# A Panorama on Wireless Mesh Networks: Architectures, Applications and Technical Challenges

Hassnaa Moustafa
France Telecom, Division R&D
Issy Les Moulineaux, France
Hassnaa.moustafa@orange-ft.com

Usman Javaid, Tinku Mohamed Rasheed,
Sidi-Mohammed Senouci, Djamal-Eddine Meddour
France Telecom, Division R&D
Lannion, France

***Abstract*—** Wireless mesh networks have emerged as a key technology for next generation wireless networks, showing rapid progress and inspiring numerous applications. This type of network seems significantly attractive to network operators for providing new applications that cannot be easily supported by other wireless technologies. The persistent driving force in the development of wireless mesh networks comes from their envisioned advantages including 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 witnessed mass market deployment. To promote the deployment of wireless mesh networks and enhance their usage, many research challenges should be considered. In this paper, we describe the possible architectures for wireless mesh networks giving a practical view on the usage scenarios and applications to turn wireless mesh networks into commodity. Furthermore, we present some technical challenges, from an industrial practice, for the deployment of wireless mesh networks and we highlight the open research issues in this field. We focus on the critical factors influencing the performance and scalability of these networks, security issues in order to assure that only authorized users are granted networks access, billing/accounting that is beneficial for clients as well as providers and the standardization efforts in this field.

*Keywords-component: Wireless Mesh Networks, Security, AAA, Performance, Scalability, Standardization.*

## I. INTRODUCTION

The area of wireless networks has gained increased importance and development during the past decade. On one hand, self organizing wireless networks (or Mobile Ad hoc Networks) are one such domain and it provides an innovative way for users to build networks at will. This user driven network, created ‘on the fly’ dynamically adjusts to conditions as nodes join or leave the network. Such a network can operate in a standalone fashion and to a certain extent is not subject to reasonably interesting business models. In contrast, the traditional cellular networks such as GSM/GPRS and UMTS networks lie in the category of infrastructure network, deployable by the network operator. The services offered in these networks are managed by the operator who is fully controlling the deployed infrastructure, with no management flexibility for the end-users. Recently, a third paradigm has emerged called Wireless Mesh Networks which lays half way between the ad-hoc and infrastructure networking domains.

Wireless Mesh Networks is an emerging 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 APs, forming at the same time a self-organized wireless backbone. 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 WMRs gateways. In both cases, the WMN's backbone is in charge of relaying all the traffic from/to WMCs. An architecture example of WMNs is given by the IETF CAPWAP WG in [1], while a comprehensive survey on WMNs and related issues is given in [2].

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.

Mesh networking is a very interesting next generation wireless paradigm which is extensively discussed in this article considering the network operator's perspective. The emergence of new wireless access technologies and standards like 802.16 (WiMAX), UWB, beyond 3G cellular, 802.11 (WiFi) etc. along with the WMN architecture is promising to enable larger cells, provide higher data rates and greater distances, and improve the capacity of multimedia communications – while offering the consumers with a greater choice and flexibility. These aspects have generated interests towards a wide variety of potential applications and usage scenarios for the mesh networking domain. However, there are various practical issues, particularly relating to performance, quality of service, security, network management and monitoring, scalability etc. that need to be solved in order to accredit the mesh network with a commercial breakthrough for network operators and service providers.

The rest of the paper is organized as follows. The next section presents a brief overview of the mesh network architecture. Section III discusses the various applications and prospective usage scenarios for mesh network and Section IV describes the research challenges to be intercepted from a network operator's perspective. Section V describes the various standardization activities for mesh networking and finally, in Section VI, we conclude the paper.

## II. WIRELESS MESH NETWORK 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 [2]. Figure 1 illustrates an example of this classification. 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. Finally, the architecture as a whole represents the hybrid mesh architecture, where mesh clients can connect to the service platform through mesh routers as well as directly meshing with other mesh clients (assuming that the mesh clients can be directly connected to the service platform). 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 driven by the user and application needs for content [3].

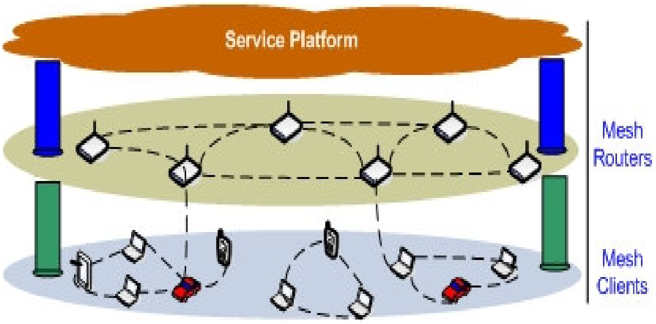

Figure 1. Mesh Network Architectures

## III. APPLICATIONS AND USAGE 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 [4]. In open mesh networks, any client node may participate. These networks may belong to different operators or administrative domains constituting a mesh federation [5]. 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 this classification, different usage scenarios are possible for both indoor and outdoor wireless mesh networks.

In the following, we discuss few practical usage scenarios and applications for closed and open mesh networks. These include, single meshed home network managed by the network owner for broadband home networking applications where the topology evolution of the home network can be based on an AP range-extended mesh network configuration or on a multi-device cooperative mesh configuration; 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. Meshes also help to tie together and to coordinate many weapons and systems in monitoring and managing the battlefield; 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.

Example scenarios for open mesh networks include: Community mesh networks deployed by operators in residential zones for provisioning of grass-roots communities wireless networks allowing them to share Internet connections via gateways. The community wireless mesh networks also enable many peer-to-peer neighbourhood applications, providing critical business opportunities in developing countries and rural areas. Metro-scale mesh networks are a broader version of community mesh networks 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; a viable application for mesh network technology would be to provide an alternate route, alongside WLAN and 3G etc., into such a core network. The mesh chain can hop around corners in an urban environment in a way the cellular systems cannot thus enabling mesh networking to be an extender of today's communication solutions.

Mesh networks also introduce an interesting business perspective when used along with wireless sensor networks. The interesting scenarios where the sensor-mesh combination will be useful are in industrial monitoring, home monitoring and building automation, environmental monitoring, value asset and perimeter security etc.

## IV. RESEARCH CHALLENGES FROM A NETWORK OPERATOR'S PERSPECTIVE

Alongside the strong and attractive features of mesh networks comes a plethora of issues, challenges and options that need to be addressed in order to devise ways for the network operator to offer innovative and unforeseen services. In this section, we present different research challenges facing mesh networks.

### 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 have been characterized below:

1. Distributed MAC and Multi-hop 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 is concerned with more than one hop connections. The aforementioned requirements make the design of the MAC functions highly challenging. Several distributed multi-hop MAC protocols have been proposed 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 real commercial breakthrough. 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 and the understanding of the used network and its application is very important in determining the practical utility of mesh networks and the enabling technologies. It is also important to consider how mesh networks could live alongside existing radio systems, in terms of interference and coexistence strategies.

#### 2. 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. But due to the fact that the ad-hoc routing protocols lack various important performance factors such as scalability, fault tolerance, QoS metrics, load balancing, lack of cross layer interaction etc., some open issues in ad-hoc routing domain should initially be solved. In contrast, certain areas such as mobility and power management in ad-hoc networks and WMNs have totally different requirements, which made ad-hoc routing solutions not appropriate for WMNs. In order to resolve the above issues, innovative solutions are indispensable in WMNs

#### 3. Application and Service Perspective

Every application and service has its own inherent characteristics which makes it work 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 serious need to adapt the existing applications to WMN architecture. Moreover, considerable efforts are also required to discover innovative new applications which at first, make the life of the customer easier and craft the WMNs to appear as a distinctive wireless network solution, at second.

#### *4.* Interoperability and Integration

Due to the emergence of heterogeneous wireless access technologies such as WiFi, WiMAX, Bluetooth, UWB, DVB etc. and the tremendous advancements in cellular systems, the interoperability and integration have become serious concerns for future wireless systems [17]. WMN is a potential candidate technology to enable the integration of various existing networks through gateway functionalities in the mesh routers. However, active research should be performed in this interesting domain to enable the users to seamlessly utilize services irrespective of the network concerned, which is actually providing that service.

### *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. In typical architectures of mesh networks, these factors generally go against each other due to its self-adjusting and non-hierarchical nature. Scalability problems are even more critical in mobile mesh architectures. When the issue of network responsiveness is added on top of all these characteristics, the equation becomes even more complicated and the guarantees of Quality-of-Service for the clients are disturbed. The typical scalability issues in multi-hop networking apply for mesh networks too, since multi-hop communications is common in WMN, i.e., 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 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 [6] 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. 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. Two classes of attacks are likely to occur in WMNs [7]: 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 [8].

#### 1. Different layers Attacks and Misbehavior 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 through special scheme as for example the rational exchange scheme [9], ensuring that a misbehaving party can not gain anything from misbehaviour. Furthermore, the absence of a central authority, a trusted third party or a server to manage security keys necessitates distributed key management.

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. Watchdog, CONFIDANT and Catch are three approaches developed to detect selfishness and enforce distributed cooperation and are suitable for WMNs [10]. Watchdog is based on monitoring neighbours to identify a misbehaving node. However, CONFIDANT and Catch incorporate an additional punishment mechanism providing necessary incentive for cooperation. As well, nodes may behave greedily in consuming channel and bandwidth for its own benefits. A mechanism that modifies 802.11 for facilitating the detection of greedy nodes is proposed in [11], also a scheme named DOMINO [12] is used to solve the problem of a greedy sender in IEEE 802.11 WLANS with a possible extension to multihop wireless networks.

### 2. 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. Authentication, Authorization and Accounting (AAA) are provided in most of the WLANs applications and commercial services through a centralized server such as RADIUS or Diameter. However, the 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. To achieve this, continuous discovery and mutual authentication should take place between neighbours, whether these neighbours are mobile nodes or fixed/mobile mesh nodes. Nevertheless, if mobile nodes move back to the range of previous authenticated neighbors or mesh nodes, it is necessary to perform re-authentication in order to prevent an adversary from taking advantage of the gap between the last association and the current association with the old neighbour to launch an impersonation attack. The IEEE 802.11i proposes a key caching option to mitigate the overhead of re-authentication; 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, where decentralized key management is necessary. Finally, the Wireless Dual Authentication Protocol (WDAP) [13] 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.

### 3. Design Considerations for WMN Security Solutions

To further ensure security of WMNs, some essential strategies need to be considered. 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. Generally, multi-layer security is desired as attacks occur simultaneously in different protocol layers. It might be important to develop a cross-layer framework for security monitoring to detect attacks responding quickly to them. Furthermore, it is necessary to provide sufficient authentication for user nodes to authenticate mesh nodes or for a down stream mesh node to authenticate an upstream mesh node. However, it is important to be mindful of the overhead caused by authentication as wireless users or mesh nodes are often constrained by limited battery, computing power 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. It is recommended that these systems allow online payment or pre-paid tokens. However, processing delay constraints should be considered as well as the need for authentication and integrity.

## V. MESH NETWORK STANDARDIZATION ACTIVITIES

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) [14,15]. 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 and.

Furthermore, the ZigBee Alliance has been working on the specifications of Low Rate WPANs (LR-WPANs) based on *802.15.4*. To date, the ZigBee standard is the only market-ready wireless mesh standard. 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 [1]. 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 [16]. SDR technology is promising to operator in terms of increasing network capacity and simplifying network reconfiguration at the same time. Also, SDR can be a powerful aid to manufacturers in providing multi-standard multi-band equipments, with reduced deployments efforts and costs, through simultaneous multi-channel processing

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.

## VI. CONCLUSIONS AND OUTLOOK

Wireless mesh networks have emerged as a promising new technology, where several vendors are offering services for their deployment. In this paper we have reviewed several important research challenges in WMNs interesting for the network operators to study the feasibility and robustness of mesh networks of mesh networks deployment for fault-tolerant applications or for offering innovative and harbingering services to clients. Cost of deployment of the network will be the main driving factor for the success of WMNs. The design choice of the mesh network at each concerned layer of operation is important for the efficient functioning of the network with respect to the performance and scalability. Owing to the physical and link layer issues, capacity enhancement procedures should be realized by exploiting the multi channel, multi radio, multi flow protocols, arriving at an integrated view on MAC functioning. Efficient cross layer designs could also provide better performance of mesh networks. As the next generation communication domain is under realization, interoperability of mesh network with different technologies is an interesting challenge and contrastingly, how mesh networking can be useful to contribute to a unified access network vision is gathering attention.

Security is a strong challenge influencing to a great extent 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.

To enable economies of scale and ensure interoperability, large companies and industry alliances are actively involved in the development of WMNs and several IEEE standards TGs are working on new standards for these networks. Despite the remarkable inherent characteristics, considerable range of standardized technologies and innovative and profitable applications which have been envisaged with this prominent technology, the network operator would always be reluctant to invest at a large scale until the presented research challenges are solved. Therefore, a significant contribution from the research community is required to take WMNs from myth to reality.

## REFERENCES

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

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

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

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

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

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

[7] Lidong Zhou and Zygmunt Haas, "Securing Ad hoc Networks," *IEEE Network Magazine*, 13(6):24-30, 1999.

[8] M. Raya and Jean-Pierre Hubaux, "The Security of Vehicular Networks," *ACM Workshop on Security of Ad hoc and Sensor Networks, SASN05*, 2005.

[9] I. F. Akyildiz, W. WANG, "A Survey on Wireless Mesh Networks," *IEEE Radio Communications*, September 2005.

[10] B. Wang, "Survey on Wireless Mesh Networks," Technical Report, http://www.cse.msu.edu/~wangbo1/papers/survey.pdf.

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

[12] 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.

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

[14] R. Bruno, M. Conti and E. Gregori, "Mesh Networks: Commodity Multihop Ad hoc Networks," *IEEE Communication Magazine*, March 2005.

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

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

[17] U. Javaid et al, "Towards Universal Convergence in Heterogeneous Wireless Networks using Ad Hoc Connectivity," 9th *Intl. Symposium on Wireless Personal Multimedia Communications (WPMC'06)*, 2006