The WiMAX forum is working to ensure the

interoperability of manufactured equipments using these standard suites. IEEE 802.16a TG introduces the mesh mode enabling multihop communication, operating in the licensed and unlicensed lower frequencies of 2-11 GHz and covering up to 50 km. 802.16a limitation concerns its target on the fixed broadband applications. Consequently, 802.16j TG was created for Mobile Multihop Relay (MMR) to study the possibility of supporting mobile stations through using multihop relaying techniques. In addition, IEEE 802.16e TG is developing an amendment to 802.16a to support subscriber stations moving at vehicular speeds. Its target is to conceive a system for combined fixed and mobile broadband wireless access, operating in the 2-6 GHz licensed bands. Simultaneously, IEEE 802.20 WG intends to provide ubiquitous Mobile Broadband Wireless Access (MBWA) in a cellular architecture that supports the mesh networking paradigm. It addresses high speed mobility issues with speeds up to 250 km/h making it suitable for train networks, operating in licensed bands below 3.5 GHz.

Furthermore, the ZigBee Alliance has been working on the specifications of Low Rate WPANs (LR-WPANs) based on 802.15.4. The IETF Control and Provisioning of Wireless Access Points (CAPWAP) WG emerged with the objective to address architectures and operations of managing large scale WLANs deployments. Mesh networking is one of the architecture examples defined by this WG and is classified as distributed WLAN architectures. The CAPWAP efforts consider the 802.11 WLAN technologies, with a liaison with the IEEE 802.11s TG. This WG is looking for extensibility for future applicability to other access technologies especially the 802.16. Finally, Software Defined Radio (SDR) benefits from today's high processing power to develop multi-band, multi-standard base stations and terminals [17]. SDR is promising to operator in increasing network capacity and simplifying reconfiguration, and aids manufacturers in providing multi-standard multi-band equipments, with reduced deployments efforts and costs. As current standards target different mesh networks environments, network operators can benefit from several standards to provide scalable and progressive WMNs deployments. Operators are expected to provide an umbrella coverage integrating several standards with a real-time trade-off to offer the users the best possible service.

V. CHALLENGES FOR WMNs

As shown above, while WMNs have strong and attractive features of mesh networks make them worthy of consideration, a plethora of issues, challenges and options need to be addressed in order to enable the network operator to offer innovative services. Here we present some of these challenges.

A. Performance Issues

The performance of any network is a critical factor that needs to be considered before it gets accepted and deployed at large scale for various commercial applications. In the context of WMNs, the issues which affect their performance include the following:

- *Distributed MAC & Multihop Communication:* Because of the 'decentralized' nature of mesh networks, the MAC function should be accomplished in a distributed manner i.e. to establish multi-point to multi-point links between the mesh nodes in the absence of centralized controller. Moreover, the MAC protocol for WMNs needs to have multihop communications at the core of its design. The aforementioned requirements make the design of the MAC functions highly challenging. Several distributed channel assignment and MAC protocols have been proposed [18] [19] which improve the throughput in multi-hop paths. However they are still far from being optimum solutions to be exploited by the network operator for commercial deployments. Apart from these, one needs to properly identify the issues related to the spectral efficiency of both high frequency and low frequency mesh systems. Proper characterization for the mesh capacity constraints is very important in determining the practical utility of mesh networks and its enabling technologies.
- *Mesh Routing:* Mesh networking requires each node to share route information with other nodes. This functionality should be assured by the mesh routing

protocol. Some efforts have been initiated to adapt the ad-hoc routing protocols for WMNs. However ad-hoc routing protocols lack various important performance factors such as scalability, fault tolerance, QoS metrics (fairness), load balancing, and lack of cross layer interaction. In addition, certain areas such as mobility and power management have totally different requirements in ad-hoc networks and WMNs. This makes ad-hoc routing solutions not particularly suitable for WMNs.

- *Application and Service Perspective:* Every application and service has its own inherent characteristics which makes it perform well on one platform and not on another. Due to the distributed multihop features of mesh networks and the non significant support from the lower layers to assure certain quality of service support for the application layer, there is a pressing need to adapt the existing applications to WMN architecture.
- *Interoperability and Integration:* Due to the emergence and rapid growth of heteregenous wireless access technologies such as WiFi, WiMAX, UWB, various cellular systems etc., interoperability and integration are a major concern for future wireless systems. While WMNs can probably serve as a unifying technology for all these disparate systems, more research still needs to be performed to ensure that seamless service can be offered to users irrespective of access technology.

B. Scalability

Scalability, and consequently, reliability and robustness are important and inter-related issues to be addressed in order to enable the operation of the numerous embedded applications envisaged for WMN systems. At first, it would appear that these characteristics are inherently unachievable due to the self-adjusting and non-hierarchical nature of WMNs. However, they are essential in any commercial network. Scalability problems become even more severe as the WMN's coverage grows. As shown in [20], the bandwidth available for each node to originate packets decreases as the expected path length increases i.e., when the scale of the network increases, the end-to-end

reliability and available bandwidth sharply drops, thereby diminishing the network performance. When the issue of network latency is added to this, the equation becomes even more complicated and the guarantees of Quality-of-Service for the clients are disturbed.

Designing a scalable mesh network requires the proper understanding of the complex inter-relationship between the contrasting network characteristics. This is especially true for applications that need to handle continuous data streams where high capacity is critical to maintain the scalability and reliability of the network. Careful design and proper characterization of the physical layer mechanisms depending on the envisaged application scenarios and an inherent foresight on the number of users, designing efficient and distributed backbone communication topologies [21] using hybrid multiple access schemes exploiting the availability of multi-radio, multi-channel systems, devising efficient routing protocols for transporting data robustly etc. can solve the existing scalability problems in WMNs.

C. Security

Security is a critical step to deploy and manage WMNs. Two classes of attacks are likely to occur in WMNs:

i) External attacks, in which attackers not belonging to the network jam the communication or inject erroneous information.

ii) Internal attacks, in which attackers are internal compromised nodes that are difficult to be detected.

Both types of attacks may be either passive intending to steal information and to eavesdrop on the communication within the network, or active modifying and injecting packets to the network. Some of the prevailing issues are as follows:

- *Different Layers Attacks and Misbehaviours in WMNs:* Attacks can exist at different layers in WMNs causing the networks' failure. At the physical layer, an attacker may jam the transmissions of wireless antennas or simply destroy the hardware

of a certain node. At the MAC layer, an attacker may abuse the fairness of medium access by sending MAC control and data packets or impersonate a legal node. Attacks may occur in routing protocols such as advertising wrong routing updates. At the application layer, an attacker could inject false fake information, thus undermining the integrity of the application. Attackers may also sneak into the network by misusing the cryptographic primitives. Consequently, the exchange of cryptographic information should take place in a manner that utilizes equal participation, ensuring that a misbehaving party can not gain anything from misbehaviour.

- *Denial-of-service (DoS) events:* Selfishness and greediness are two misbehaviours that are likely to take place in WMNs. Nodes may behave selfishly by not forwarding packets for others in order to save power, bandwidth or just because of security and privacy concerns. There have been approaches developed to detect selfishness and enforce distributed cooperation and are suitable for WMNs [22]. Some monitor neighbours to detect misbehaving nodes while others, in addition, incorporate penalties to provide an incentive for cooperation thereby keeping greedy behaviour to a minimum [23]. The DOMINO mechanism [24] solves the greedy sender problem in 802.11 WLANS with a possible extension to multihop wireless networks. It should be noted that external DoS events where the radio signal itself gets jammed can also be considered as attacks. However, they do not necessarily lead to a breach in security.

- *Authentication, Authorization and Accounting:* Authentication and authorization are important counter-attack measures in WMNs, allowing only authorized users to get connections via the mesh network and preventing adversaries to sneak into the network disrupting the normal operation. Authentication, Authorization and Accounting (AAA) are provided in most of the WLANs applications and commercial services through a centralized server such as RADIUS. However, a "pure" centralized scheme is not appropriate in WMNs and secure key management is much more difficult. Thus, distributed authentication and

authorization schemes with secure key management are important in WMNs. To allow users' mobility with seamless and secure access to the offered services in the mesh network, authentication should be performed during mobile nodes' roaming across different WMRs and across different domains. The IEEE 802.11i standard proposes a key caching option to mitigate the overhead of re-authentication [25]. However it is vulnerable to impersonation attacks, in which a malicious access point uses previously cached authentication keys to dupe user nodes. Other vendors' specific solutions are proposed by Cisco, Aruba and Trapeze networks, integrating a switched architecture in the 802.11i authentication aiming to centralize the storage of authentication keys, therefore to accelerate the re-authentication. These solutions work well in WLANs applications, resolving the expensive overhead of re-authentication. However, there are no associated security mechanisms to prevent attacks on stored keys, and these solutions are not scalable to WMNs. Finally, the Wireless Dual Authentication Protocol (WDAP) [22] provides dual authentication for wireless station and its corresponding AP/router in a wireless network via an authentication server. WDAP includes authentication, de-authentication and roaming authentication protocols and can be applied in WMNs considering wireless stations as user nodes with access points playing the role of mesh nodes.

To further ensure security of WMNs, protocol integration is critical. Security mechanisms need to be embedded into MAC protocols to detect and prevent misbehaviour in channel access, and into network protocols providing a secure routing. As in wired networks, multi-layer security is desired as attacks occur simultaneously in different protocol layers. A cross-layer framework for security to detect and respond to attacks is necessary. It is also necessary to provide sufficient capabilities for mutual authentication among nodes. However, such schemes must generate as little overhead as possible due to the nature of the medium and node constraints such as limited power, processing capabilities or memory space. Also, unacceptable authentication delay might impact service continuity.

D. Accounting and Billing

WMNs need special accounting mechanisms and tailored billing systems with appropriate business models considering the benefits of both mobile users and service providers. To assure service availability and continuity, inter-domain accounting is important in WMNs. High packet loss ratio and security requirements should be carefully handled in this case, where authentication, replay protection and data integrity are indispensable. The economic interests require the application of usage sensitive billing systems based on the gathered accounting information for each client.

VI. FUTURE OF WMNs

Wireless mesh networks have emerged as a promising new technology, where several vendors are offering services for their deployment. Cost of deployment of the network will be the main driving factor for the success of WMNs.

Security is a strong challenge influencing the commercial deployments of WMNs, however there is still a strong need for efficient solutions adapted for different security requirements and for different usage scenarios. These solutions have to counter attack in all protocol layers, guaranteeing collaborative behaviours between mobile nodes. Trust relationships should exist among stakeholders for authentication, authorization, accounting and billing of end users. Well performing tools need to be developed for mesh design, maintenance, monitoring and management; such that the future's mesh networks should be self managed rather than unmanaged ones.

In Chapter 3, we propose an architectural framework that helps address the challenges in deploying WMNs for network operators. This includes solutions for provisioning, security and billing issues. We address the problem of provisioning by presenting a novel scheme where network credentials are de-coupled from the network hardware (similar to GSM cellular technology) such that network providers can operate a 'hybrid'

architecture where credentials are centrally provisioned but deployed in the network in a distributed fashion. We also address the issue of billing and inter-domain operability for 'roaming' users.

In this thesis, we leverage the properties of WMN to help ensure scalability of the framework while maintaining reliability. We show, through protocol analysis, that this framework can help solve some of the major challenges currently faced in the WMN commercial space.

Chapter 3

A FRAMEWORK FOR SELF-CONFIGURATION

As mentioned in the preceding chapters, a key challenge to the widespread adoption of WMNs is economics. The pervasiveness of wireline technologies in many environments is so deep that for WMNs to achieve penetration, they have to be quicker and cheaper to deploy than the competition. Since the cost of hardware for most technology is negligible over the lifespan of its use, this key economic incentive in WMNs has to be achieved in the areas of deployment and operation. To achieve this, WMNs have to be self-configuring. The best way to achieve this is via a consolidated framework enabled by cross-layer design. In such a framework, features and information gathered in a particular layer or protocol phase gets utilized at the higher layers or stages.

We seek to address this challenge by proposing a solution to the self-configuration of WMNs. This framework outlines a feasible architecture for wireless mesh networks utilizing a practical view on the usage scenarios. We also explore critical factors influencing the performance and scalability of these networks, security issues (to ensure only authorized users are granted network access), as well as billing/accounting that is beneficial for clients as well as providers. The framework has been termed ACORN (**A**utomatic **C**onfiguration **O**f **R**adio-based **N**etworks).

I. OVERVIEW OF WMN OPERATION

A wireless mesh network (WMN) is a communications network made up of radio nodes organized in a mesh topology. The coverage area of the radio nodes working as a single network is sometimes called a mesh cloud. Access to this mesh cloud is dependent on the radio nodes working in harmony with each other to create a radio network. Typically, a mesh network is reliable and offers redundancy since links are typically "any-to-any". When one node can no longer operate, the rest of the nodes can still communicate with each other, directly or through one or more intermediate nodes. Wireless mesh networks are technology-agnostic i.e. they can be implemented with various wireless technology including 802.11, 802.16, cellular technologies or

combinations of more than one type. This characteristic is a very important feature of WMNs as some access technologies are better suited to certain parts of the network than others.

A wireless mesh network can be seen as a special type of wireless ad hoc network. It is often assumed that all nodes in a wireless mesh network are static and do not experience mobility. This is not always the case. The mesh routers themselves may be static or have limited mobility. Often the mesh routers are not limited in terms of resources compared to other nodes in the network and thus can be exploited to perform more resource intensive functions. In this way, the wireless mesh network differs from an ad hoc network since all of these nodes are often constrained by resources. In addition, the mesh routers are more likely to have un-interrupted power source (AC power). Wireless mesh networks have a relatively stable topology except for the occasional failure of nodes or addition of new nodes. The traffic, being aggregated from a large number of end users, changes infrequently. Practically all the traffic in an infrastructure mesh network is either forwarded to or from a gateway, while in ad hoc networks or client mesh networks the traffic flows between arbitrary pairs of nodes.

WMN infrastructure can be decentralized (with no central server) or centrally managed (with a central server). While there are advantages to the network being centrally managed, certain features (routing, link management etc.) have to operate in a decentralized manner for the network to function properly. Nodes act as routers to transmit data from nearby nodes to peers that are too far away to reach in a single hop, resulting in a network that can span larger distances. WMNs work in a similar fashion to the wired Internet. Data will hop from one device to another until it reaches its destination. Dynamic routing algorithms implemented in each device allow this to happen. To implement such dynamic routing protocols, each device needs to communicate routing information to other devices in the network. The routing algorithm used should attempt to always ensure that the data takes the most appropriate route to its destination. Different metrics can be utilized to make this decision

II. ASSUMPTIONS

Based on the information above, some key assumptions were made while developing this framework.

1. Internet access occurs only via the mesh infrastructure nodes. These nodes are largely stationary or move very infrequently.

2. The subscription module (token or smartcard) used in the WMN devices is tamper-resistant. Any attempts to modify its contents results in a network notification and invalidation of the token. This Token contains the subscriber's ID, ESSID, assigned wireless channels (where applicable e.g. in a regulated environment), and PKI private key.

3. IP address assignment is adaptable based on the network the node is allowed to join. This differs from most other projects that concentrate on configuration and not deployment i.e. it is implicitly assumed that there are no competing networks. This is also critical to our objective to allow commodity hardware to be used for different networks. The key difference between nodes belonging to different networks would be subscription-based credentials stored on a module or some form of smart card.

4. It is designed to be routing-protocol agnostic. There is no need to design a routing protocol specifically for the network. Any routing protocol (proactive or reactive) should be able to work within the mesh. The discovery, boot-strapping and registration process all serve to aid Layer 3 reachability i.e. the topology built during network discovery should be useful to any routing protocol.

5. The nodes used in the WMN are multi-channel, multi-radio nodes; Data and control packets can be sent out via either interface. Channels are bound to links and not nodes (edges, not vertices). Channel assignment seeks to assign more non-overlapping channels to connections closer to the root. The number of channels assigned by node is limited to the number of radios present. Channel re-use should be utilized wherever possible. The following assumptions are made:

   - There is a control radio for management
   - The channel assignment is provided for self-configuration
   - The network has a known good connection state that can be used for fallback

6. The composite metric used to determine the network's topology is unique. It is calculated in a distributed fashion, adaptive and is weighted to give preference to link reliability (interference, Signal-to-Noise ratio), channel capacity (bandwidth) and queue occupancy which helps ensure intrinsic topology fairness. Queue occupancy should a weighted average calculated over a sample period.

7. Self-healing should not trigger a re-configuration of the topology tree. It should use alternate links discovered during the discovery, bootstrapping and registration process. This will ensure long-term stability of the network's topology. This is done over the common signalling channel. To prevent long-term unfairness, in the event of a failure, a node should try to discover another parent node after a certain period of time. It should do this by scanning for beacons promiscuously. In the event that a node has only one link (i.e. no standby connections), it should automatically start the membership and initialization phase again.

8. When the tree needs to be recalculated due to a long-term change in physical connectivity, it should be done as locally as possible i.e. it should occur in the

"leaves" of the tree first (children nodes) before spreading to the branches (delegated parent nodes) and maybe the root (parent nodes). This takes advantage of the fact that nodes closer to the root (the 'branches') are more stable than edge nodes (the 'leaves'). This is due to the fact that those nodes are likely to be installed by the provider which means that their connectivity is better constructed with a less likely chance of failure.

9. The algorithm is both distributed and centralized. The discovery, boot-strapping and registration process are distributed while the centralized portion consists of agents running on the nodes reporting to a centralized manager with status on various network variables as well as configuration of parameters such as IP addressing and QoS settings.

10. It is assumed that not all nodes are cooperative. While we believe our scheme can work for community-based WMNs, it is developed using a service provider-oriented concept where identity of the subscriber is essential to the delivery of service.

III. NODE INITIALIZATION

A. Problem Description

When a node initially powers up, it needs to perform certain operations to properly join itself to the network. The stage is known as node initialization. A node that is attempting to rejoin the network also has to go through these steps to ensure it rejoins the WMN in a non-disruptive and seamless manner.

Typical operations that occur during this phase include basic node verification and channel assignment.

B. Related Work

Channel assignment is essentially a link layer (MAC) operation, a great deal of attention has been centered on the development of efficient MAC layer algorithms to minimize link contention and ensure relatively rapid establishment of links.
Because of this, channel assignment is one of the most heavily explored research areas of WMNs. Wireless is an intrinsically unreliable medium so it is of utmost importance that nodes in the network have some semblance of link organization if there is to be meaningful communication and cooperation among them.

There have been many works tackling the problem of channel assignment in wireless networks.

The design of MAC layer algorithms in WMNs pose challenges not necessarily experienced in other wireless technologies:

- MAC for WMNs is concerned with more than one hop communication. Classical MAC protocols are limited to one-hop communication while the routing protocol takes care of multihop communication. While this approach makes protocol design easier, it does not work well in WMNs, because data transmission and reception at a node is not only affected by nodes within one hop but within two or more hops away. The hidden node issue in a multi-hop wireless LAN is such an example [26].

- MAC is distributed and cooperative and works for multipoint-to-multipoint communication. Even in situations where the network has centralized control, multihop communication can cause local traffic

patterns to be vastly different from one part of the network to another. The MAC protocol must ensure all nodes to cooperate in transmission.

- The MAC protocol should have the knowledge about network topology which can help better cooperation among nodes in the network. This can significantly improve the MAC performance in a multi-hop environment.

There are two general approaches that have been used for the development of MAC layer protocols in WMNs:

Single-channel MAC: The single-channel MAC is the most pervasively deployed link layer scheme for wireless networks. 802.11 WLANs are based on the CSMA/CA protocol (Carrier Sense Multiple Access With Collision Avoidance). Protocols such as those found in [27,28] are enhancements of the CSMA/CA protocol. Schemes in this category typically adjust parameters of CSMA/CA such as contention window size and modify backoff procedures. Even though they may improve throughput for one-hop communications, their performance suffers in WMNs as they usually yield a low end-to-end throughput, because they cannot significantly reduce the probability of contentions among neighboring nodes. The benefits of any scheme using this approach are likely to diminish in environments where links have frequent contention and packet collision.

Cross-layer design leveraging physical layer techniques: Two major schemes exist in this category: MAC based on directional antenna [29,30] and MAC with power control [31]. The first scheme relies heavily on advanced antenna technology to ensure that communication between nodes is as focused as possible to reduce interference. However, its practical use is questionable as it is highly unlikely that the antenna's beam will be perfect 100% of the time. Cost and complexity or hardware is also an issue. The second set of schemes utilizes

power control to reduce interference [32,33]. This can help reduce exposed nodes problem, especially in a dense network, thereby improving spatial reuse in the network. However, hidden nodes still exist and may become worse because lower transmission power level reduces the possibility of detecting a potential interfering node [34].

Multi-channel MAC: A multi-channel MAC can be implemented on several different hardware platforms, which also impacts the design of the MAC. The design can be based on a single transceiver or multiple transceivers.

With a single transceiver, only one channel can be active at a time. Multiple nodes may operate on different channels to help boost network capacity. To coordinate transmissions between network nodes under this situation, protocols such as the multi-channel MAC in [35] and the seed-slotted channel hopping (SSCH) scheme [36] are needed.

With multiple transceivers, a radio includes multiple parallel RF front-end chips and baseband processing modules to support several channels operating simultaneously. On top of the physical layer, there is only one MAC layer to coordinate the functions of multiple channels. An example of this is the Engim multi-channel wireless LAN switching engine [37]. However, as far as we know, designing an efficient MAC protocol for this type of physical layer platform is still an open research topic.

Multi-radio MAC: In this scenario, a network node has multiple radios each with its own MAC and physical layers. Communications in these radios are totally independent. Thus, a virtual MAC protocol such as the multi-radio unification protocol (MUP) [38] or Microsoft's Mesh Connectivity Layer [39] is required on top of MAC to coordinate communications in all radio links and

channels. Although, one radio can have multiple channels, a single channel is used in each radio for simplicity of design and application.

While this approach is probably best suited for WMNs due to its simplicity and scalability potential, it could suffer from the same issues as single channel MAC solution i.e. a multi-radio MAC implementation can approached as a single channel MAC scheme for two radios in the same node.

It is clear from the above that most of the underlying issues with MAC design and channel assignment in WMNs are a direct result of the shortcomings of the CSMA/CA protocol. TDMA is probably better suited for channel access in WMNs. While TDMA has its shortcomings (interference between time slots on the same frequency, bandwidth limitations due to dead time), its characteristic of allowing multiple transmitters to re-use the same frequency channel can be the missing ingredient in the scalability of WMNs especially in unlicensed frequency bands. A variant of TDMA, dynamic TDMA, is used in the IEEE 802.16a protocol. This utilizes a scheduling algorithm to dynamically reserve a variable number of time slots in each frame to variable bit-rate data streams, based on the traffic demand of each data stream. This helps make more bandwidth available in the system as needed thereby mitigating one of the shortcomings of TDMA.

Our opinion is that a hybrid approach to the MAC design problem may actually work best for WMNs. For example, combining TDMA with a scheduling algorithm such as that proposed in [40] can ensure better utilization of the timeslots thereby increasing bandwidth in the network. This can then be used with a channel graphing algorithm that helps determine local regions of traffic in the network and minimize interference between timeslots on the same frequency i.e. different channels will be used in different regions of the network. In some circumstances, power control can also be used to optimize network topology [41], minimize the interference between neighboring nodes, thereby improving the network's capacity.

C. Solution

It is assumed that the core network has achieved a stable connectivity state. This is a fair assumption as all wireless mesh gateways (WMGs) are installed by the provider and are not likely to be moved. The node initialization stage is for wireless mesh routers (WMRs) that are joining the network. WMRs can either be installed by the provider or a subscriber.

The WMR performs a hardware check to ensure that all its hardware is functioning properly. It then starts sending out maintenance beacons (broadcast) every second at the base power level. Transmitting at the base power level helps ensure that the broadcasts do not impact the network unnecessarily. They also help assure that any nodes that receive it are definitely within good transmission range of the WMR. These beacons contain the following information:

- Enterprise Service Set ID (ESSID)
- Wireless Channels (WCH). This indicates what channels have been assigned to the network. It is set to zero (or unused) in a non-regulated environment.
- Cipher of ESSID and Subscriber/Node ID encrypted with the Service Provider's Private key.
- Node Status (NSTAT) – Bridge (B), Gateway (G), Subscriber (S), Access (A), None (Unused)
- One-way hash of Node Status (Bridge, Gateway, Subscriber, Access, None) and Subscriber/Node ID. WMGs have Node IDs (NID) instead of SID

All this information is pre-computed and encoded into the tamper-resistant token by the Service Provider upon subscription. Also included in the token is the Service Provider's PKI certificate)

These beacons are forwarded all over the network till they arrive at a WMG which forwards them to the core provider network. The core provider network contains the services that the network provides (authentication, authorization, accounting, billing, certificate services etc.)

Every WMR/WMG that receives this beacon sends a beacon back to the originating node (unicast). The node trying to initialize keeps track of the beacons it receives. If it receives a beacon from another node three times in succession (within a specified time period), it stores the transmitting node in its neighbourhood table. If it receives a beacon from a WMG (as indicated by the node status) and verifies it by decrypting the cipher of the ESSID and NID, it stores it immediately.

In the event that the node receives multiple beacons that satisfy the requirements above e.g. when there is dense connectivity, the WMR does the following to select the nodes to put in its neighbourhood table:

- The three nodes with the highest RSSI are put in the neighbourhood table. These three nodes could be WMGs (which indicates that the node is closer to the 'top' of the network) or WMRs (which indicates that the node is closer to the 'bottom' of the network) or a mixture of both. WMGs are always preferred over WMRs.
- Other nodes with RSSIs above a certain threshold are put in an alternate neighbourhood table. If two nodes have the same RSSI, the node with the newer SID or NID is put in the neighbourhood table while the other is put in the alternate neighbourhood table. In the unlikely event that two nodes have the same SID or NID, the node selects whichever beacon was received first.

The alternate neighbour table serves two main purposes:

1. It is used for rapid rebuilding of a node's neighbourhood in case one of its preferred neighbours fails.
2. It can help alleviate contention for resources. This can help achieve load sharing in the network by diverting traffic away from overloaded nodes.

At the end of this stage, the WMR should have its neighbourhood list complete.

D. Protocol Flow Diagram

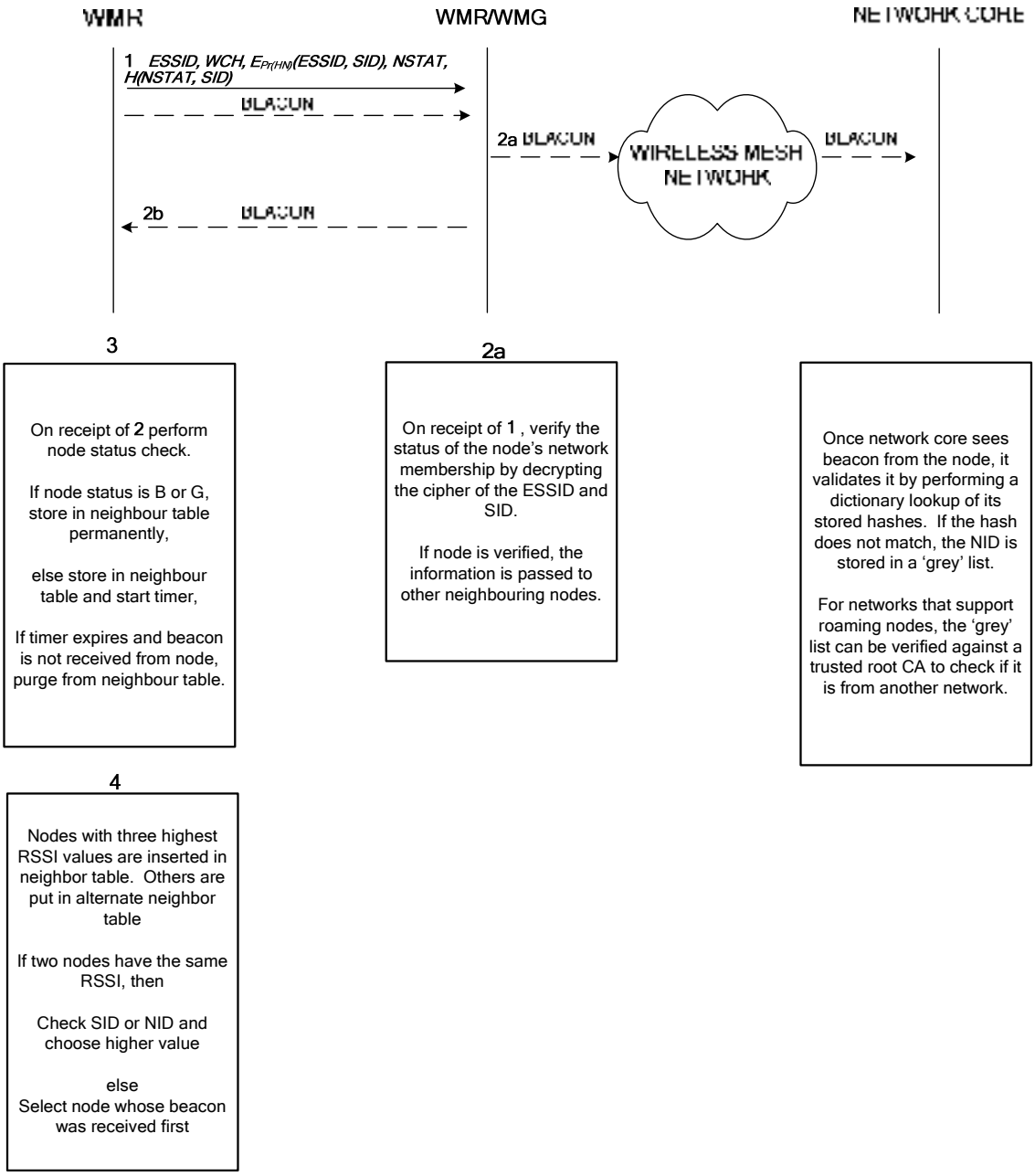

Figure 3 Node Initialization

IV. NODE BOOTSTRAPPING

A. Problem Description

After the node initializes, it has to properly join the network topology. This is especially important in wireless networks as the ability to sense a node does not necessarily mean it is best to communicate using that node. This stage is known as node bootstrapping. The node uses the information gained from the initialization stage (neighborhood list, RF properties etc.) for this stage. This ensures that the phase can be completed as quickly as possible.

B. Solution

As nodes receive and send beacons, the node gathers information about the topology network. The node is able to establish its neighbourhood and determine which nodes it can 'hear' clearly. This achieves two objectives:

a. If all checks pass, it means the node is a valid member of the network and can be reasonably determined to be under the control of a valid subscriber. If this is a guest node from a foreign network, the node still gets connected from a topology perspective but is not allowed to utilize any network services until the Network registration stage (described below) is complete. Also, no local nodes will be able to pass any application traffic until after the Network registration phase.

b. The node can use the received signal strength (RSS) of the beacons to determine which neighbours it is strongly connected to. This helps it utilize the

best connections possible. The node can also use this information to help alleviate the "hidden terminal" problem.

The hidden terminal problem has been well chronicled in the literature and many solutions have been proposed [42]. In our scheme, the hidden terminal problem is addressed in the bootstrapping stage using an iterative Power Control algorithm. When a node bootstraps, it gradually increases its signal power in staggered steps from the base transmit level to see how many nodes is able to sense it. This is done using a random time generator (RNG) to prevent synchronization with other nodes. A special topology beacon is used for this purpose. The beacon contains the ESSID and a hash of the ESSID and SID. Due to the staggering provided by the RNG and the very unlikely event that two nodes come up exactly at the same time, the traffic in the network can be kept to a tolerable level (no broadcast storm) with the devices transmitting in a poll-like manner (which helps ensure accurate reception of topology beacons). Since WMNs are mostly static by nature, the process will be able to determine, with a high degree of accuracy what links and nodes can be interfered with by one node's transmissions.

This step is only done during boot strapping and is done on a node-by-node basis. By doing this, the node can determine the threshold signal level beyond which it can not reach any additional nodes. This is the power level at which it can operate and be "totally visible" in the network. When a node is able to sense another node it does not previously know, it replies to this node and adds it to its neighbour or alternate neighbour list. This scheme should help ensure that the entire network reaches "power equilibrium" - new nodes can not sabotage the network by destroying existing communication. Alternatively, the transmit power can be limited either by regulatory domain or the service provider.

The checks in the "power up" stage help ensure that the nodes involved at this stage are not malicious. Another advantage of using the power control method

is that it takes into account the fact that the radio propagation properties of various nodes in the network may be different. This way, the node can determine in a fairly accurate way what other nodes could possibly be affected by its transmissions. This leads to the formation of "collision neighbourhoods" or cliques.

Nodes that sense multiple "collision neighbourhoods" are designated "sponsor nodes" or "bridge nodes" (i.e. summary reports from multiple nodes contain different node sets). The Gateway nodes are predetermined by the service provider as they are the nodes that constitute the wireless backhaul. The closest neighbours will be determined based on received signal strength (RSS) and they will agree on a common channel based on the wireless technology used for the network. The complexity of this stage is that wireless links are not necessarily bi-directional and orthogonal channels (especially in 802.11 b/g) are scarce. The likelihood that a node will be in multiple collision neighbourhoods is high (especially in dense WMNs).

Each node sends out a summary report (broadcast) with all the nodes in its collision neighbourhood to other nodes after the bootstrapping stage is complete. Based of all the received reports, each node builds a subtree with itself as the root (combined with the RSS information from the topology beacons) with paths chosen optimally. This is a reactionary process. Only nodes who lose paths will broadcast a new summary report which may or may not trigger path calculations at other nodes.

C. Process Flow Diagram

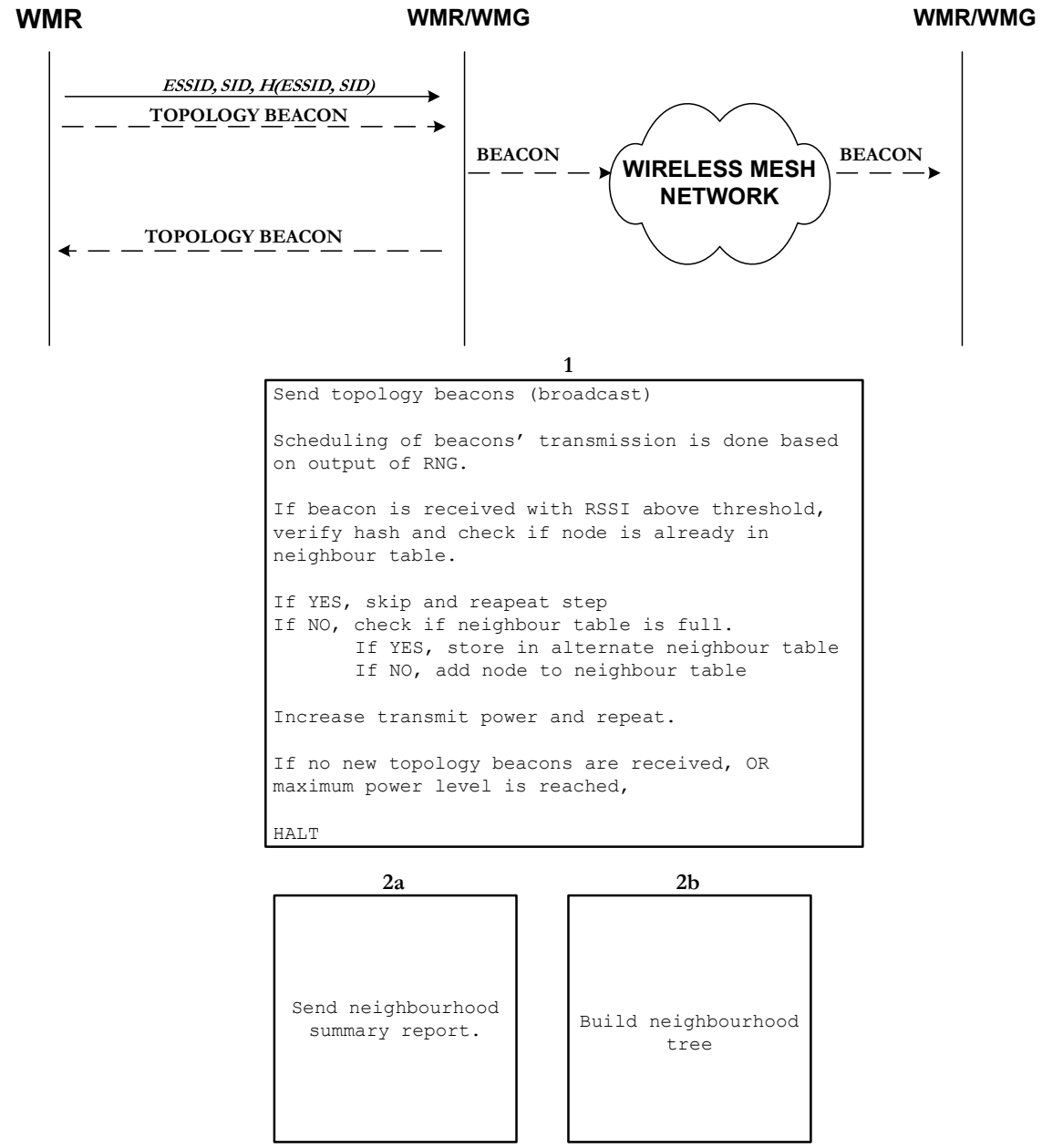

Figure 4 Node Bootstrapping

V. NETWORK OPTIMIZATION

A. Problem Description

The network optimization stage utilizes various mechanisms to ensure that the network topology built in the previous stages can be used to provide higher-layer services to subscribers. It addresses features such as routing, mobility and network hierarchy determination.

B. Related Work

The network optimization stage utilizes various mechanisms to ensure that the network topology built in the previous stages can be used to provide higher-layer services to subscribers. It addresses features such as routing, mobility and network hierarchy determination.

Just like any typical network, WMNs require a mechanism that enables the nodes to dynamically exchange information based on measured link conditions. Historically, routing protocols provide this functionality in wired networks. As expected, routing in WMNs is different from those in wired networks and cellular networks due to the differences in network architecture and node capabilities.

Historically, WMN routing has taken its cues from ad-hoc network routing. For example, mesh routers of Firetide Networks [43] are based on topology broadcast based on reverse-path forwarding (TBRPF) protocol [44] while Microsoft mesh networks are built based on dynamic source routing (DSR) [45]. Despite the availability of several routing protocols for ad hoc networks, the design of routing protocols for WMNs is still an active research area for several reasons. First of all, new performance metrics need to be discovered and utilized to improve the performance of routing protocols. Moreover, the existing routing protocols treat the underlying MAC protocol as a transparent layer. However,

the cross-layer interaction must be considered to improve the performance of the routing protocols in WMNs. More importantly, the requirements on power efficiency and mobility are much different between WMNs and ad hoc networks. In a WMN, nodes (mesh routers) in the backbone have minimal mobility and no constraint on power consumption, while mesh client nodes usually desire the support of mobility and a power efficient routing protocol.

Such differences imply that the routing protocols designed for ad hoc networks may not be appropriate for WMNs. The following features need to be present in an optimal routing protocol for WMNs:

Performance metrics: Many existing routing protocols use minimum hop-count as a performance metric to select the routing path. This has been demonstrated not to be valid in many situations. Such protocols do not capture link quality or buffer occupancy in the performance metric. To solve this problem, performance metrics related to link quality are needed. If congestion occurs, then the minimum-hop count will not be an accurate performance metric either. Usually Round trip time (RTT) is used as an additional performance metric. The solution is that a routing path must be selected by considering multiple performance metrics.

Convergence: One of the objectives to deploy WMNs is to ensure robustness in the event of link failures. If a link breaks, the routing protocol should be able to quickly select another path to avoid service disruption.

Load balancing: One of the objectives of WMNs is to share the network resources among many users. When a part of a WMN experiences congestion, new traffic flows should not be routed through that part. Performance metrics such as RTT help to achieve load balancing, but are not always effective, because RTT may be impacted by link quality.

Scalability: Setting up a routing path in a very large wireless network may take a long time, and the end-to-end delay can become large. Furthermore, even when the path is established, the node states on the path may change. Thus, the scalability of a routing protocol is critical in WMNs.

Adaptive Support of Both Mesh Routers and Clients: Considering the minimal mobility and no constraint of power consumption in mesh routers, a much simpler routing protocol can be developed for mesh routers than existing ad hoc routing protocols. However, for mesh clients, the routing protocol must have the full functions of ad hoc routing protocols. Consequently, it is necessary to design an efficient routing protocol for WMNs that can adaptively support both mesh routers and mesh clients.

Much of the recent work in multi-channel 802.11 routing has looked at jointly solving the channel assignment and routing problem. An algorithmic approach that optimizes for throughput is considered in [46], and an approach that preserves network connectivity for QoS is explored in [47]. These are centralized solutions that assume the availability of a global network view (e.g., traffic demand, nodes' status, etc.). However, a distributed approach (which we have adopted in this framework) may be more suitable to ensure scalability even when the network is centrally managed. In addition to helping the network scale, having the routing protocol accommodate arbitrary routing topologies may help the WMN function better as a whole. While this may appear to be a contradiction – after all, the WMN will probably have some semblance of a structure after network bootstrapping is complete – having the routing protocol operate this way can help ensure long-term fairness in the network's traffic patterns. If the routing protocol follows the channel assignment graph strictly, there is a distinct likelihood that certain parts of the network will be more heavily loaded than others.

Weighted Cumulative Expected Transmission Time (WCETT) [48] and Metric of Interference and Channel-switching (MIC) [49] are routing metrics that exhibit characteristics suitable for routing in WMNs.

C. Solution

As stated above, our aim is to make the framework routing protocol-agnostic. One of the reasons for this is that even in the most predictable networks (i.e. wired networks); different routing protocols offer different advantages depending on the network's topology. Just like in the wired world, we believe it is important for the service provider to have a choice of protocols to implement for their mesh network. What is most important is the cost function (combination of metrics) used by the protocol accurately represents the network's topology.

Any routing protocol, with some modification, should be able to make use of the information generated by the node initialization and bootstrapping stages to improve performance and decrease convergence time.

VI. NETWORK REGISTRATION

By utilizing the hello and topology beacons transmitted during the previous stages, all essential node parameters have been forwarded to the core network. The core network also checks the subscriber's details by decrypting the cipher of the ESSID and SID and checking it against the list of valid subscribers. Once the subscriber is confirmed to be valid, the provider network sends a PKI certificate encrypted with the subscriber's public key. This ensures only the targeted subscriber can decrypt the certificate. This certificate will contain various parameters about the network such as the subscriber's IP settings, service level (QoS), roaming privileges etc. This ensures that only valid subscribers get the necessary parameters to utilize the network's services.

The core network assigns IP addresses and other service parameters such as DNS settings to the nodes in the network. However, it does this on a delegated basis using the node's status as an indicator. Gateway and Bridge nodes are assigned distinct blocks of IP addresses and Network settings are assigned based on which bridge or gateway node is in the node's neighbourhood. By definition, a gateway node should be within one hop (i.e. directly connected) of the core network while the bridge nodes are within one hop of the gateway nodes. Subscriber nodes will have their IP addresses assigned by Gateway or Bridge nodes. Alternatively, a subscriber node can automatically generate its IP address from its upstream node's block using an RNG. For subscriber nodes that have connectivity to the network via Bridge nodes, the subscriber node will choose the assignment from the closest "bridge" node. To accommodate 'deep' networks, all nodes designated as subscriber nodes will perform address translation on their upstream interfaces for access nodes.

VII. NETWORK MAINTENANCE

Network Maintenance encompasses all of the phases mentioned above. Topology maintenance is done on a distributed basis. Nodes that lose connectivity to the network go through the node initialization and/or bootstrapping stages to re-join the network. Routing and topology changes are communicated during network optimization stage on an ongoing basis.

It is important that security is achieved during network maintenance to prevent the network from being compromised. Authentication and encryption may be jointly achieved by signing each encrypted frame with a hash of the public key and the device ID. It is assumed that the device ID is unique. To ensure the uniqueness and security of the device ID, a small (random) string of digits may be applied as an extension during registration. This could be cross-checked against the neighbour list compiled apriori on each node during registration and initialization to be sure that the Device ID/private key pair belongs to the same node. Any node that fails this test is assumed to be undergoing registration and is passed through the authentication and integrity tests. This process leads them to establish a shared symmetric key with their parents (upstream nodes) and peers before engaging in active communication.

VIII. SECURITY

ACORN relies heavily on security. As can be seen from the above, security is incorporated in every phase of the network. We believe this is important for two reasons:

- It helps prevent malicious nodes from becoming part of the network.
- It helps ensure that security can be provided in a scalable and non-intrusive fashion.

A. System Approach

Security is best done in layers and deployed in a pervasive manner in a network. From a physical perspective, security credentials for the subscriber should be stored a physical token e.g. a storage card inserted into the node could contain security credentials that identify the subscriber and not necessarily the device. This will help separate the service from the hardware. No network configuration material should be stored on the token and it should be impervious to tampering

Since credentials are separated from the wireless device, service authentication is performed for the subscriber. This helps extend the network's flexibility to provide services for subscribers from other networks. Authentication ensures that only permitted subscribers are allowed to use the network's services. Authentication is also necessary to conduct central operations such as billing, subscriber management etc. Authentication (via hash algorithms) and encryption (utilizing stream ciphers) at the link layer occurs between the nodes/devices. A node can not join the network if it is not under the control of a valid subscriber. This helps prevent against replay or MITM attacks. Only information that is publicly accessible in broadcast messages. If sensitive information has to be sent in broadcast packets, it should be limited to information that has limited use in terms of impact or should be time-sensitive to limit the exposure.

In ACORN, the subscription token is assumed to be impervious to tampering and all keying material is destroyed if the token is reverse-engineered in any way. Therefore, it is assumed that secret keys do not become available outside the device in an unsecured way. It is also assumed that a device will not be able to intentionally or inadvertently 'leak' its keying material to other devices, unless the keying material is protected, such as during key-transport.

It is assumed that the security software and hardware operates as expected. Thus, implementations of security protocols, such as key-establishment, properly execute the complete protocol. Further, random number generators operate as expected. It is also assumed that separate applications using the same radio – the so-called application endpoints – trust each other (i.e., there is no cryptographic task separation). In addition, lower layers (e.g., Network or MAC) are fully accessible by any of the application endpoints. These assumptions lead to an open trust model for a device: different layers of the communication stack and all applications running on a single device trust each other.

The aim is to cryptographically protect the interfaces between different devices only based on the users being valid subscribers of the network. The separation of the interfaces between different stack layers on the same device is addressed via proper hardware design.

The layer that initiates a message is responsible for securing it. We base security on the premise that when two devices exchange messages in a secure way, they will use the same link key, irrespective of whether this message is a MAC message, a Network message, or an application endpoint message. End-to-end security should be applied such as to ensure that only source and destination devices have access to their shared link key.

The SKKE (Symmetric-Key Key Establishment) protocol would be ideal for link layer security. The building blocks required for SKKE include the AES block cipher [50], an unkeyed hash function (e.g., the Matyas-Meyer-Oseas hash based on AES[51]), and a (pseudo) random number generator. For maximum hardware and software reuse, the random number generator (RNG) itself may employ the AES algorithm. The RNG could also be used for distributed IP address assignment.

In the SKKE (Symmetric-Key Key Establishment) protocol, a trust relationship is established using a shared, secret, and symmetric key, referred to as a master key. This master key, for example, may be derived using some cryptographic method, may be installed by a CA, may be based on user-entered data (e.g., PIN, password, or key), or may be read off the package or chassis of the wireless product (e.g., a bar code). The secrecy and authenticity of the master key needs to be upheld in order to maintain the trust foundation of the SKKE protocol. To help ensure this, we propose that the key be burnt into the token upon subscription by the user.

Successful completion of SKKE results in the following:

- Both devices share a link key;
- Each device knows that the other device has computed the correct link key;
- No device has complete control over the link key that is established; and
- No forward secrecy (Eavesdropping and compromise of the master key in the SKKE protocol exposes all the future and past communications).

If the SKKE protocol is successfully used and each device knows beforehand that only the other device possess the master key, then implicit key authentication is achieved (i.e., each device is sure that no other device has access to the established link key). If possible, the keying material should be occasionally renewed. This could be triggered by some external event such as self-healing or link re-establishment. If the SKKE protocol is used without each device knowing who has access to the master key, then implicit key authentication can still be achieved provided that no eavesdropping occurs (i.e., no passive attacks), that no messages are modified (i.e., active attacks), and that the protocol is executed in an environment where the two devices have a non-cryptographic way of establishing the identity of the other device.

In order to be able to manage and control the security of the network, special security roles can be implemented in certain devices. A device with security proxy capabilities can be used to configure a network by provisioning initial trust data to network devices. The initial trust data tells a device which devices to trust and can include device addresses, master keys, public keys, or certificates. End devices need the capability to recognize (i.e., authenticate) a security proxy before accepting initial trust data. Authentication of a security proxy can be done using cryptographic means (e.g., public key). Since a security proxy device may not always be kept physically secure, it should be impervious to revere engineering. A physical breach of the device should result in the destruction of all security related material. While the argument can be made that having security proxies can speed up the authentication process, we believe it may offer more functionality by improving the scalability of the network by helping distribute the security processing.

ACORN uses a Certificate Authority (CA) or Key Distribution Center (KDC) to provide trust in the WMN. The CA or KDC is kept physically secure (within the provider's network). So, compared with a security proxy, it should be less likely that a CA or KDC will be stolen, lost, or under physical control of an attacker. In keeping with traditional definitions, a CA distributes initial trust data for public-key based systems (e.g., private keys, public keys, root keys, and certificates) and a KDC distributes initial trust data for symmetric-key based systems (e.g., a master key burnt into the subscriber's token).

For public key cryptography, the Certificate-Based Key-Establishment (CBKE) [52] can be used. CBKE uses public-key technology with digital certificates and root keys. A digital certificate is simply a public key together with the subscriber ID, signed by the CA. Certificates can provide a mechanism for checking cryptographically to whom the public key belongs and whether the subscriber a legitimate member of a particular network. Once a certificate and root key are

securely provisioned to a device, active and passive attacks in subsequent key-establishment protocols can be thwarted.

163-bit Elliptic-Curve Cryptographic (ECC) techniques are recommended for the CBKE protocol. ECC techniques offer a reasonable computational load (especially since they will be performed infrequently in most application scenarios), and smaller key lengths for equivalent security than other techniques. Small key lengths are important to minimize the size of message storage buffers on network devices, which in turn reduces their implementation cost.

Ideally, both the symmetric-key based and the public-key based protocols should be designed such as to maximize commonalities between message flows and to allow re-use of cryptographic building blocks. This way, a single implementation of telecommunication overhead and error handling seems to be possible. Furthermore, each protocol step, including those for elliptic-curve based key establishment with certificates, could be implemented within a single frame, due to their small length of less than 100 bytes.

IX. BILLING

A. Problem Description

This is a major area of contribution for our work. As has been indicated in previous chapters, for WMNs to be truly successful in commercial deployments, the technology has to be attractive to Service Providers. Even for WMN deployments with free subscriber access, the ability to track network usage may be important. Having the knowledge of who is using the network can help improve targeted advertising and other revenue-generating activities used to operate and maintain the network.

B. Related work

A lot of this work in this area has been homogenous in nature i.e. only one type of network has been considered [53]. In [54] a solution is proposed where the billing mechanisms of GSM/GPRS networks are combined with WLAN technology. However, their work does not incorporate the ubiquitous mobile station with seamless access to both networks. The user has to stop and restart the service i.e. manually changes the network interface. Other works [55] consider billing with one access technology. Buddhikot et al [56] incorporated an accounting module into their IOTA gateway. Though implied in the paper, it is not specified how different service levels can be tracked in the billing information. Security is also an issue. There is no provision made in the protocol to prevent the network providers from colluding to cheat the subscriber. While it may argued that this has never been a major issue in the traditional PSTN, it must be noted that the stakes are higher in the next-generation networks. Not only does the volume of traffic vary depending on the application, connectivity is not necessarily circuit-based. As such, there must be a mechanism to ensure that the user is billed only for traffic originated by or destined to his station.

In their paper, Zhou and Lam [57] specify a model for secure billing in mobile networks. Their work is not limited to any particular access network. Their protocol is secure and does give a lot of insight into its feasibility in an integrated network. However, they do not address the different service levels that a network may provide and how billing data may be generated for different services.

The model presented seeks to address the need for accounting data for different types of services a network may provide. We also suggest a method for reliably and securely exchanging the data between the guest and home networks. It is generally assumed that most inter-network roaming subscribers would be from a 3G network. While this view may be the general case (it is expected that most 2G and 2.5G customers will eventually be 3G subscribers), it is quite possible that public WLANs (hotspot providers) and WMNs will also have a sizable number of subscribers. Hence, it is important that the billing solution has the right mix of scalability and portability so that a wide spectrum of network providers will be able to implement it.

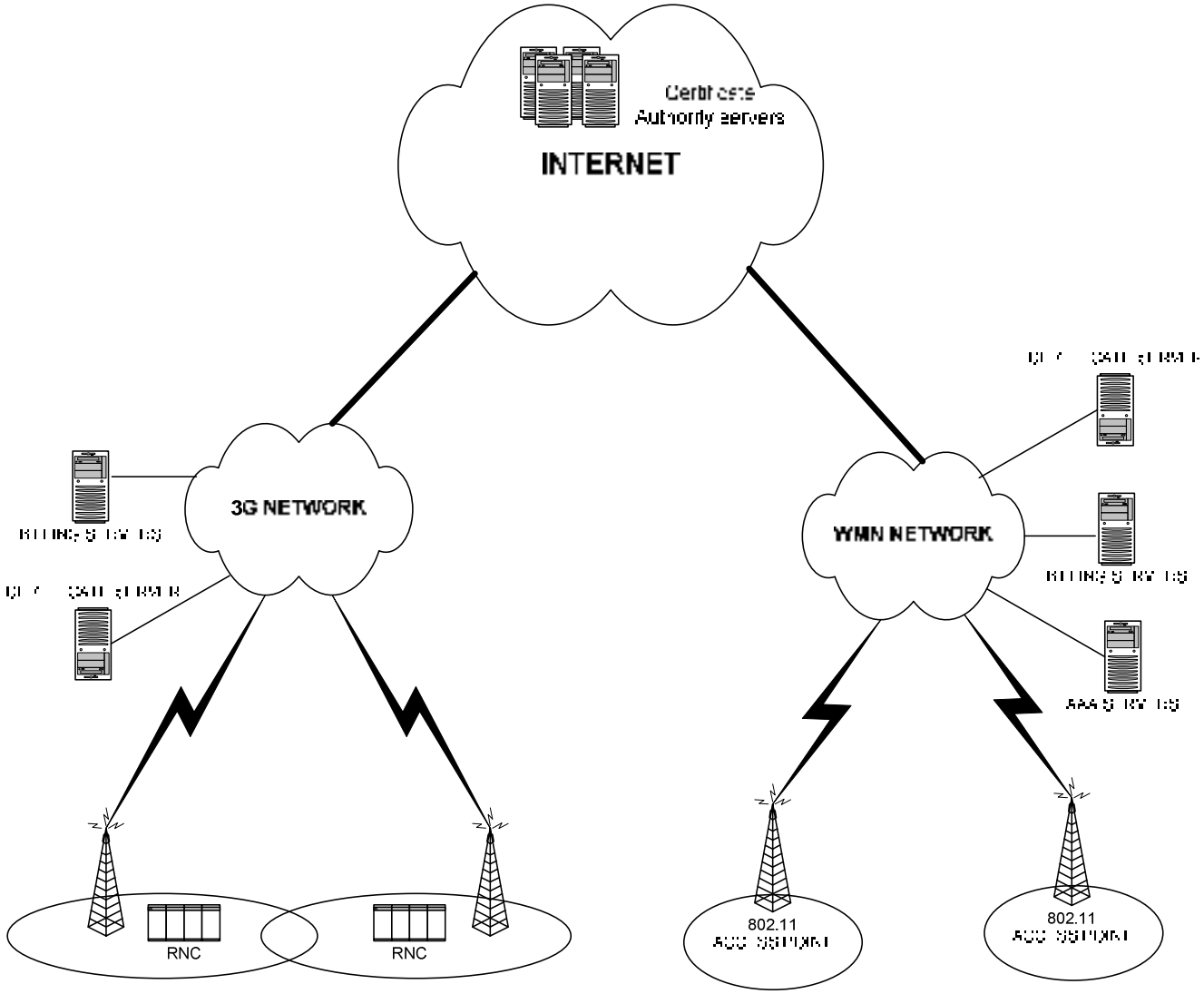

Figure 5 Block Diagram of an Integrated 3G/WMN Network

C. Solution

The following assumptions have been made.

1. Protocol conversion, encapsulation and other network-related issues (seamless hand-off, interface selection etc.) are addressed by the underlying network architecture.
2. The billing policies are decided by individual networks. Since customer billing will always be performed by the home network, it is not necessary for the guest network to process a bill.
3. The service itself may or may not be provided by the network. Video-on-demand, gaming etc. may be provided by an independent third party. The billing protocol is only for traffic transported on the network by the user. It is not responsible for ensuring that subscription status of the user of external services.
4. The user trusts its home network. The home network does not necessarily trust the foreign network.
5. The home and foreign networks trust the certificate authority.
6. The user and its home network share a common secret key. This key is stored on the user's smart card/token in a tamper-resistant manner.

The following notation is used to present elements of the scheme:

- U = a user, possibly roaming in a foreign network. When italicised, it represents an identifier. When used with a subscript, it represents the user's identity to another entity
- FN = foreign network. When italicised, it represents an identifier
- $S_{Pr()}$ = Signing using the private key of the entity in parenthesis. The key is already provided by the provider on the subscription token.
- $V_{P()}$ = Verification using the public key of the entity in parenthesis

- HN = foreign network. When italicised, it represents an identifier
- k = a secret encryption key. A subscript indicates its attachment to an entity. The key is derived using an RNG.
- $E_{Pr()}$ = Encryption using the private key of the entity in parenthesis.
- $E_{P()}$ = Encryption using the public key of the entity in parenthesis.
- S = Signing using a temporary signature. A subscript indicates its attachment to an entity
- V = Verification of a temporary signature. A subscript indicates its attachment to an entity
- $H()$ = A one-way hash of the parameters in parenthesis
- N = A nonce. A subscript indicates its attachment to an entity

It is a good security practice to use different keys for signing and encryption. This scheme adheres to this practice.

Registration

When a user U roams into a foreign network N (i.e. a network of which it is not a subscriber), the registration phase of the protocol is activated. This can be done during the network registration phase. Because the node initialization and bootstrapping stage still allow the node to join the network's topology, it can attempt to register with the foreign network.

Here are the steps in this phase:

1. U tries to locate a network to join. It broadcasts a nonce N_U, its home network identifier *HN* and $E_{P(HN)}(N_U, k_U, FN)$.
2. FN checks its certificate servers to see if it has a certificate indexed by *HN*. If it does not, it performs step 3. If it does, it goes directly to step 4. FN may have a certificate permanently stored for HN (due to a roaming agreement) or a cached one derived from previous requests from HN's subscribers.

3. FN sends an encrypted message $E_{P(CA)}(HN)$ to the certificate authority (CA). The CA checks the HN, verifies it against its list of valid certificates. If valid, the CA sends a signed, encrypted message with the certificate of the HN as its payload, $S_{Pr(CA)}[E_{P(FN)}(C(HN))]$. If not, it sends a null certificate message back to FN and FN terminates the registration attempt. The FN verifies the certificate and checks its contents. The FN should be able to get the HN's gateway location, its name and administrative information from the certificate. Other attributes may include public keys for encryption and signature verification as well as the regional certificate authority that issued and signed the certificate. This certificate can be stored by *FN* for the validity period of the certificate or a shorter, pre-determined period. This will help prevent frequent requests to the CA during intermittent or transient connections.
4. FN generates a nonce N_{FN} and sends it to HN along with $E_{P(HN)}(N_U, k_U, FN)$.
5. HN decrypts $E_{P(HN)}(N_U, k_U, FN)$ to recover (N_U, k_U, FN). From this information, it confirms the validity of the subscriber and the foreign network's identity. HN also performs the actions in step 2 (if needed). HN then sends the following to FN.

$$S_{Pr(HN)} [E_{P(FN)}(U_F , N_F, V_U, T)]$$

$$E_{kU} (N_U, U_F, S_U, T)$$

HN also generates a certificate $C_U = [U_F , N_F, V_U, T, S_{Pr(HN)} (U_F , N_F, V_U, T)]$ and sends it to FN.

6. FN sends $E_{kU} (N_U, U_F, S_U, T)$ to U along with a one-way hash $H(k_U, N_U)$ and C_U. U decrypts $E_{kU} (N_U, U_F, S_U, T)$ to retrieve its nonce and signing key. It also retrieves T which tells it how long the certificate is valid for. If T expires, U should re-register. Therefore, T should be set to be long enough to allow for uninterrupted sessions but short enough to prevent a

hijacking of the communication session. The hash algorithm should be publicly known. Along as k_U is kept secret and N_U is truly random, $H(k_U,N_U)$ should generate a unique, symmetric key for session encryption between U and FN. To ensure a balance, U should perform the hash as well to verify the key (it already knows k_U and N_U). As long as the hashing algorithm is the same and no cheating has occurred, the computations by U and FN for $H(k_U,N_U)$ would yield the same result.

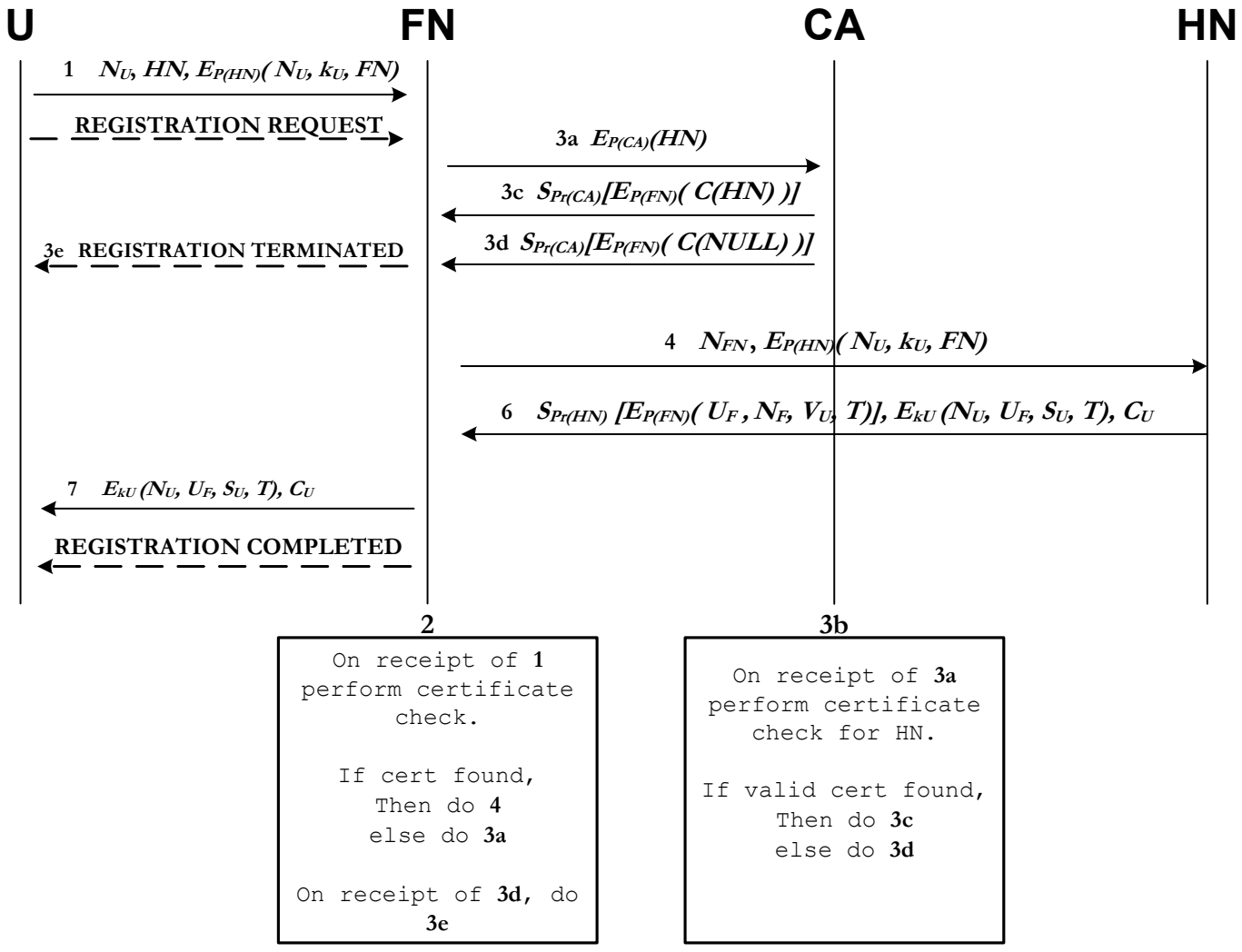

Figure 6 Registration Phase

If a node does not successfully register, the foreign network updates its 'grey' list and moves the node to its 'black' list. This list is sent to registered WMN nodes during network updates. The nodes update their neighbour tables by removing the node. The only way the node can rejoin the network at this point is to re-start the node initialization process.

Service Request

After registration at FN is complete, U may request for service. It is important to note that at this stage, U is any node that requires service (roaming or local). For the sake of clarity, we have decided to keep the nomenclature consistent and use FN as a generic term to refer to the network providing service to the node (local or roaming).

The request may be made by the application or the mobile station itself. Depending upon the application and protocol suite implemented, the actual request may be made in a variety of ways. To make the protocol as generic as possible, a specific mechanism for service guarantees and bandwidth reservation at the logical and/or MAC layers is not postulated. The main reason for this is the proposed loosely-coupled approach to integration. As such, a multimode device (i.e. 3G and WMN) will use the protocol of the connected network to negotiate a service level.

This works as follows

1. U chooses a random number n and generates a chained series of one way hashes such that

   $$H^{i}(n) = H(H^{i-1}(n)) \text{ where } i = (1,2,3,\ldots)$$

   U keeps these hash values secret. Once again, the hash algorithm is known to U and FN. The security lies in the randomness of n. These

values should be pre-computed by U to save time in future stages of the protocol.

2. U then sends U_F, $S_U(U_F, R, m, t_i, H^m(n))$ to FN. It also sends FN a value j which is a counter initialized to 1.

3. FN checks T for the certificate C_U to ensure that the signature is still valid. If this is true, V_U is then used to verify the signature. The number of hashes m, the last hashed value $H^m(n)$, and the request R are then known to FN. Additionally, U_F (the temporary identity of U) is known for billing purposes. Different service requests sent during the same registration period are differentiated using t_i (a timestamp in UTC format). For each t_i, a check should be made to ensure that it is less than the local time of the network. A different (R, t) combination will require a new billing record. R is sent to the lower level protocols to provide the requested service level. The lower level protocols send back the provided service, R'. It is possible that the network will not be able to provide the service requested so R and R' may not be the same.

4. FN sends $E_{P(HN)}(C_U, FN, R')$ to the HN

5. HN decrypts $E_{P(HN)}(C_U, FN, R')$. It checks the temporary certificate to see if it valid. If it is, it checks the roaming policy in the certificate of FN. This policy contains the pricing policy for roaming users of the foreign network. If HN agrees to the pricing policy, it sends an acknowledgement to the FN containing the following information

$$S_{Pr(HN)}[E_{P(FN)}(C_U, HN, R')], E_{kU}(C_U, HN, R')$$

HN may also check the roaming restrictions of the user to ensure that the user is allowed to use the service.

6. FN verifies the signature and decrypts the contents of the message. It sees that the HN has approved the service for the specified user. FN then sends the following to U.

$$E_{kU}(C_U, HN, R', l)$$

l is a pre-determined interval determined by the FN based on the service provided. It is used as a heartbeat during the bill collection phase to ensure that U is still using the service. l should also be specified in the roaming policy so that the HN is aware of it.

7. U decrypts the message. If *HN* is correct, it knows that the HU has certified the provided service for its current certificate. It can also verify R' meets its needs, if the application requires it. It then sends the following as an acknowledgement to FN.

$E_{H(k)}[E_{kU}(C_U, HN, R', l)]$ where $H(k) = H(k_U, N_U)$ (the session key)

8. FN decrypts the message. If it matches what was sent in 6, it starts providing service and starts billing.

A possible issue here may be the number of different exchanges and computations that are needed for provision of service. This is the most important phase of the protocol and it is essential that all parties play a role in determining what service can be provided (and is eventually provided) to U. The evidence gathered in this stage can prove useful during bill repudiation by either of the parties.

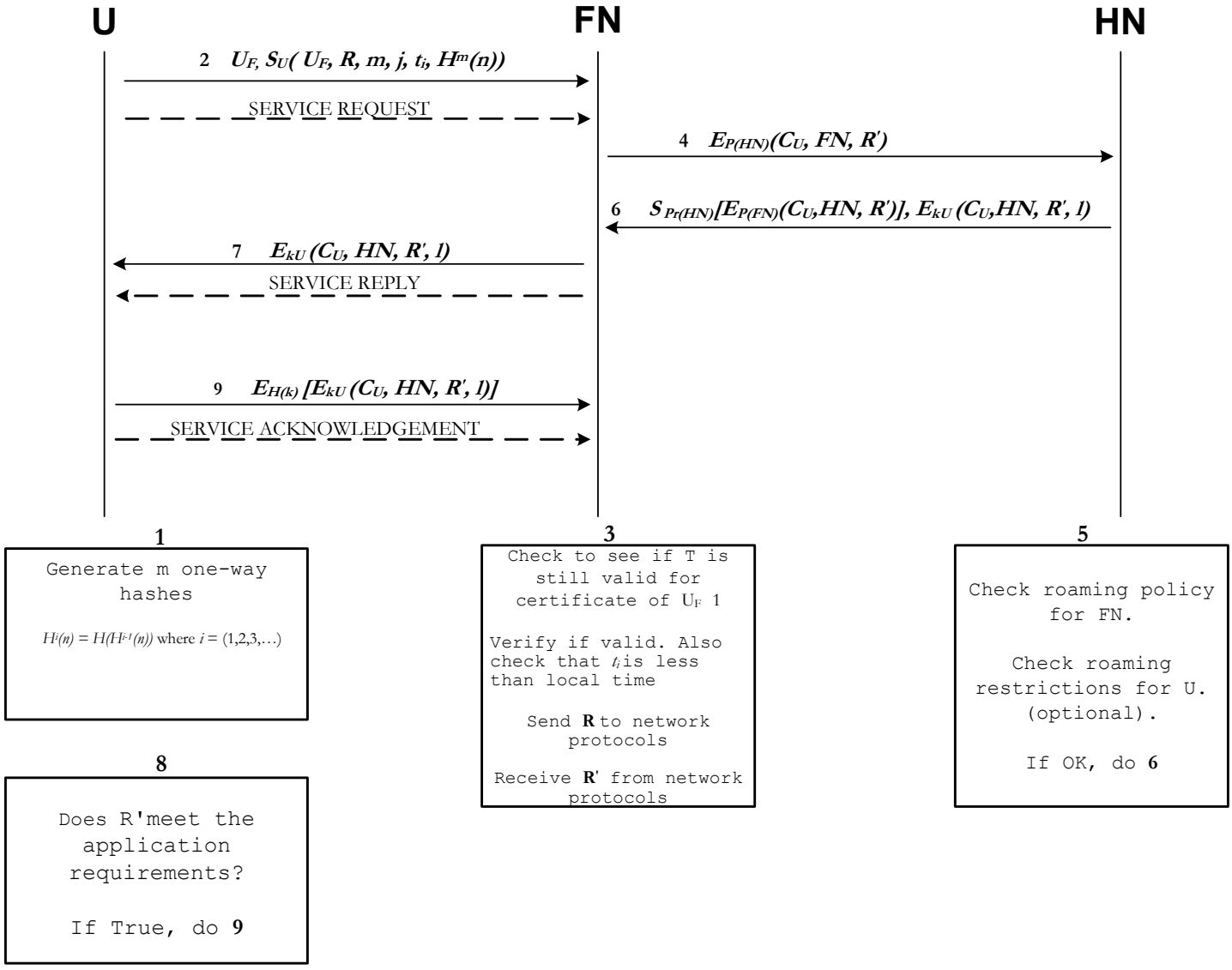

Figure 7 Service Request Phase

Collection of billing data

This phase of the protocol is based on the use of event-driven triggers. These triggers reside between the user and the billing engine in a conceptual entity called the event handler. These triggers dictate the actions of the billing engine; they tell it when to start, stop, pause or resume billing. They also pass the user attributes needed to create a billing record to the billing engine. It is important that the precision of these triggers are high for synchronization purposes. For each particular flow, the billing engine should receive only one trigger at a particular point in time.

The location of the billing engine and its triggers is very important. Since per-user flows constitute the information needed for billing, the flows have to be detected before there is any traffic aggregation in the network. The billing engine has to be able to access the air interface directly to collect to retrieve the byte count. Therefore, the billing engine has to be located as close to air interface as possible. For a WMN network, it may be placed close to the gateway nodes. In a 3G network, it may be placed close to the Radio Network Controller (RNC). Even though the billing phase is composed of many components, it should be noted that they are functional and not physical components. For instance, to obtain billing information as quickly and as accurately as possible, it may be beneficial to implement these components as part of the WMN Gateway nodes or RNC. This could be done through the use of a specialized module that can be installed in a chassis. Since these components are typically owned by the service provider and not the subscriber, non-commodity hardware can be used for this without affecting the network's flexibility. This kind of implementation may also improve scalability as more modules could be added as needed.

All communication between U and FN is encrypted using the private key agreed on during the registration phase. Apart from providing security, the FN can use this as an identification method to ensure that it updates the right billing record. The key will be different if the device re-registers. This is consistent with the

operation of the protocol since a loss of registration (i.e. loss of hash values) will cause the STOP trigger to activate. The billing engine also uses information from the network protocols to determine which service is being billed. As such, the billing is done per-user, per-service ensuring optimum granularity and ease of interpretation.

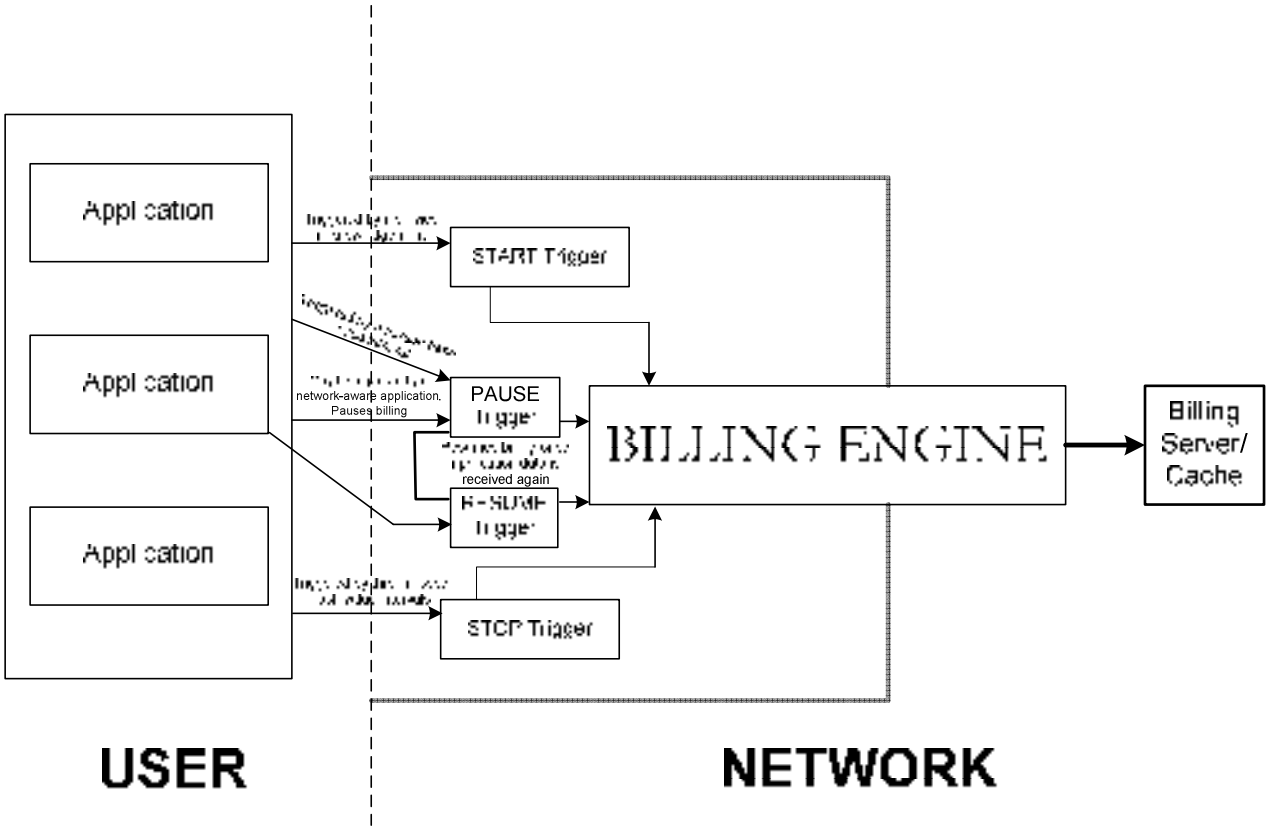

Figure 8 Billing Phase

After the user has sent a service acknowledgement to FN, the START Trigger passes the credentials to the billing engine and billing starts. It should be noted that through the other service requests and service reply exchanges, a billing record is already created in the billing database. This is done to speed up the protocol. If the service is not provided, the record should have no actual billing data. The billing engine continually monitors the network for flows for all

service requests. With each successive l, the engine writes the byte count to the billing record and increments L by 1. Since l is a static, time-based interval, it serves as a time counter as well. This practice is acceptable since duration-based billing is often done using blocks of time. It also does hash checking. It runs the hash algorithm to see if the received hash value is the one just before the stored hash value. If it is, it overwrites the stored value. This is the logic behind the chained hash. As long as the hash algorithm is one-way, the only entity that can know the previous value in the chain is the generator of the hash chain i.e. the user. Using this method, it can be guaranteed the billing record is for the right user and the user was billed for service rendered. Other decisions may also be made by the event handler as shown in the figure below.

To further enhance the security of this stage, impersonation of the user node can be subverted by ensuring that the first hash value transmitted in the chain is signed by the node using S_U (from the service request phase). This can be verified by the foreign network using V_U. Signing the first hash value in the transmission does not impose an unduly heavy computational load on the node and accomplishes an important security objective.

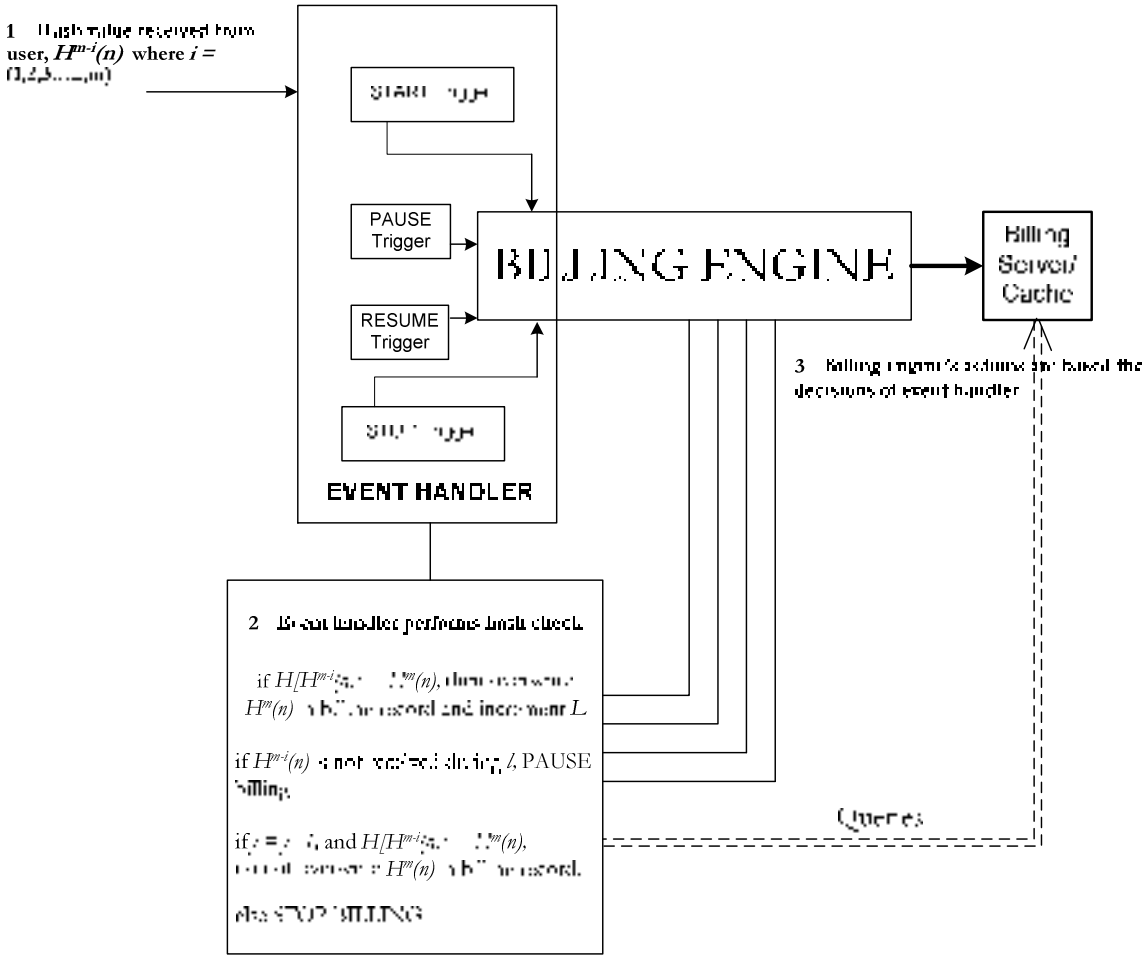

Figure 9 Hash Checking

If the application is network-aware, it may send messages to the PAUSE and RESUME triggers to pause and resume billing respectively. This is intended to prevent the billing database from becoming too fragmented. If the application senses that the network has become too degraded for acceptable service, it may use these triggers to ensure that the user is not billed for unacceptable service. When service is resumed, the billing engine need not write another record to the billing server; it just resumes writing data to the existing one. The PAUSE trigger passes application state information to the RESUME trigger so that it is

aware of the flows that are currently paused. The PAUSE trigger may also be used to pause billing when a hash value interval is missed by the user. This feature is useful in the event of a horizontal handoff. The STOP trigger sends a message to the billing engine to stop writing to the billing record. It does this when the user does not send a hash value for three consecutive hash value intervals. Typically, when three hash value intervals are missed, it is either due to a degraded network connection or the user not using any applications. Either way, the user is no longer actively using the network and billing should be stopped. Even if the missed intervals are as a result of a handover, it is likely that the application would have timed out during this period and a new service request would have to be made.

The billing server may just be a cache itself. Depending on the complexity of the existing network architecture, a billing server may be already present. In this case, the "billing cache" could be used as a temporary storage that writes its information periodically to the main billing system.

Irrespective of the host network, the conceptual operation of the billing engine is the same. The information gathered is transmitted to the billing server securely for storage for a specified period of time.

D. Issues and Challenges

Transmission of billing data: The secure transmission of billing information is central to this protocol. The transmission has to be authenticated, encrypted and signed by the sender i.e. the foreign network. The certificates retrieved during the registration phase have already provided the information needed to do this. The foreign network uses the public key of the home network to encrypt the billing data and then signs the information. The home network then verifies the transmission and decrypts the records.

Since the transport network (for the billing solution) is the Internet, the connectionless nature of IP also raises some concern due to latency. Billing records travelling over different paths or routes could arrive out of order. Higher layers of the protocol stack should take care of this issue. It is not envisaged that latency will be a major concern as the billing application itself runs locally on the data store. Besides, billing information is not time-critical as the user probably gets billed at pre-determined intervals e.g. monthly.

Handoff within the Foreign Network: Although it is assumed that handoff has already been handled at the network level, it is pertinent to postulate what the effect of handoff may be on this billing protocol. Since registration and service requests occur at the network level, the same user information should be made available throughout the network. The 3G networks already have location registers as part of their architecture. However, this kind of location management is not native to WMNs. Through the use of AAA servers, it may be possible for the network to know what foreign users are already registered and what services they have been permitted to use. Thus, when a handoff occurs, the network could use *L* as a keepalive to notice that when the user moves. As mentioned above, the non-receipt of a hash value by the billing system may be due to a degraded link. It is also possible that the user has moved out of the range of the wireless access point. The billing for the user/service combination is paused while the user moves within range of another access point. When the new access point receives the hash value, it performs a hash on it and compares it to what is stored in the billing cache/server. Due to one-wayness of the hash algorithm and the random number used initially, there will be (with high probability) only one hash value that would match this computation. The newly received hash value is then put into the billing record, service is resumed and billing continues. A failure of this operation would cause the application to fail and a new service request would need to be generated.

Depletion of Hash Values: Due to the need to use *L* as a keepalive as well as a timing mechanism for duration-based billing, L should be set to a value as low as

possible. The authors of [57] recommend a value of 6 seconds. However, for long service sessions (e.g greater than 20 minutes), storing enough hash values on the user's smartcard/token will be infeasible. The most logical way around this issue is to generate enough hash values for short flows but implementing a mechanism that would allow the user to generate more hash values as needed without losing the non-repudiation characteristics of chained hashing. The *j* counter can be used to implement this.

As mentioned above, the j counter is initialized to 1 when the service is requested. This information (along with L) is put in the user's billing record. Once the user is about to sent the first hash value (which is the last to be sent according to the protocol), it increases the value of *j* by 1 and sends this to the foreign network. Once the event handler sees the new value for *j,* it still does the hash check but also checks the value of *j* in the billing record. If the hash check is true and the value of *j* received is an increment of 1 compared to the billing record's information, the hash value in the billing record is not overwritten. During the computation period for new hash values, it is possible that the user will miss a hash interval. Though this is not expected (hash algorithms are usually very efficient and fast), at the very worst, it will cause the billing to be paused. The user then repeats step 1 of the service request phase to generate new hash values (preferably based on a new random number) and sends a new $H^m(n)$ at the hash value interval. To make this scheme work, it is necessary that m does not change. It is recommended that m does not exceed 200. 200 hash values is sufficient for 20 minutes of service, assuming L = 6 seconds. Given that the length of each hash is 20 bytes (e.g. a SHA-1 generated hash value), this will require about 4KB of storage on the smart card. Most smart cards can provide this amount of storage.

By doing this, *j* can be used as an indicator of how many times the user ran the hash algorithm during the session. The user can not cheat the foreign network due to the check of the billing record. Neither can the foreign network cheat the

user as it has no way of recursively executing the hash algorithm to get previous hash values.

Roaming: An important piece of this protocol is to reduce the need for a formal roaming agreement between operators. This is a key requirement if the goal of ubiquitous access (part of the promise of WMNs) is to come to fruition. To accomplish this, a "roaming policy" is included in each operator's certificate. As shown in the service registration phase, when a request is made to a home network it validates the identity of the foreign network. The roaming policy tells the home network how the foreign network bills visitors. This policy should be detailed enough to enable the home network make an informed decision. It should categorise traffic by class and unit of billing. The price of each billing unit should also be clearly defined. For instance, the hash value interval may also represent the block of time used to bill voice calls. Even though this interval is in each billing record, it may not be pertinent to the billing of data and multimedia services. It may also state the geographic location of the foreign network.

Based on its pre-defined thresholds, the home network then approves the service request. This shows the foreign network that the home network has agreed to its service of the user. Since there is the possibility of denial based on the foreign network's roaming policy, a hybrid solution where the roaming policy is used in combination with a traditional roaming agreement can be used by the home network. This gives the home network operator the flexibility to assure its subscribers of guaranteed services within a specified area. For instance, an operator in the United States can sell a subscription to a user with guaranteed coverage in North America and optional service in Europe and Asia. In this case, the identity of the networks can be checked against a local database included in the network's certificate server. If there is a match, the service is authorized immediately (thereby skipping the check with the certificate authority). This will also be the case for a network whose roaming policy has

been approved through a previous check. This may also give the operator the flexibility offer more service levels.

Push-Based Services: Due to their nature, some aspects of push-based services (e.g text messages, e-mail) may not be directly billable by the protocol. However, this may not be a huge concern. Even if a service is not requested by the user, the user has to register with the FN. The FN can charge the HN a nominal fee for the registration of a user for the validity period of the certificate C_U. This may also be done through the roaming policy but is probably better implemented using a formal roaming agreement.

Settling of Disputes: FN will submit the billing information, as well as U's temporary certificate C_U, to HN periodically. This will enable FN to receive payment from HN. The billing information includes the service request, the provided service, the hash value interval L and j (on behalf of U). Therefore, a billing record should have the following:

$$U_F, R, m, t_i, H^m(n), j, R', L, S_U(U_F, R, m, t_i, H^m(n)), H^{m-L}(n)$$

HN also adds a timestamp t_r to indicate when the bill was received. U will receive a bill from HN periodically. If U disputes a bill, it requests that HN checks to see if it was wrongly charged. This is acceptable since it is assumed that U trusts HN. However, this request should be presented to HN within a particular time-frame.

To verify the accuracy of the bill, HN will do the following:

1. HN will use V_U to check $S_U(U_F, R, m, t_i, H^m(n))$. HN also compares R and R'
2. HN will check to see $m * j \geq L$.
3. HN will check to see if $H^L(H^{m-L}(n)) = H^m$. $H^{m-L}(n)$, is the last chained hash value received from the user during billing.
4. HN will check to see if $(l * L) \leq T$. Also, HN checks $t_i \leq t_r$.

The first step is to prove that service was requested and the service provided by FN was no higher than the requested level of service. Even though R^i is not signed, the service acknowledgement shows that the U accepted it.

The second step proves that hash algorithm was run enough times to generate enough hash values for the service. This step may be skipped if $j = 1$.

The third step ensures that the service was provided to the user for the duration of the billing record.

Steps 2 and 3 prove that *U* is responsible for the bill.

The fourth step proves that the service must have been provided during the period when the temporary certificate was still valid. The timestamp check is used to prevent replay attacks where FN provided the service to U at some point in the past and attempts to double-bill. It may be possible for U and HN to collude on the fourth step. However, this is highly unlikely. Besides, FN does a check during service request to ensure that an accepted request was sent by U before it was received at FN. It is also noted that neither of the timestamps is used for actual billing.

If any of the steps fail, HN can conclude that U was wrongly charged.

It should be noted that the accuracy of this stage (and indeed the protocol as a whole) is heavily dependent on the synchronization of time. While small discrepancies may be tolerated, efforts should be made to synchronise the timing of all parties involved. This may be done using a synchronization protocol (e.g. secure NTP) and a GPS clock.

Bill Payment: Although the payment arrangement between the home and foreign networks has not been addressed directly in this work, it is expected that the secure implementation of this scheme will leave no ambiguity when a bill has been certified as valid. As such, the foreign network can send a detailed bill to

the home network and expect it to be paid. This can be done via a payment protocol that has been mutually agreed on by both operators. Alternatively, the bill may be paid based on a payment scheme specified in the certificate of the foreign network.

Chapter 4

EVALUATION OF THE SCHEME

Our goal is to evaluate the building blocks of our framework vis-à-vis other architectures that have been documented in the literature.

RoofNet [15] and MeshCluster [58] are two of the architecture frameworks that have been well documented in the literature. In addition, prototypes and testbeds have been implemented to verify their performance and features.

From the perspective of a network operator, the following have to be addressed by a viable architecture:

- Performance issues
- Scalability
- Security
- Accounting & Billing

I. PERFORMANCE

The performance of any network is a critical component that needs to be considered and validated before the network gains acceptance for large scale deployment. In the context of WMNs, issues which affect network performance include:

1. MAC Layer Communication
2. Mesh Routing
3. Application and Service Perspective
4. Interoperability and Integration

MAC Layer Communication: Because of the nature of mesh networks, the MAC function should be accomplished in a distributed manner i.e. to establish multi-point to multi-point links between the mesh nodes quickly while the nodes are joining the network. In addition, a MAC protocol for WMNs has to take connections with multiple hops into account.

Roofnet uses the 802.11 MAC protocol and relies on its routing protocol to ensure that lossy links are avoided. The authors of [15] note that nodes may interfere with each other and cause persistent packet loss. The ETT (Expected Transmission Time) metric used to choose routing links tries to compensate for this by choosing links based on the loss rates of periodic broadcast probe packets sent at each of the 802.11b bit-rates (1, 2, 5.5, and 11 Mbps). It chooses the bit-rate that will achieve the highest throughput after accounting for the cost of 802.11 re-transmissions. It does the best it can using the limitations of a MAC protocol designed for single-hop communications.

MeshCluster employs the enhanced AODV-Spanning Tree (AODV-ST) protocol to proactively construct spanning trees whose roots are the gateways in the mesh network. By building a connectivity tree, the protocol aims to significantly reduce route discovery latency and achieve lightweight, soft state route maintenance. The gateways periodically broadcast RREQ (route request) messages to initiate the creation of spanning trees. Before a RREQ is broadcasted, a gateway sets the *destination-only* flag in the RREQ and sets the RREQ destination address to the network-wide broadcast address. These settings differentiate normal route discovery RREQs from the RREQs for spanning tree creation. As the RREQs are broadcasted hop-by-hop throughout the mesh network, the spanning tree is implicitly formed through the creation of reverse routes to the gateway at the relays. For relay-to-relay communication, a relay node initiates a RREQ with the destination flag set and the destination address set to the address of the node to be

reached. The destination flag is set because the most up-to-date path information is required at the source during path selection.

ACORN uses a multi-stage approach to build neighbourhood cliques. The neighbourhood discovery is done in a distributed fashion to ensure that the entire network does not get affected by multiple nodes initializing at the same time. The use of an alternate neighbour table also helps improve convergence in the event that a node loses the connection to its preferred neighbour. Our scheme also seeks to avoid collisions between nodes with overlapping transmission ranges using its iterative power control algorithm. This helps ensure that we avoid collision and interference between nodes in close proximity.

Routing: Mesh networking requires each node to share route information with other nodes. This functionality is assured by the mesh routing protocol. In addition, features such as scalability, fault tolerance, QoS metrics, load balancing, and cross layer interaction. Mobility and power management are also important in WMNs as users may roam (albeit infrequently) between WMRs and may be power-constrained due to their form factor.

As indicated above, Roofnet uses the ETT metric to build its routing tables and achieve relatively stable performance in a lossy, high-interference environment. The ETT Metric favours routes that minimize the expected transmission time required to deliver a packet across the network. ETT takes into account 802.11b transmit bit-rates as well as loss rates.

In AODV-ST (used in MeshCluster), an RREQ contains a metric field which is set to zero by the gateway. When an intermediate relay receives an RREQ, it checks if the RREQ is a gateway-initiated RREQ. If the condition is satisfied, it creates a reverse route to the gateway provided the RREQ is received on the best known path to the gateway. The relay can make this determination because of the metric field contained in the RREQ. This field is updated by each intermediate relay to represent the characteristics of

the path it has traversed. The specific handling of the field at each relay is dependent on the path metric being used. Once a relay creates a reverse route entry for the gateway, it sends a gratuitous RREP back to that gateway. This gratuitous RREP also has a metric field that is set to zero initially. The field is updated at every intermediate relay on the path to the gateway. When an intermediate relay receives the gratuitous RREP, it creates a forward route to the originating relay. It updates the path metric to the originating relay with the metric value contained in the gratuitous RREP.

According to [58], any routing metric can be used with AODV-ST as long as it satisfies two requirements: the metric must increase in value with increasing hop count and it must be a bi-directional metric, i.e., the metric must give equal weight to a path's performance in the forward and reverse directions. The ETT metric has been tested with AODV-ST but is not an optimal choice for a multi-radio WMN because it does not consider the frequency diversification of a path during path selection [39]. Further exacerbating this issue is the fact that AODV-ST is a distance-vector routing protocol in which link-level information is not disseminated by design. The authors of [58] conclude that this can lead to sub-optimal routing for their architecture. MeshCluster also employs IP-in-IP tunnels to reduce the routing table at relays to the sum total of number of relays and access subnets.

According to the designers of MeshCluster, one possible solution is to use the Weighted Cumulative Expected Transmission Time (WCETT) metric [39]. WCETT requires knowledge about each link in the path, such as the link's delay and its assigned frequency. This complicates the support of WCETT in AODV-ST. Link state protocols that can be used instead of a link-aware routing metric include OLSR and OSPF.

Due to the reasons above, one of the major design aims for ACORN was to make it routing-protocol agnostic. We believe that the service provider should have a choice of what Mesh routing protocol is best suited to run in their network. The node initialization and bootstrapping stages gather a lot of network information that can be fed into a routing protocol to assist in the computation of a metric that accurately

reflects the network's topology. We believe this helps the flexibility of the architecture as newer, improved routing protocols can be integrated into the network over time without major changes to the architecture.

Service Provisioning: Every application has its inherent characteristics which makes it more suited to certain platforms. For example, a "chatty" protocol will work better in a wired network (with lots of high bandwidth links) than on a wireless network. Due to the distributed multihop features of WMNs as well as the lack of cross layer interaction for most applications, there is a need to adapt the existing applications to WMN architecture. Another approach is to deploy new applications that focus on service delivery first and the network second. This will lead to a service model with communication protocols that can deliver similar SLAs over multiple networks.

One key element of service provisioning in WMNs is mobility. Roofnet is specifically targeted for community networks where relays are expected to be static and end-user mobility is minimal. There is very little support for mobility. The MeshCluster architecture was designed to provide support for roaming users via Mobile IP and DHCP based mobility.

ACORN does not directly address user mobility at this time. As noted in [58], there are client-side peculiarities that have to be taken into account. This is one of our priorities for future research. With regards to service provisioning for roaming users, the billing phase of the infrastructure ensures that users can access services in a secure manner from any part of the network.

Interoperability: Due to the emergence of heterogeneous wireless access technologies such as WiFi, WiMAX, Bluetooth, UWB, DVB etc. and the tremendous advancements in cellular systems, interoperability and integration have become major considerations for future wireless systems. WMN is a potential candidate technology to enable the integration of various existing networks through gateway functionalities in the mesh routers.

Neither Roofnet nor MeshCluster address interoperability in their frameworks. ACORN was built with interoperability as one of the cornerstone requirements. The network registration and billing phases of the protocol is essential in providing network services to supporting users from different network types and service providers. The use of a PKI infrastructure helps establish trust without the need for an established roaming agreement between providers.

II. SCALABILITY

Scalability, reliability and robustness are important requirements for any network infrastructure not just WMNs. In typical WMNs architectures of mesh networks, these factors appear to be at odds with each other. For example, strategies designed to provide scalability generally require a hierarchical structure (not a native feature of WMNs). Scalability problems are even more critical in mobile mesh architectures. The typical scalability issues in multi-hop networking apply for WMNs as well. When the scale of the network increases, the end-to-end reliability sharply drops, thereby diminishing the network performance.

Designing a scalable mesh network requires the careful design and proper characterization of the physical layer mechanisms depending on the envisaged application scenarios and a fairly accurate idea of how many users need to be supported. Other considerations include backbone communication topologies, increased wireless spectrum capacity through the use of multiple radios, channels and access schemes.

Roofnet, partly because of its focus on community collaboration, does not have an architecture that can scale on the service provider level. There is no hierarchy in the WMN and the system is not engineered to provide SLA guarantees to its users. For example, volunteer users share their internet connectivity with other users. While this helps improve the redundancy and lower the cost of the network somewhat, it does not allow for a manageable system that can be monitored and provisioned centrally – an essential part of any service provider's network operations.

MeshCluster has a hierarchical structure through the use of gateways and relays so it holds some promise for scalability. However, the use of AODV-ST puts a limit on scalability due to the reactionary nature of the routing updates.

ACORN approaches scalability in the WMN by creating disjoint neighbourhoods of nodes. These neighbourhoods have connectivity to each other via WMGs or 'bridge' nodes – WMRs that have rich connectivity to both WMGs and WMR in other neighbourhoods. This structure takes advantage of the fact that in a service provider network, the majority (if not all) of the services are located in the Core of the network. This enables some structure to be put in place apriori to streamline traffic flow. Another advantage of having disjoint neighbourhoods is the fact that a lot of 'chatty' link-layer traffic can be contained within certain areas of the network when necessary. This helps ensure the stability of the network which in turn improves its scalability.

III. SECURITY

Security is a critical step to deploy and manage WMNs. Since the access to any deployed wireless mesh network is possible for any wireless enabled device, it should be ensured that only authorized users are granted networks' access.

Attacks can be either external or internal to the network and may exist at different layers in WMNs causing the networks' failure. At the physical layer, an attacker may jam the transmissions of wireless antennas or simply destroy the hardware of a certain node. At the MAC layer, an attacker may abuse the fairness of medium access by sending MAC control and data packets or impersonate a legal node. Attacks may occur in routing protocols such as advertising wrong routing updates. At the application layer, an attacker could inject false fake information, thus undermining the integrity of the application. Attackers may also sneak into the network by exploiting the cryptographic building blocks.

Selfishness and greediness are two misbehaviours that are likely to take place in WMNs. Nodes may behave selfishly by not forwarding packets for others in order to save power, bandwidth or just because of security and privacy concerns.

Neither Roofnet nor MeshCluster include any specific mechanisms to provide security natively in the network. ACORN, on the other hand, makes use of secure protocols in a pervasive manner throughout the entire lifecycle of the network. In general, two classes of attacks are likely to occur in WMNs

i) External attacks, in which attackers not belonging to the network jam the communication or inject erroneous information. This can also be termed a DoS (Denial of Service) attack.

ii) Internal attacks, in which attackers are either internal nodes that have been compromised or intruder nodes that are difficult to detect as they may be impersonating legitimate nodes. Both types of attacks may be either passive (eavesdropping) or active (modifying and injecting packets to the network).

Due to the nature of the wireless medium, DoS attacks are hard to predict and mitigate. An attacker could jam the entire wireless spectrum with excessive traffic rendering it unusable. In ACORN, the security credentials are decoupled from the hardware. In addition, they are stored on a tamper-resistant token that is extremely difficult to reverse engineer without credential invalidation. This makes it very difficult for an attacker to impersonate a valid subscriber. No node can access network services until the Network Registration Stage. By this stage, the validity of the node and subscriber would have been verified by the Core Network. If the node does not have valid credentials – it would be extremely hard for an attacker to get some – it does not get added to the network's logical topology.

For legitimate nodes that may behave greedily, traffic policing can be imposed by the network to ensure that network control traffic is not subject to starvation.

Authentication Authorization and Accounting (AAA): Authentication and authorization are important counter-attack measures in WMNs, allowing only authorized users to get connections via the mesh network and preventing adversaries to sneak into the network disrupting the normal operation. AAA is provided in most of the wireless applications and commercial services through a centralized server such as Remote Authentication Dial In User Service (RADIUS). For WMNs, distributed authentication and authorization schemes with secure key management are important. To allow users' mobility with seamless and secure access to the offered services in the mesh network, authentication should be performed during mobile nodes' roaming across different WMRs and across different domains.
To achieve this, continuous discovery and mutual authentication should take place between neighbours, whether these neighbours are mobile nodes or fixed/mobile mesh nodes. Authentication should be regularly checked to ensure that the integrity of the network is not compromised.

There also needs to be security mechanisms in place to prevent attacks on stored keys. To further ensure security of WMNs, security mechanisms need to be embedded into MAC protocols to detect and prevent misbehaviour in channel access, and into network protocols providing secure routing. Generally, pervasive security is desired as attacks occur simultaneously in different protocol layers. It is also important to provide sufficient authentication for user nodes to authenticate mesh nodes or for a down stream mesh node to authenticate an upstream mesh node.

As stated above, neither Roofnet nor MeshCluster include any specific mechanisms to provide security natively in the network. ACORN, on the other hand, makes use of secure protocols in a pervasive manner throughout the entire lifecycle of the network. It also leverages the ability of the network core to provide centralized security services

(AAA, PKI etc.) to ensure that the nodes can be controlled and subscriber credentials validated before permitting access to network services.

It is important to note that there are many similarities between the security scheme in ACORN and those in other wireless infrastructure technologies (e.g. 3G). This is mainly due to the fact that a lot of the mechanisms have been well-established in the literature and real-world implementations and security best practices have been followed. However, there are a few key differences between ACORN and 3G in this regard:

1. Security is pervasive and compulsory in ACORN. All stages of the protocol have security built-in. Unlike 3G, security is not an optional feature. The user is not able to selectively enable/disable security on a per-application basis.
2. Implementation of security is specific to the subscriber and not the device. 3G includes mechanisms for verifying the IMEI of the device. Hardware device information is extremely hard to synchronize on a wide scale and is not considered for ACORN. This is especially true if the goal of using commodity hardware is realized. In ACORN, there is no assumption or need to secure the subscriber's device hardware.
3. For roaming users, the involvement of the foreign network (from a security perspective) is limited to information needed to provide network services and subscriber billing. Authentication and validation of the user is still done by the home network. This ensures that the home network is involved in user authentication and service authorization instead of implicitly trusting the foreign network and delegating all billing control to it.

IV. ACCOUNTING AND BILLING

WMNs need special accounting mechanisms and tailored billing systems with appropriate business models considering the benefits of both mobile users and service providers. To assure service availability and continuity, Inter domain accounting is

important in WMNs. High packet loss ratio and security requirements should be carefully handled in this case, where authentication, replay protection and data integrity are indispensable. The prevailing economic model requires the application of usage sensitive billing systems based on the gathered accounting information for each client.

As far as we know, ACORN is the only documented WMN architecture in the literature that directly addresses billing and service delivery. The billing phase of the protocol functions in a secure manner. All parties involved contribute in the exchanges needed for registration and service provision. Non-repudiation of billing is also provided. The billing solution is platform-independent. To ensure network scalability and flexibility, it is designed as en extension to the basic network architecture. None of the stages are dependent on the underlying network infrastructure.

The billing protocol does not require major changes in the underlying network infrastructure. For the user, a smartcard/token with the necessary credentials is all that is needed. The certificate and authentication infrastructure can be added seamlessly to the network. The billing components can either be implemented on a separate physical entity or as part of existing equipment (e.g. through the addition of a module). This also helps improve the scalability of the billing architecture

Since the proposed architecture does not require any "forklift" changes to the network, it can be implemented after the network is up and running. Its cost can be managed and spread over a period of time. For instance, a service provider may decide to issue new or updated tokens only to subscribers who have a roaming subscription. The protocol does not adversely affect the ability of the network to perform data transmission. With the exception of the billing engine, all other parts of the protocol work at the application layer. If the billing engine is implemented in hardware, any performance degradation may be reduced further.

Through the use of trusted certificates with roaming policies, home networks can approve service for their subscribers on the fly even if they have never had formal dealings with the foreign network before. Certificate authorities can be regionalised (similar to Regional Internet registries) to speed up authentication of service providers.

C h a p t e r 5

CONCLUSION

A major obstacle to the widespread deployment of WMNs as a connectivity solution for large wireless access networks is the operational efficiency of running such a network. The cost of hardware (capital expenditure or 'CapEx') is rapidly falling while the cost of running the infrastructure (operational expenditure or 'OpEx') keeps rising. Hence, even though WMNs offer the promise of quick and easy deployment (in comparison with wired access technologies), the cost of maintaining a stable level of service is still prohibitively high. As a result, over the lifetime of a network, wired access networks may actually turn out to be cheaper.

One key strategy to help make WMNs more competitive is to make it possible for the network to automatically configure wireless mesh nodes in a distributed fashion while ensuring security and service provisioning. In this work, we address this challenge by proposing a solution for the self-configuration of WMNs and the provisioning of wireless subscriber connectivity. This algorithm allows end-point WMN nodes to be automatically provisioned and configured in a secure, distributed and conflict-free manner. It also introduces the concept of decoupling the service from the hardware.

The architecture is both distributed and centralized. The distributed portions include neighbour discovery, topology construction and beaconing. The centralized aspects include monitoring agents deployed on nodes (used to monitor device and network metrics) and report to the central station, QoS and SLA guarantees and security. A key aspect of our architectural framework is that is readily lends itself to a service-provider based service model. We believe this is a critical feature of the system because WMNs have to pass the economic litmus test to be considered a viable technology for the future.

Future Work

We are proposing the construction of a WMN testbed to verify our architecture in real-world scenarios. While we are confident that the framework addresses the requirements of a service–provider managed WMN, we would like to test different channel assignment and WMN routing protocols within the architecture for comparison purposes. We believe this is important as one of our aims with the design of this framework was to allow for flexibility in the implementation of protocols for different functions in the WMN. The evaluation of different MAC and routing layer protocols in a testbed will help guide the implementation of real-world WMNs.

An important goal of this work was the reduction or elimination of provider roaming agreements which hamper true inter-provider service delivery. As a future research goal, power-efficient means for implementing the user aspects of the protocol will be explored. Even though the most computationally-intensive parts of the protocol are done in the provider networks, the access node still has a fair amount of computation to do (random number generation, hashing). This also has an effect on the amount of power that the mobile station consumes.

It may also be possible to optimize and improve the efficiency of the billing phase so that registration and services can be set up more quickly. This will be an important issue for the provision of time-sensitive services like multimedia applications. It is also important for short-lived sessions. The protocol performs similarly for short and long service flows. The effects of horizontal handoff (roaming within the same network) on billing were briefly explored. However, vertical handoff (e.g. if the user returns to the home network during service provision) will be explored in the future as well. The billing phase may also benefit from an open protocol to access subscriber information (QoS, SLA etc.) irrespective of the underlying network architecture. While it is expected that the billing protocol will only need a few tweaks to accommodate prepaid services, its implementation will be explored in the future as well.

BIBLIOGRAPHY

[1] Nortel Networks, *http://www.nortel.com*

[2] Cisco Networks, *http://www.cisco.com*

[3] Tropos Networks, *http://www.tropos.com/*

[4] BelAir Networks, *http://www.belairnetworks.com/*

[5] IEEE 802.11s Task Group S, Meetings Update
http://grouper.ieee.org/groups/802/11/Reports/tgs_update.htm

[6] Municipal Wi-Fi: Easier said than done.
http://www.economist.com/science/displaystory.cfm?story_id=9244199

[7] E L. Yang, P.Zerfos, and E. Sadot, Architecture taxonomy for control and provisioning of wireless access points (capwap)," RFC 4118, June 2005.

[8] I. Akylidiz, X. Wang and W . Wang, "Wireless Mesh Networks: A Survey" Computer Networks – Elsevier Science no. 47, Jan. 2005.

[9] B. Schrick and M. Riezenman. Wireless Broadband in a Box. IEEE Spectrum Magazine, pp. 38–43, June 2002.

[10] Mihail L. Sichitiu. Wireless Mesh Networks: Opportunities and Challenges. in Proc of the Wireless World Congress, (Palo Alto, CA), May 2005.

[11] D. Beyer. Fundamental Characteristics and Benefits of Wireless Routing ("Mesh") Networks. in Proc. of the International Technical Symposium of the Wireless Communications Association, (San Jose, CA), Jan. 2002.

[12] S. G. Methley et al, "Efficient Mobile Mesh Networking: Testing Scalability Hypotheses," IEE 3G and Beyond, London, 2005.

[13] M. Pietro and R. Molva, Chapter 12 in book. "Mobile Ad hoc Networking," John Wiley and Sons, 2004.

[14] S.R. Murthy and B.S. Manoj, "Ad hoc Wireless Network Architectures and Protocols," Prentice Hall PTR, 2004.

[15] D. Aguayo, J. Bicket, S. Biswas, D.S.J. De Couto, R. Morris, "MIT Roofnet Implementation". http://pdos.lcs.mit.edu/roofnet/design/

[16] M. J. Lee and al.,"Emerging Standards for Wireless Mesh Technology," IEEE Wireless Communication, April 2006.

[17] M. Uhm, "Making the Adaptivity of SDR and Cognitive Radio Affordable," DSP Magazine, May 2006.

[18] Y. Liu, E. Knightly. Opportunistic Fair Scheduling over Multiple Wireless Channels. in Proc. of IEEE INFOCOM '03.

[19] A. Nasipuri, S. Das. A Multichannel CSMA MAC Protocol for Mobile Multihop Networks in Proc. of IEEE WCNC '99.

[20] J. Li, C. Blake, D. De Couto, H, Imm, L. Morris. Capacity of Ad Hoc Wireless Networks. International Conference on Mobile Computing and Networking, 2001

[21] H. Ju and I. Rubin, "Backbone Topology Synthesis for Multi-Radio Meshed Wireless LANs," proceedings of IEEE INFOCOM 2006.

[22] H. Moustafa et al, "A Panorama on Wireless Mesh Networks: Architectures, Applications and Technical Challenges," WIMESHNETs 06, August 2006

[23] P. Kyasanur and N. H. Vaidya, "Detection and Handling of MAC Layer Misbehaviour in Wireless Networks," International Conference on Dependable Systems and Networks (DSN'03), 2003.

[24] M. Raya, J. P. Hubaux, I. Aad, "Domino: A system to detect greedy behavior in IEEE 802.11 hotspots," 2nd International Conference on Mobile Systems, Applications and Services (MobiSys2004), 2004.

[25] X. Zheng et al., "A Dual Authentication Protocol for IEEE 802.11 WLANs", International Symposium on Wireless Communication Systems (ISWCS'05), 2005.

[26] J. So, N. Vaidya, "Multi-channel MAC for ad hoc networks: handling multi-channel hidden terminals using a single transceiver", *ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC), pp. 222–233, May 2004*.

[27] F. Cali, M. Conti, E. Gregori, "Dynamic tuning of the IEEE 802.11 protocol to achieve a theoretical throughput limit", *IEEE/ACM Transactions on Networking 8 (6) (2000) 785–799*.

[28] D. Qiao, K. Shin, "UMAV: a simple enhancement to IEEE 802.11 DCF", *Hawaii International Conference on System Science, 2002*.

[29] Y.B. Ko, V. Shankarkumar, N.H. Vaidya, "Medium access control protocols using directional antennas in ad hoc networks", *IEEE Annual Conference on Computer Communications (INFOCOM), pp. 13–21, 2000*

[30] R.R. Choudhury, X. Yang, R. Ramanathan, N.H. Vaidya, "Using directional antennas for medium access control in ad hoc networks", *ACM Annual International Conference on Mobile Computing and Networking (MOBICOM), pp. 59–70, 2002.*

[31] N. Poojary, S.V. Krishnamurthy, S. Dao, "Medium access control in a network of ad hoc mobile nodes with heterogeneous power capabilities", *IEEE International Conference on Communications (ICC), pp. 872–877, 2001.*

[32] "Cometa Networks shutting down", *http://www.wi-fiplanet.com/news/article.php/3355671*

[33] Y.-C. Tseng, C.-S. Hsu, T.-Y. Hsieh, "Power-saving protocols for IEEE 802.11 based multi-hop ad hoc networks", *IEEE Annual Conference on Computer Communications (INFOCOM), pp. 200–209, 2002.*

[34] K. Jain, J. Padhye, V. Padmanabhan, L. Qiu, "Impact of interference on multi-hop wireless network performance", *ACM Annual International Conference on Mobile Computing and Networking (MOBICOM), September 2003, pp. 66–80.*

[35] J. So, N. Vaidya, "Multi-channel MAC for ad hoc networks: handling multi-channel hidden terminals using a single transceiver", *ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC), pp. 222–233, May 2004.*

[36] P. Bahl, R. Chandra, J. Dunagan, "SSCH: slotted seeded channel hopping for capacity improvement in IEEE 802.11 ad hoc wireless networks", *ACM Annual International Conference on Mobile Computing and Networking (MOBICOM), pp. 216–230, 2004.*

[37] Engim Inc., Multiple Channel 802.11 Chipset. *http://www.securitytechnet.com/resource/rsc-center/Tolly/TS204116.pdf*

[38] A. Adya, P. Bahl, J. Padhye, A. Wolman, L. Zhou, "A multi-radio unification protocol for IEEE 802.11 wireless networks", *International Conferences on Broadband Networks (BroadNets), 2004.*

[39] Microsoft Mesh Networks. "Self-Configuring Wireless Mesh Networks", *http://research.microsoft.com/en-us/projects/mesh*

[40] H. Cheng, N. Xiong, L.T. Yang, "Distributed scheduling algorithms for channel access in TDMA wireless mesh networks". *Journal of Supercomputing, Volume 45 , Issue 1 , July 2008 pp.105-109*

[41] L. Li, J.Y. Halpern, P. Bahl, Y-M. Wang, R. Wattenhofer, "A cone-based distributed topology-control algorithm for wireless multi-hop networks", *IEEE/ACM Transactions on Networking, Volume 13 , Issue 1 (February 2005) pp. 147 - 159*

[42] C.L. Fullmer and J.J. Garcia-Luna-Aceves, "Solutions to Hidden Terminal Problems in Wireless Networks," Proceedings of ACM SIGCOMM '97, Cannes, France (Sep. 14-18, 1997).

[43] Firetide Networks. *http://www.firetide.com*

[44] R. Ogier, F. Templin, M. Lewis, "Topology dissemination based on reverse-path forwarding (TBRPF)", *IETF RFC 3684, February 2004.*

[45] D.B. Johnson, D.A. Maltz, Y.-C. Hu, "The dynamic source routing protocol for mobile ad hoc networks (DSR)", *IETF Internet-Draft, July 2004.*

[46] A. Raniwala, K. Gopalan, and T. Chiueh. "Centralized channel assignment and routing algorithms for multi-channel wireless mesh networks". *Mobile Computing and Communication Review,8(2) pp. 50–65, 2004.*

[47] J. Tang, G. Xue, and W. Zhang. "Interference-aware topology control and qos routing in multi-channel wireless mesh networks". *MobiHoc '05, pages 68–77, New York, NY, USA, ACM Press, 2005.*

[48] R. Draves, J. Padhye, B.Zill, "Routing in Multi-Radio, Multi-Hop Wireless Mesh Networks", *ACM Mobicom, 2004.*

[49] Y. Yang, J. Wang, R. Kravets, "Interference-aware load balancing for Multihop Wireless Networks", *Tech. Rep. UIUCDCS-R-2005-2006-2526, Department of Computer Science, University of Illinois at Urbana-Champaign, 2005.*

[50] FIPS Pub 197, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, US Department of Commerce/N.I.S.T., Springfield, Virginia, November 26, 2001. *Available from http://csrc.nist.gov/.*

[51] S. M. Matyas, C. H. Meyer, and J. Oseas, "Generating strong one-way functions with cryptographic algorithm," *IBM Tech. Disclosure Bull., vol. 27, no. 10A, 1985, pp. 5658-5659.*

[52] T.S. Messerges, J. Cukier, T.A.M. Kevenaar, L. Puhl, R. Struik, E. Callaway, "A security design for a general purpose, self-organizing, multihop ad hoc wireless network", *Proceedings of the 1st ACM Workshop on Security of Adhoc and Sensor Networks, 2003, pp. 1–11.*

[53] J.H. Park, "Wireless internet access for mobile subscribers based on the GPRS/UMTS network", *IEEE Communiations Magazine, pages 38–49, April 2002*

[54] S. Blott, C. Martin, Y. Breitbart, J. Brustoloni, T. Gramaglia, H. Korth, D. Kristol, R. Liao, E. Scanlon, A. Silberschatz, "User-Level Billing and Accounting in IP Networks", *Bell Labs Tech. Journal, September 1999*

[55] M. Currence, A. Kurzon, D. Smud, L. Trias., "A Causal Analysis of Usage-based billing on IP Networks" *http://citeseer. nj.nec.com/currence00causal.html*

[56] M. Buddhikot, G. Chandranmenon, S. Han, Y. W. Lee, S. Miller, L. Salgarelli, "Integration of 802.11 and Third-Generation Wireless Data Networks", *IEEE INFOCOM 2003*

[57] J. Zhou and K-Y Lam, "Undeniable Billing in Mobile Communication", *Mobile Computing and Networking, pp. 284-290, 1998*

[58] K. Ramachandran, M. Buddhikot, G. Chandranmenon, S. Miller, E. Belding-Royer, and K. Almeroth. On the Design and Implementation of Infrastructure Mesh Networks. *In IEEE WiMesh2005, San Jose, CA, Sept 2005.*