Mesh Technology enabling Ubiquitous Wireless Networks

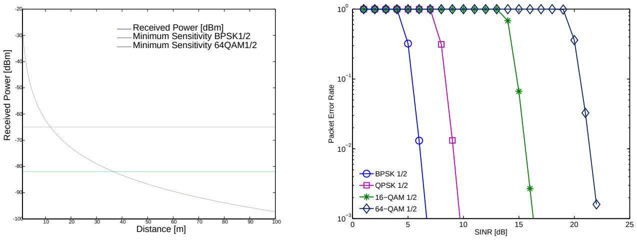
(Invited Paper)

Guido R. Hiertz*, Sebastian Max*, Erik Weiß*, Lars Berlemann*, Dee Denteneer†, Stefan Mangold‡
*Chair of Communication Networks, Faculty 6, RWTH Aachen University, Aachen, Germany
E-Mail: {grh|smx|erw|ber}@comnets.rwth-aachen.de
†Philips, Eindhoven, The Netherlands
‡Swisscom Innovations, Bern, Switzerland

***Abstract*— Today's wireless networking technology provides high data rates. With IEEE 802.11n products, data rates beyond 500 Mb/s are soon feasible for *Wireless Local Area Network (WLAN)*. Due to a standstill in standardization the project IEEE 802.15.3a it was disbanded in 2006. Companies are pushing therefore their own solutions to the *Wireless Personal Area Network (WPAN)* market. Shortly, 480 Mb/s will be available for WPAN applications. For large scale networks, IEEE 802.16 (aka *Worldwide Interoperability for Microwave Access (WiMAX)*) offers a solution for the *Wireless Metropolitan Area Network (WMAN)* market. Besides point-to-point connections, IEEE 802.16e supports mobile connections too.**

With recent development, wireless technology for ubiquitous connections is available in the market. Sensitive *Modulation and Coding Schemes (MCSs)*, *Multiple Input/Multiple Output (MIMO)* and other new *Physical Layer (PHY)* technologies provide high data rates. However, upcoming wireless technology does not increase coverage. Like preceding standards, highest data rate is only available for short range communication. Therefore, supply of large areas with high speed connections demands dense installation of backbone connected devices. While *Capital Expenditure (CAPEX)* for hardware is low, deployment is expensive. The *Operational Expenditure (OPEX)* of wired and fiber optic networks is high. Furthermore they are not as widely deployed as needed for dense installation of connection points to the core network. Hence, rollout of high speed wireless networks is delayed until a solution is provided. Relay based deployment and Mesh topology for wireless networks helps to overcome the cost barrier. With this meshing functionality, wireless networks of the IEEE 802 standard family are a promising low-cost alternative to cellular *Third-Generation (3G)* networks In this paper we provide insight to current activities of *Institute of Electronics and Electrical Engineering (IEEE) Working Groups (WGs)* regarding Mesh technology. Furthermore we show possibilities and limitations of *Wireless Mesh Networks (WMNs)*.

***Index Terms*— Wireless Mesh Networks, IEEE 802.11s, IEEE 802.15.5, IEEE 802.16j, WLAN, WPAN, WMAN**



(a) Received power vs. distance

(b) Packet error rate vs. SINR

Fig. 1. At 100 mW transmission power and attenuation factor $\gamma = 3.5$ a 64-QAM¾ MCS that supports 54 Mb/s according to IEEE 802.11a has a range of approximately 10 m. However, distance is not the only value to consider. Depending on network topology, devices experience different amount of interference. Main source of interference are other devices in and out of own reception range. Interference determines SINR. SINR has direct impact on PER. Thus, interference is another factor limiting the performance of wireless networks.

I. Introduction

CURRENT research in the field of *Multiple Input/Multiple Output (MIMO)* and *Ultrawideband (UWB)* technology enables wireless high speed *Physical Layer (PHY)* technologies for mass markets. Similar to legacy technology, highest data rate demands high *Signal to Interference plus Noise Ratio (SINR)*. As transmission power and bandwidth is limited, coverage becomes limited too. Highest data rates are available on short range only. To cover large areas with wireless high speed access, dense deployment of network infrastructure is needed. Current *Institute of Electronics and Electrical Engineering (IEEE)* standards define different network infrastructures. In IEEE 802.11 [1] an *Access Point (AP)* provides network access and offers association service to the stations. Stations can roam between different APs. Although medium access is distributed, it is the AP's responsibility to hand-over sessions and to forward frames from and to other stations or networks. Thus, the physical topology in IEEE 802.11 *Wireless Local Area Network (WLAN)* is centralized with the AP remaining in the center. For high rate *Wireless Personal Area Network (WPAN)* IEEE defines 802.15.3 [2]. Similar to IEEE 802.15.1 (aka Bluetooth), IEEE 802.15.3 uses centralized medium access. A *Piconet Controller (PNC)* grants medium access and manages its associated *Devices (DEVs)*. Thus, IEEE 802.15.3 builds physical and logical star topologies. The PNC has full control over the *Wireless Medium (WM)*. A comparable topology exists in IEEE 802.16 [3], [4]. The *Wireless Metropolitan Area Network (WMAN)* standard describes solution known from *European Telecommunications Standards Institute (ETSI) Broadband Radio Access Networks (BRAN) High Performance Local Area Network 2 (H2)*. A *Base Station (BS)* controls medium access and provides service to its associated *Subscriber Stations (SSs)*. IEEE 802.16 supports point-to-point and point-to-multipoint connections. WMANs can operate in

WICON'06, The 2nd Annual International Wireless Internet Conference, August 2-5, 2006, Boston, MA, United States

licensed and unlicensed frequency bands. Therefore, all current wireless high speed technology uses a kind of centralized approach. Depending on regulatory rules, different power limitations exist:

- Licensed operation of IEEE 802.16 may use up to 30 W depending on the frequency band,
- Radio communication in the 2.4 GHz *Industrial, Scientific, and Medical (ISM)* band is limited to 100 mW in many countries,
- 100 mW to 1 W output power is allowed in the 5 GHz license-exempt band and,
- the US *Federal Communication Comission (FCC)* grants permission for UWB communication in the spectrum between 3.1 GHz and 10.6 GHz with transmission power not exceeding 74.1 μW/MHz.

Thus, in many scenarios, sufficient SINR can be achieved only on short range, see Fig. 1. To provide high data rate, dense deployment of central wireless network coordination entities is needed. With products designed for mass market applications such as *Voice over IP (VoIP)* hardware costs are no limiting factor. However, *Capital Expenditure (CAPEX)* increases due to needs for backbone connection. All aforementioned central entities operate as bridges that connect the wireless broadcast segment with a network of a different technology. In many cases such backbone is built upon networks that use technologies defined in the set of IEEE 802.3 (Ethernet) standards. The wired backbone is used by central entities to share information, forward frames and to manage the wireless network. With dense deployment of wireless-to-wired bridges in large area, wired network must be densely installed too. Fiber optic links can overcome length related issues. However, installation is expensive especially in in outdoor deployment. To reduce cost, relaying technology provides the alternative.

The rest of the paper is organized as follows. In section II we introduce *Wireless Relay Networks (WRNs)* and describe their application. In section III we introduce *Wireless Mesh Networks (WMNs)* and explain differences to WRNs. Furthermore, we explain phenomena that emerge in WMN. In section IV we give an overview to current Mesh related activities in the IEEE 802. In section V we provide an overview of the current draft for Mesh WLAN in the IEEE 802.11 *Working Group (WG)*. Simulation results in section VI performance and section VII concludes the paper.

II. Wireless Relay Networks

Relay-based deployments have three main advantages:

- Capacity optimization,
- area optimization and
- the provision of coverage to shadowed areas [5].

Coverage range of central entities can be extended when the relay device acts as slave device to another entity, see Fig. 2. Relay devices operate under guidance of the central entity and provide the same services to client devices. Data to or from the central entity is sent to or from a client device via the relay device. Hence, data is relayed via a multi-hop path. Although a centrally coordinated *Wireless Relay Networks (WRNs)* may use several hops, usually a two hop approach is applied. Relays may be fixed or mobile. The introduction of relays decreases communication distances and thus improves *Signal to Interference plus Noise Ratio (SINR)* allowing the usage of more sensitive and faster *Modulation and Coding Schemes (MCSs)*.

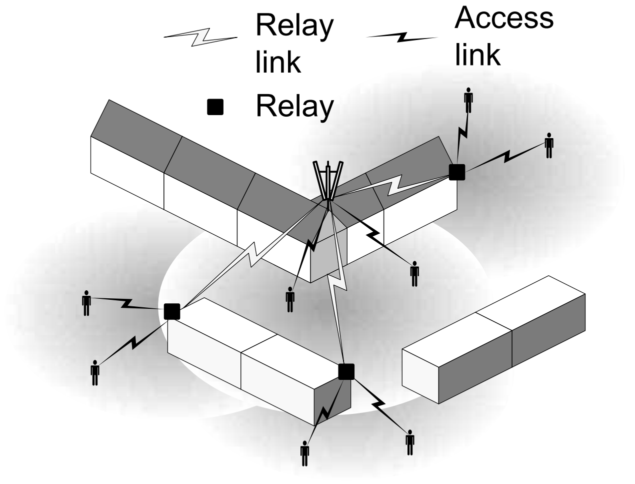


Fig. 2. In WRNs central entities coordinate multiple relay devices. The relay devices operate as slaves to the master device. Relays work transparently, thus they provide the same services to the client devices as the central entity does. Relays are dependent on the central entity. Without the master device they cannot operate.

With regard to frequency channels, a relay based system can be classified according to in-band and out-of-band operation. WRNs may operate on single or multiple frequency channels. With single frequency WRNs, client and relay traffic share the same frequency band and the relaying is don in the time-domain. The WRNs operates in-band with the access side traffic. Coexistence support is necessary and fine traffic segregation is needed to provide the WRN with necessary resources to forward remote and locally generated traffic. Multiple channels may be exploited with a single or multiple radios in WRNs devices. With multiple frequency channels static traffic segregation is possible. Access side and relaying traffic can be delivered on different frequency channels. However, distribution of the access side to different channels and dynamic channel assignment for the WRNs may potentially increase the overall capacity compared to static frequency assignment.

III. Wireless Mesh Networks

Devices of *Wireless Relay Networks (WRNs)* operate under guidance of a coordination entity: The relays introduce an intermediate level in hierarchy. The coordinating instance delegates responsibility to the relays. If the coordinating instance fails, the WRN cannot operate. While relay devices depend on other entities, devices in *Wireless Mesh Networks (WMNs)* may operate on their own. A WMN extends functionality provided

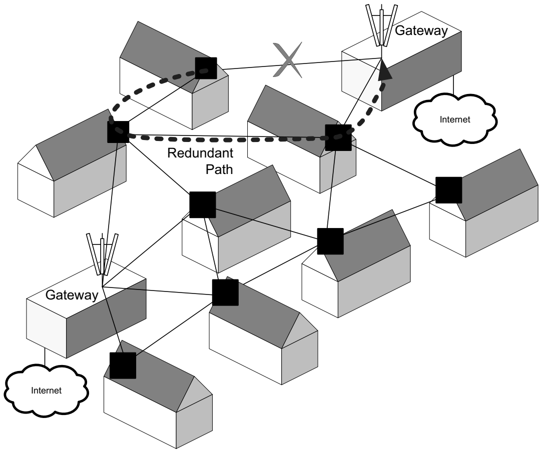


Fig. 3. WMNs can form arbitrary network topologies. Each WMN device has several neighbors. Thus redundant paths exist. In case of failed neighboring device or failed link, WMN devices can reroute traffic. As each WMN device works as wireless router, the WMN devices operate autonomously.

by WRNs. Each device in a WMN operates as a wireless router [6] with possibly several paths available to a desired destination. In contrast, WRN devices communicate with other pre-defined devices only. The topology of information exchange forms a star topology with the coordinating entity in the center in the WRN. However, topology in WMN is totally different, see Fig. 3. Since WRNs provide sub-set functionality of WMNs, in the following we focus on WMNs.

A. Usage scenarios

Besides fixed infrastructure deployment, *Wireless Mesh Network (WMN)* technology is applied in highly changing environment too. The following usage scenarios have been identified by different standardization bodies:

- Car to Car WMNs help to avoid accidents. While in motion at high speed, cars constantly exchange information. The information is distributed to other cars that receive danger warning messages earlier. Furthermore, oncoming cars can relay traffic and warn of hidden obstacles or difficult road conditions. Message prioritization is an important element to allow for low delay message exchange.
- Military application of WMN foresees ad-hoc scenarios, where combatants use the wireless network for distributed, decentralized communication among the troops. Tanks may operate as back haul network of the WMN providing access for soldiers. Tanks move in combat units that have low relative speed to each other. Self-healing and redundant path for frame exchange are one of the key elements of this usage scenario
- The public safety scenario foresees establishment of ad-hoc wireless communication networks for emergency respond in disaster areas. Fire engines may operate as a platform for the WMN infrastructure. Support for mobile video cameras, *Voice over IP (VoIP)*, positioning plans, body monitoring of firefighters and their localization are key elements in the public safety scenario. As no infrastructure may be available, the WMN shall autonomously operate. Mobile battery operated devices may enlarge the coverage area of fire units and help to interconnect firefighters inside a disaster area.
- *Consumer Electronic (CE)* application scenarios foresee cheap devices that can be seamlessly integrated into a network of existing multimedia devices. On order to keep cost low, each device should only comprise a single transceiver. The WMN in the home environment delivers *Quality of Service (QoS)* sensitive audio/video streams and provides access to the Internet. Instead of expensive wired installation the WMN provides plug-and-play. Auto-configuration and ad-hoc deployment are important elements to support.
- Public access/provider networks can be cheaply deployed with WMN technology. Ease of outdoor and indoor installation is an important for provider operated WMNs. Especially in outdoor scenarios, connection to the fixed backbone is not available in all desired areas and long range fiber optics may be too expensive. Therefore, WMNs can develop new markets and hotspot areas where no service could be provided before.
- Office and enterprise networks benefit from flexibility provided by WMNs. Constant changes in companies require changes to the network as well. With WMN topologies can be easily changed and access to the company network may be provided anywhere in the office. For the WMN in the enterprise scenario, security is a key element.

Mobile WMNs operate in highly changing environment. Thus, complexity increases. Furthermore, network management becomes complicated and more frequent topology updates increase overhead. After having motivated the usage of WMNs we focus in the following on static WMN deployment.

B. Mandatory functionality

As previously discussed, *Wireless Mesh Networks (WMNs)* operate different than wireless single hop networks. To cope with the harsh environment encountered, WMNs need additional functionality. Thus, all current development in standardization bodies considers auxiliary functions or amendments of:

- *Medium Access Control (MAC)*,
- Path selection and,
- Security.

1) MAC design considering emerging effects: In contrast to single-hop networks, *Wireless Mesh Networks (WMNs)* introduce new problems that emerge from frames being relayed across multiple hops. A WMN can be treated as sum of continuously overlapping neighboring networks. In single-hop wireless networks all devices in the network are either in mutual reception range or have a common intersection of their set of neighbor devices. In contrast in WMNs, devices are mutually unaware of each other. The hidden and exposed device problem becomes acute in WMN. Hence, channel

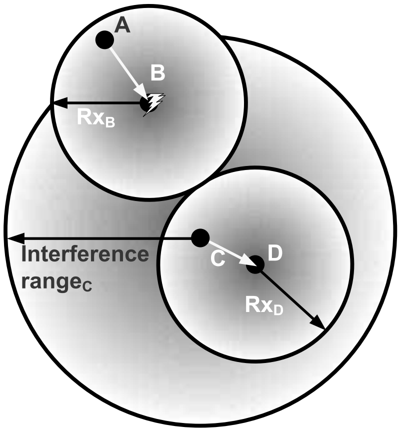


Fig. 4. Rx_B respectively Rx_D denotes the reception range of devices B and D. Device C cannot detect transmission from A to B. Thus it is unaware of B receiving data. C's transmission to D interferes at B. A's transmission fails.

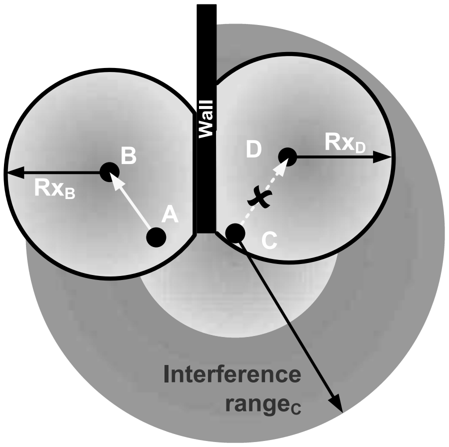


Fig. 5. Due to high attenuation of a wall, C cannot interfere at B. However, C senses A's transmissions. As C has no knowledge about the receiver B it refrains from channel access. Thus, C is an exposed device that cannot make use of spatial frequency reuse for transmission to D.

access coordination mechanism for WMNs needs to take those high potential source of interference into account.

a) Hidden device: A hidden device is classified as a device that is close to the receiver side of a frame exchange, but out of reception range of the transmitter. Here, the terms close and far are related to wireless signal propagation. There is no direct relationship to distance incorporated. Amendment IEEE802.11e [7] of the *Wireless Local Area Network (WLAN)* standard IEEE 802.11 defines:

> Hidden station: A station whose transmissions cannot be detected using *Carrier Sense (CS)* by a second station, but whose transmissions interfere with transmissions from the second station to a third station.

A frame transmission of a hidden device has high potential to interfere with other frame exchanges, see Fig. 4. Since C cannot sense the transmitter A, it cannot detect an ongoing transmission. However, the hidden device C is nearby to the receiving device B and thus can easily interfere with its frame reception. A common way to overcome the problem of hidden device is the exchange of short channel reservation frames prior to the data frame exchange as for instance the *Request To Send/Clear To Send (RTS/CTS)* handshake of IEEE 802.11. The reservation frame sent by the transmitter indicates the planned transmission duration of the data frames that shall follow. The receiving device responds by another reservation frame to the transmitter device. The latter reservation frame indicates the same transmission end. Other devices in the surroundings of either the transmitter, receiver or both need to overhear at least one of the previously exchanged reservation frames to learn about the upcoming frame exchange in their neighborhood. Then, they can refrain from channel access and avoid interference to those devices exchanging data frames. To learn the reservation information, a successful reception of at least one of the reservation frames is needed. Usually the reservation information is sent therefore at the most robust *Modulation and Coding Scheme (MCS)*. However, with large discrepancy between interference and reception range, the reservation frames may not secure a sufficiently large area: Collisions may still occur. The reservation frames are most likely not received by all devices which can harmfully interfere with the receiver. This issue is specifically serious when using high speed *Physical Layer (PHY)* technologies where reception range is only a minor fraction of interference range or when considering devices of high mobility.

According to specific deployment, environment and size of the *Wireless Mesh Network (WMN)*, a single device is in reception range of a minor fraction of all Mesh devices. It has only few direct, but many more indirect, hidden, neighbors. Those indirect neighbors are mutually not aware of each other. Only intermediate, relaying devices can help to inform the indirect neighborhood about the existence of such hidden devices.

b) Exposed device: A device is called exposed if by means of the applied protocol or current conditions on the *Wireless Medium (WM)*, the device decides that frame transmissions are not allowed. Hence, the device refrains from channel access, although simultaneous transmission to an ongoing transmission would be possible, see Fig. 5. As an exposed device is not harmful to other transmissions, most wireless standards do not take it into account therefore. However, in dense *Wireless Mesh Networks (WMNs)* with limited available bandwidth exposed devices can be a serious source of capacity waste. To overcome the performance limiting effect of exposed nodes, the *Medium Access Control (MAC)* protocol used within the WMN must not arbitrarily interchange the roles of receiving and transmitting device.

For protocols that use immediate acknowledgments after frames of arbitrary duration, the exposed device problem cannot be solved. As the transmitter is required to successfully receive an acknowledgment to its data transmission, no other concurrent transmission in the surroundings of the transmitting

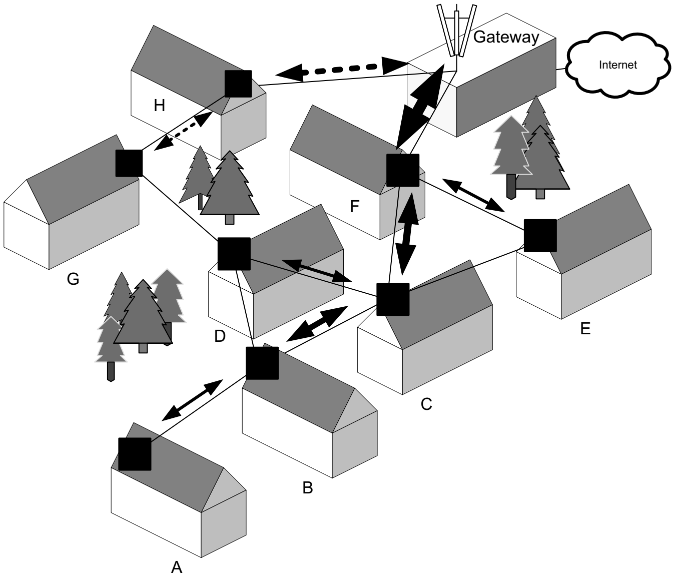


Fig. 6. Due to physical network topology, radio propagation environment, and path selection devices A, B, C, D and E decide to use device F as connector to the portal. Device H is also attached to the portal. However, it carries only G's traffic in addition to its own. The dotted lines indicates the less congested link. If the WMN design does not take traffic aggregation into account, severe disparity in experienced performance is consequence. Although ML (F-Gateway) carries much more traffic than (H-Gateway) both may have same access probability.

device is possible. As devices neighboring to the latter device cannot detect the end of the transmission if they concurrently transmit, either a cell based approach may be used where each frames has same length or information when the acknowledgment frame is expected must be provided to the device that intends to transmit concurrently. Depending on the specific network environment, the exposed device problem may be severe and limit the achievable performance of the network. Similar to *Central Processing Unit (CPU)* design, WMNs may benefit from simultaneous usage of orthogonal resources. Superscalar approaches as of example instruction pipelining and exploitation of parallelism in CPU design provides substantial speed-up in terms of instruction flow-rate. Whereas independent functional units concurrently work in a CPU, in WMNs the WM needs to be similarly referred to. Obstacles, walls, and buildings provide sufficient shadowing that enables simultaneous transmission in the same frequency band without interference. Detection and identification of such opportunities for simultaneous transmissions become important elements in the design of dense WMNs.

c) Congestion and Fairness Issues: In networking, fairness denotes a specific means of resource sharing. If several traffic flows equally share a link, total fairness may be achieved. Different characteristics of fairness may be distinguished. Standard IEEE 802.11 [1] provides fairness based on frames. No matter what size the payload has and which *Modulation and Coding Scheme (MCS)* is used for transmission, all frames have equal chance to get access to the *Wireless Medium (WM)*. With standard IEEE 802.11e [7], a paradigm shift is introduced. Here, fairness is based on the available capacity of the WM. Fairness among frames of equal priority is based on transmission duration. With each medium access, a device gains share of capacity called *Transmission Opportunity (TXOP)*. The TXOP allows for certain transmission duration only. Thus, devices that use different MCS achieve different throughput, although they may have equal share in terms of transmission duration.

In any case, with the number of flows being large and the capacity being small, none of the traffic flows may be able to fulfill its *Quality of Service (QoS)* requirements [8]. *Flow Admission Control (FAC)* helps to prevent endless sharing of link capacity. It preserves existing traffic flows and denies the access of additional ones to a network. Thus, it behaves unfair to newly arriving calls. A different approach is achieved by traffic prioritization. It helps to discriminate different traffic flows. Depending on the prioritization rules, high priority traffic may even starve lower ones. Thus, capacity is shared according to specific rules among flows of unequal priority. Both mechanisms, FAC and prioritization are needed in WMNs to guarantee optimal operation. Within WMNs, some links or devices become bottle necks, e.g., traffic must pass a portal device that has connection to both the Internet and the WMN. The overall traffic is aggregated at the portal device. The portal device saturates and determines the capacity of WMNs. Under the assumption of sufficiently fast connection to the Internet, a bottle neck portal device constantly receives or transmits frames. In its surroundings almost no capacity may be left over. Thus, other radio communication in its neighborhood may be affected too.

2) Path selection at MAC layer due to Cross-layer impacts: Wireless Mesh Networks (WMNs) based on multi-hop connections use routing mechanism to forward data from source to destination. Such routing protocols are developed by the *Mobile Ad-hoc Networks (MANET)* group in the *Internet Engineering Task Force (IETF)*. However, application of these protocols has limited performance. Since the *Internet Protocol (IP)* is unaware of radio conditions and neighboring devices, constant broadcasting limits performance. Furthermore, information such as *Packet Error Rate (PER)* or *Modulation and Coding Scheme (MCS)* used on a specific link is not available at the IP layer. Hence it operates blindly.

In contrast to IP based routing schemes, current research includes routing into the *Medium Access Control (MAC)* layer, thus enabling transparent WMNs that support any higher layer protocols. To distinguish from IP routing, in WMNs the term path selection is used. A connection between two Mesh devices is denoted as *Mesh Link (ML)*. A Mesh Path is a concatenated set of MLs. Path selection protocols calculate the best path between destination and source device. The selection process is distributed – Each Mesh devices independently calculates Mesh Paths. Path selection process can be influenced by ML properties:

- Hop count,
- ML link speed,
- ML congestion status,

- cost for transiting traffic and,
- delay

are examples for path metrics. To learn about neighboring devices and neighbors' neighbors, Mesh devices constantly exchange path selection information. The exchange of path selection metrics introduces overhead in contrast to *Wireless Relay Networks (WRNs)* where such topology information exchange is not needed due to the centralized structure.

C. Security

In information technology, security distinguishes three main aspects:

- Confidentiality,
- Integrity and
- Availability.

Confidentiality denotes that information is available to authorized entities only. A message is confidential if only the allowed entities can decode it. Integrity ensures that the communication messages are not modified. A network may be described as available if it is able to provide the desired service. With respect to *Wireless Mesh Networks (WMNs)* and their specific topology, new aspects unknown from single-hop networks emerge. Since independent devices use a common resource to mutually provide several services, different levels of trust may be observed. In WMNs, at least the following aspects additionally need to be considered:

- Authentication of Mesh devices
  - Full access with permission to forward frames
  - Partial access with permission to register with multiple neighboring devices
  - Association with a single Mesh device only
  - No access
- Participation in Mesh path selection
  - Generation and propagation of Mesh paths selection information
    - Paths to Mesh internal destinations
    - Paths to external networks
  - Reception of Mesh path selection information
- Detection and identification of rogue Mesh devices
- Exclusion and de-authentication of compromised Mesh devices
  - Propagation of according messages within the WMN

Depending on the required level of security, a WMN solution may address less or more of the aforementioned aspects. In many WMN implementations either a single authentication server is used or neighboring Mesh device mutually authenticate based on a shared secret. As many approaches for wireless Mesh networks operate in the *Medium Access Control (MAC)* layer, end-to-end security is usually considered as out of scope.

Authentication provides the secure exchange of encryption keys. The encryption keys ensure message integrity and confidentiality. Revocation of encryption keys becomes necessary if an attacker has corrupted one or more devices to gain access to the WMN. Detection of a rogue device is difficult. However, if message integrity cannot be guaranteed, not only unicast messages may be affected. Management frames that provide path selection information are usually sent as broadcast messages. With this information being corrupted, attackers may inject modified path selection messages that lead to false decisions. If all devices treat a specific device as their preferred next hop it may become a black hole. With an attacker being able to reset hop counts, frames may loop forever and the WMN becomes congested.

Constant availability of wireless networks is difficult to achieve. With interference, mobility, noise and fluctuation in channel path propagation, even operation of an undisturbed WMNs is a challenging task. WMNs operate in different bands like for instance the unlicensed *Industrial, Scientific, and Medical (ISM)* band at 2.4 GHz. It is used for several different applications; communication networks, analog audio- and video-bridges etc. Public *Wireless Local Area Network (WLAN)* and *Wireless Personal Area Network (WPAN)* networks operate as secondary users in the ISM band. They have to accept any interference. Depending on the cost-benefit analysis of an attacker powerful noise emission may be simple enough for a *Denial of Service (DoS)* attack. Hence, securing a WMN against DoS attacks depends on whether licensed or unlicensed spectrum is used.

Other issues such as multicast transmissions or operation of partly secured WMNs cannot be handled here due to limited space.

IV. Mesh technology in IEEE 802

Currently, three *Working Groups (WGs)* of the *Institute of Electronics and Electrical Engineering (IEEE)* project 802 (*LAN/MAN Standards Committee (LMSC)*) work on *Wireless Mesh Networks (WMNs)*:

- WG 802.11 defines the *Wireless Local Area Network (WLAN)* standard. At present IEEE 802.11 has largest amount of members of all IEEE 802 WGs. *Task Group (TG)* "S" develops amendment for *Extended Service Set (ESS)* Mesh Networking [9].
- WG 802.15 works on low and high rate *Wireless Personal Area Networks (WPANs)*. IEEE 802.15 has the second largest amount of members. IEEE 802.15.5 develops a recommended practice for Mesh WPANs.
- WG 802.16 is the *Broadband Wireless Access (BWA)* WG that develops standards for *Wireless Metropolitan Area Network (WMAN)*. The current standard [3], [4] foresees Mesh topology. However, no systems are currently available. In addition, IEEE-SA Standards Board approved project IEEE 802.16j in March 2006. Its task is the definition of a *Mobile Multihop Relay (MMR)*.

Although IEEE 802.16 defines Mesh topology already in its baseline standard, it is not well described and thus currently unused. IEEE 802.16j works on *Wireless Relay Network (WRN)* solution that enables customer devices to operate as relays for the operator. Nomadic, fixed and mobile relays are considered. Those relays operate under guidance of the provider controlled *Base Station (BS)* in licensed spectrum.

Thus, IEEE 802.16j does not define solution or extension of the baseline document for WMNs.

As active participants in the IEEE standardization process, the authors are involved in the design of IEEE 802.11s and IEEE 802.15.5. Additionally, the authors are intensively involved in the development of relay-based 4th generation cellular multi-hop networks. Currently, IEEE 802.15.5 focuses on high rate WPAN solution. In its present stage, the TG tries to overcome the legacies of the IEEE 802.15.3 centralized *Medium Access Control (MAC)* that hardly supports Mesh networking. As IEEE 802.11 is the oldest of the aforementioned WGs, its amendment for WMN is most mature. Therefore, we focus on IEEE 802.11s and give insight and details in section V. In section VI we provide simulation results that allow assumption of the performance of IEEE 802.11s. Details on broadband multi-hop networks are not discussed here but can for instance be found in [10]–[12].

V. Mesh WLAN – IEEE 802.11s

In 2003 the *Standing Committee (SC) Wireless Next Generation (WNG)* of IEEE 802.11 received presentations regarding Mesh *Wireless Local Area Network (WLAN)*. On behalf of the proposers, SC WNG requested from IEEE 802.11 *Working Group (WG)* formation of a *Study Group (SG)*. In January 2004 the Mesh SG held its first session. Its main task was definition of the *Project Authorization Request (PAR)* and 5 Criteria (5C) that are needed to request formation of a new *Task Group (TG)*. From July on, SG "*Extended Service Set (ESS)* Mesh Networking" became TG "S".

A. Terms and definitions

Each *Access Point (AP)* and its associated stations form a *Basic Service Set (BSS)*. In its basic form, *Task Group (TG)* "S" defines the Mesh *Wireless Local Area Network (WLAN)* as a network of interconnected APs [9]. The Mesh WLAN spans among the BSSs. As defined in *Institute of Electronics and Electrical Engineering (IEEE)* 802.11, several interconnected BSSs may form an *Extended Service Set (ESS)*. An ESS has a single unique *Service Set Identifier (SSID)*. In contrast to the *Basic Service Set Identification (BSSID)*, which equals the *Medium Access Control (MAC)* address of the AP, the SSID is maintained by the network operator. To interconnect several BSS, IEEE 802.11 uses the *Distribution Service (DS)*. IEEE 802.11s provides one means of a DS. As presented in [13], the term *Wireless Distribution System (WDS)* is misleading and should not be referred to in regard to Mesh WLAN. As APs are not the only devices that may be part of a Mesh WLAN, TG "S" has a well defined set of terms and definitions. As requested by the *Project Authorization Request (PAR)*, TG "S" does not mandate changes to IEEE 802.11 stations. The Mesh WLAN is formed among APs only. An AP that forwards frames is called *Mesh Access Point (MAP)*. If the access functionality is missing, it works as forwarder only. Such entity is called *Mesh Point (MP)*. Hence, all MAPs are MPs. However, not all MPs are MAPs. A *Mesh Portal (MPP)* is an entity corresponding to a standard portal. Mesh uni- and broadcast frames are *MAC Service Data Units (MSDUs)* delivered within the Mesh WLAN. Between neighboring MPs, a *Mesh Link (ML)* is used for communication. A concatenated set of ML from a source MP to a destination MP forms a Mesh Path. Each intermediate MP on a Mesh Path operates as immediate receiver or immediate transmitter. It uses the according address fields of the four address scheme of IEEE 802.11 frames.

B. Baseline document

During the standardization process, 35 proposal intents have been received by *Task Group (TG)* "S". In July 2005, 15 proposals were presented. After rounds of elimination in September in November, the two remaining proposals from *Wi-Mesh Alliance (WiMA)* and SEE-Mesh merged. The joint proposal became baseline document during *Institute of Electronics and Electrical Engineering (IEEE)* plenary meeting in March 2006. The mandatory set of functions includes requirements for security, path selection and *Medium Access Control (MAC)*. The mandatory MAC is based on IEEE 802.11e and uses the *Enhanced Distributed Channel Access (EDCA)* for arbitration of channel access. In its simplest form, a single frequency channel Mesh *Wireless Local Area Network (WLAN)* operates as overlay to existing *Basic Service Sets (BSSs)*. The *Mesh Access Points (MAPs)* and the stations associated with the APs compete on the wireless channel. Competition among stations and their BSS serving MAP has several implications. *non-QoS Station (nQSTA)* support the *Distributed Coordination Function (DCF)* only. DCF does not support prioritization. Unlike *QoS Station (QSTA)* that support EDCA, nQSTA have fixed backoff parameters that cannot be controlled by a *QoS Access Point (QAP)*. Under the assumption of support for the IEEE 802.11e *Quality of Service (QoS)* mechanisms by the MAP it operates as QAP too. However, with several nQSTAs in the BSS the *Mesh QoS Access Point (MQAP)* competes with all of them on accessing the *Wireless Medium (WM)*. As no priority is granted by the nQSTA to the MQAP, the downlink traffic in the BSS is affected. Furthermore, the Mesh WLAN traffic cannot be segregated. Depending on the overall *Extended Service Set (ESS)* topology, this may have severe impact on the performance. The bottleneck MQAP might be hindered to handle the Mesh WLAN backhaul traffic accordingly. To grant priority to the MQAP, it needs to implement the *Hybrid Coordinator (HC)* functionality too. Only the HC uses the *HCF Controlled Channel Access (HCCA)* that gives full control over the WM. Hence the HC-MQAP may set-up traffic streams with its QSTA and can increase its share of capacity of the WM as no backoff is used when performing the HCCA. The HC-MQAP controls its BSS in total. The absence of backoff when performing HCCA has severe impact on neighboring BSS. As other, potential *Quality of Service Basic Service Set (QBSS)* may have their own HC too, constant collisions cannot be prevented. As all neighboring HCs access the WM after it has been identified as idle for a *Point (Coordination Function) Interframe Space (PIFS)* interval, their frames collide [14]. Mutual interference

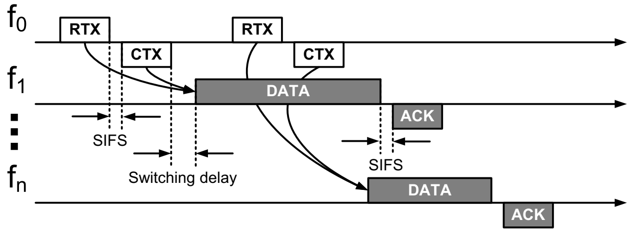


Fig. 7. CCF provides solution for multi-frequency Mesh WLAN. Devices tune their radio during CCW to a common frequency channel. On this channel devices negotiate on channel for data frame exchange. RTX and CTX messages indicate frequency switch. Here, devices A and B negotiate to switch to frequency channel f_0. While they exchange frames, other devices may use different, orthogonal frequency channels.

of simultaneous transmissions severely impacts the BSS and the ESS respectively Mesh WLAN in total. In single frequency Mesh WLAN that need to rely on single transceivers in each MAP, HCCA cannot be applied therefore.

C. Common Channel Framework (CCF)

The *Common Channel Framework (CCF)* approach foresees exchange of *Request to Switch (RTX)* and *Clear to Switch (CTX)* control frames. *Mesh Points (MPs)* use the RTX/CTX handshake to negotiate on frequency channels for data frame transmission. As different frequency channel operate orthogonally, MPs with single transceiver cannot communicate if they are tuned to different channels. A *Channel Coordination Window (CCW)* defines a shared resource to which all MPs simultaneously tune their radio at given times. MPs repetitively tune to the common channel, where they negotiate on the channel usage, see Fig. 7. To allow all MPs to make use of the CCW, synchronization among them is needed. The joint baseline document has optional sections that explain how to synchronize a Mesh *Wireless Local Area Network (WLAN)*. MPs that have negotiated on a channel for their data frame exchange tune their radio to the new channel and sense the channel. If the *Wireless Medium (WM)* is detected as idle for a *Distributed Coordination Function Interframe Space (DIFS)* interval, frames can be exchanged. Although availability of the channel the MPs have agreed on cannot be guaranteed, channel access has high probability as other MPs do not use the channel due to the sequential nature of RTX/CTX handshake in the common channel. Unlike *Request To Send (RTS)*/*Clear To Send (CTS)* handshake that enables immediate reservation of the frequency channel; RTX/CTX handshake enables reservation in frequency domain.

D. Mesh Deterministic Access

As second *Medium Access Control (MAC)* amendment, the *Mesh Deterministic Access (MDA)* works as distributed *Wireless Medium (WM)* reservation mechanism. Inspired by the *Distributed Reservation Channel Access (DRCA)* as defined in *Mesh Coordination Function (MCF)* of *Wi-Mesh Alliance (WiMA)*, the joint baseline document offers an optional reservation based channel access mechanism that enables prediction of the channel usage. Using Information Elements (IEs) in management frames such as beacons for example, MPs negotiate with their neighbors on MDA *Transmission Opportunity (TXOP)*. An MDA TXOP is called *MDA Opportunity (MDAOP)*. An MDAOP has predefined duration and start time. At the beginning of an MDAOP, the owner has the right to access the WM using higher priority. A different set of *Enhanced Distributed Channel Access (EDCA)* parameters (*Arbitration IFS Number (AIFSN)*, CWmin, CWmax etc.) shall be used by the *Mesh Point (MP)* that holds the MDAOP. As the reservation is not a strict one, other stations may have grabbed the channel earlier. The MDAOP holder then defers until other transmissions end and its local *Carrier Sense (CS)* indicates an idle channel. Using the MDA access parameters it competes on the channel then. As with *Common Channel Framework (CCF)*, to use MDA the MPs involved in the MDAOP need to be synchronized. To further enhance the probability of successful frame reception during MDA reservations, the MDAOP information is broadcasted in beacons frames and repeated by neighboring MPs. Thus, the direct and indirect neighborhood is informed about future transmissions. The announcement of planned frame exchanges allows dealing with hidden MPs and can lower the interference. Hence, all MDA supporting MPs store information on direct and indirect MDAOP internally. This information is used by neighboring MPs that are not involved in the MDAOP to refrain from channel access as they preset their local *Network Allocation Vector (NAV)* at the beginning of a neighboring MDAOP. This provides priority to the MDAOP owner and lower collision probability, thus granting higher priority to the MDAOP owner. In contrast to CCF, MDA enables reservation in the time domain. However, spatial frequency reuse better than current IEEE 802.11 cannot be reached, because still both - receiver and transmitter - of an MDAOP emit power in form of data and *Acknowledgment (ACK)* frames onto the WM. As the role of being in transmit or receive mode is interchanged (the transmitter sends data frames that are received by the receiver and the receiver sends ACK frames back to the transmitter after each successfully received data frame), interference prediction cannot be performed due to arbitrary data frame lengths. Fragmentation, block acknowledgments and frame aggregation may be arbitrarily used by the transmitter. The receiver replies relative to the end of a frame transmission after a specific duration. Hence, it is not predictable when the transmitter expects feedback from the receiver. Therefore, no other MP, which may be outside of interference rang to the transmitter, can reuse the frequency channel concurrently, as the transmitter may be in receiving mode itself at any time. However, MDA offers predictable channel usage that enables support for *Quality of Service (QoS)* in a distributed manner. Furthermore, the coordination of planned transmissions in the future allows for the usage of smart antennas that may beamform to the transmitter at the expected point in time. MDA offers other MPs the opportunity to collaborate and cooperate. Unlike competition based access with high probability of collisions, MDA inherently works as collision prevention mechanism. Since neighboring MPs mutually inform about their own, their neighbors and their neighbors' neighbors transmissions, mutual interference can be prevented and frame transmissions have higher success probability, thus enhancing overall spectrum usage. As MPs arrange their frame transmissions, arbitration period can be prevented. Such arbitration periods are limiting performance of Mesh networks as they cannot be reduced and are waste of capacity.

E. Path selection

The IEEE 802.11s baseline document describes the "Extensible Path Selection Framework". This framework defines a single mandatory path selection algorithm that must be implemented in any *Mesh Point (MP)*. Other path selection methods may be vendor specific. A Protocol Identifier determines the path selection method other than the default one. The operator of a network may set this value manually e. g. Path selection algorithm for *Wireless Mesh Networks (WMNs)* need additional metrics as input in contrast wired networks. The *Task Group (TG)* “S” baseline document describes

- Channel access overhead O_{ca} (depending on *Physical Layer (PHY)*),
- Protocol overhead O_p (depending on PHY),
- Number of bits B_t in a test frame (depending on PHY),
- PHY bit rate r and,
- Frame error rate e_{pt} for the test frame.

The Airtime Link Metric Function calculates the airtime cost c_a:

$$c_a = [O_{ca} + O_p + \frac{B_t}{r}] * \frac{1}{1 - e_{pt}}$$

Airtime cost is calculated per *Mesh Link (ML)*. It is used as input for the *Hybrid Wireless Mesh Protocol (HWMP)*, which is the mandatory path selection protocol. Consideration of other metrics is implementer specific. As the name indicates, HWMP combines on-demand and proactive protocol aspects. As optional path selection protocol, the baseline document describes *Radio Aware Optimized Link State Routing (RA-OLSR)*. Details on both can be found in [9].

F. Security

As mandated in the *Project Authorization Request (PAR)*, the baseline document reuses IEEE 802.11i for *Mesh Link (ML)* security. End-to-end security along a Mesh path consisting of several MLs is beyond the scope of the baseline document. Both centralized and distributed authentication and key management are supported. With a centralized *Authentication Server (AS)*, each *Mesh Point (MP)* and station authenticates with the AS. Without an AS, MPs use the distributed IEEE 802.1X authentication model, where MPs mutually authenticate. Therefore, MPs work as supplicant and authenticator. Details regarding the security concept can be found in [9].

VI. Simulation-based Analysis

We use event-driven stochastic simulations based on the IEEE 802.11a *Orthogonal Frequency Division Multiplexing (OFDM) Physical Layer (PHY)*. The simulations were performed using the *Wireless Access Radio Protocol 2 (WARP2)* simulation environment developed at the Chair of Communication Networks, Faculty 6, RWTH Aachen University [15]. It is programmed in *Specification and Description Language (SDL)* using Telelogics TAU SDL Suite. The channel model used in WARP2 to accurately simulate erroneous radio propagation on the *Wireless Medium (WM)* is presented in [16]. In accordance with *Institute of Electronics and Electrical Engineering (IEEE)* recommendations, throughout this paper all mathematical notations and unit descriptions are given according to [17].

Fig. 8 shows the simulation scenario. Six stations receive data from the Internet via a two and three hop path. Stations a, b and, c are associated with *Mesh Access Point (MAP)* A. Stations d, e and, f are associated with MAP D. MAP A has connection to the *Mesh Portal (MPP)* C via MAP B. MAP D has direct connection to MPP C. As worst case scenario, frame size is set to 80 B. The MAPs are separated by 25 m. They use QPSK¾ as *Modulation and Coding Scheme (MCS)*. Stations are close to their MAPs. Therefore 64-QAM¾ is used within in *Basic Service Set (BSS)*.

In the present stage, the mandatory *Medium Access Control (MAC)* functions of IEEE 802.11s are described by the *Enhanced Distributed Channel Access (EDCA)* as known from IEEE 802.11e [7]. As it does not provide means for spatial frequency reuse, the performance is limited. Furthermore, fairness between different multi-hop paths cannot be guaranteed. The simulation results in Fig. 9 show that stations a, b and, c achieve less throughput than stations d, e and, f. Due to a smaller hop count, the latter ones are in advantage.

Under the simplified assumption that only neighboring device interfere with each other, we can identify concurrent links. In the following, “||” denotes “concurrent to”. Thus, we have: (C-B) || (D-{d|e|f}) and (C-D) || (B-A). However, (A-{a|b|c}) cannot operate simultaneously to any other link.

Hence, an optimum transmission sequence could be {(C-B) || (D-d), (C-D) || (B-A), (A-a), (C-B) || (D-e), (C-D) || (B-A), (A-b), (C-D) || (D-f), (A-c)}. Each step in the sequence is limited by the slowest transmission. Links (C-B), (C-D) and (B-A) use QPSK¾, while the other use 64-QAM¾. Thus at the end of the sequence six stations have each received 80 B. Under the assumption of No-*Acknowledgment (ACK)* policy, each data frame is separated by a *Short Interframe Space (SIFS)* period. According to [18] we calculate (1):

$$\begin{aligned}
& \text{Total System Throughput} \\
= \ & \frac{6 * 80\text{B}}{\text{Duration}(6 * 80\text{B@QPSK}{}^{1}\!/\!{}_{2} + 2 * 80\text{B@64QAM}{}^{3}\!/\!{}_{4})} \\
= \ & \frac{6 * 80\text{B}}{6 * (112\mu\text{s} + \text{SIFS}) + 2 * (56\mu\text{s} + \text{SIFS})} \\
= \ & \frac{6 * 80\text{B}}{6 * 128\mu\text{s} + 2 * 72\mu\text{s}} \\
= \ & 4.2{}^{Mb}\!/\!{}_{\text{s}} \qquad (1)
\end{aligned}$$

Under the assumption of ACK frames sent back by the receiving device, an additional SIFS provides time for transceiver turnaround. Thus the achievable throughput is (2):

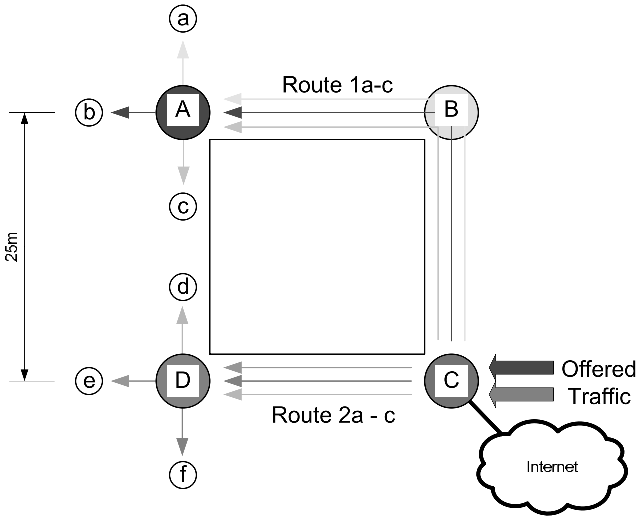


Fig. 8. MAP C has connection to the Internet. It provides access to MAPs B and D. Stations a, b and, c receive frames via MAP A. Stations d, e and f receive frames via MAP D. Besides attenuation due to path propagation, each wall attenuates the radio transmission by 6 dB. Transmission power is fixed to 100 mW. With regard to the IEEE 802.11a PHY, in our simulation we assume an attenuation factor $\gamma = 3.5$ for the 5 GHz frequency band.

$$
\begin{aligned}
&= \frac{6 * 80\text{B}}{912\mu\text{s} + 8 * (\text{SIFS} + \text{ACK@QPSK}{}^1\!/_2)} \\
&= \frac{6 * 80\text{B}}{912\mu\text{s} + 8 * (16\mu\text{s} + 32\mu\text{s})} \\
&= 3.0\,{}^{Mb}\!/_{\text{s}} \qquad (2)
\end{aligned}
$$

Fig. 10 provides an example for an optimum spatial reuse distance. Under the assumption of interference range being less than two times reception range, static frame sizes, equidistant placement of Mesh devices and constant transmission power, optimum spatial reuse distance in string topology can be defined. (1) and (2) assume such background for the scenario in Fig. 8. In comparison to the simulation results shown in Fig. 9 capacity of the WM can be much better exploited.

The low performance of IEEE 802.11 *Wireless Local Area Network (WLAN)* in multi-hop situation and shadowed areas is explained in Fig. 11. IEEE 802.11 MAC performs backoff with every transmission attempt. However, such medium access is unpredictable as distributed, decentralized scheme is performed. Thus, even in a full *Downlink (DL)* scenario with traffic generated by a single source only frames collide due to uncoordinated transmission attempts. Furthermore, Fig. 8 shows that IEEE 802.11 access scheme does not guarantee fairness. With increasing traffic offered per Mesh Path, the Mesh Paths with less hops dominate. Thus, route 2 with three hops starves. Each additional hop increases collision probability. Therefore, even in simple scenarios the IEEE 802.11 MAC operates with low efficiency in *Wireless Mesh Network (WMN)* topology. Compared to [19]–[21] the achievable system capacity is far from optimum.

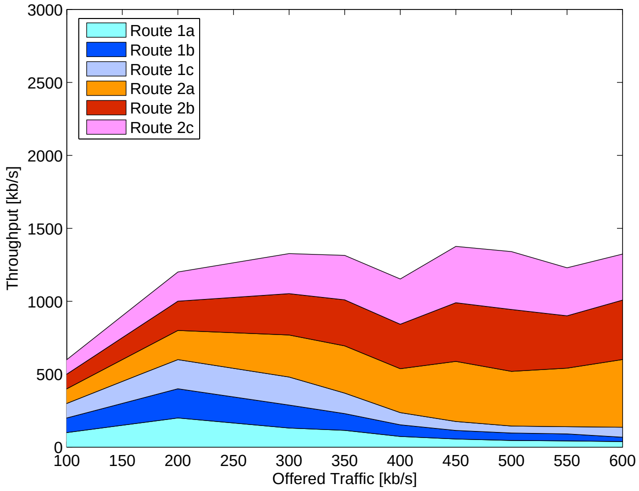


Fig. 9. The figure shows cumulative end-to-end throughput vs. offered traffic per route. Links between MAPs use QPSK¾. Connections to the stations run at 64-QAM¾.

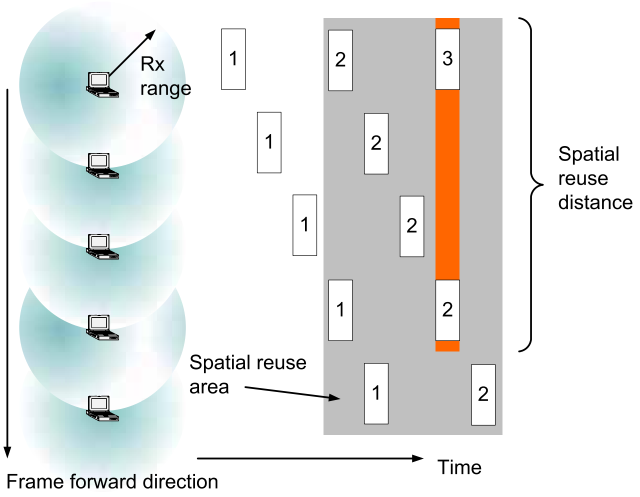


Fig. 10. In the optimum case of the interference range being less than two times reception range, static frame sizes, equidistant placement of Mesh devices and constant transmission power, the spatial reuse distance in a string topology can be defined. Here, the WM can be reused at a distance of three hops.

VII. Conclusions and Outlook

Wireless Mesh Networks (WMNs) are important elements to provide ubiquitous wireless access. Due to high deployment costs of the wired backbone, WMNs offer solution to cover areas that are unprofitable currently. With increasing amount of users that require wireless high speed data services, any new wireless technology will incorporate support for *Wireless Relay Network (WRN)* or WMN based deployment. Due to limited spectrum and densely deployed devices, efficient medium access schemes are needed.

Recent research [22]–[24] presents new methods that increase efficiency in WMNs and allow to exploit the available capacity of the *Wireless Medium (WM)*. Our future work will concentrate on decentralized medium access schemes that

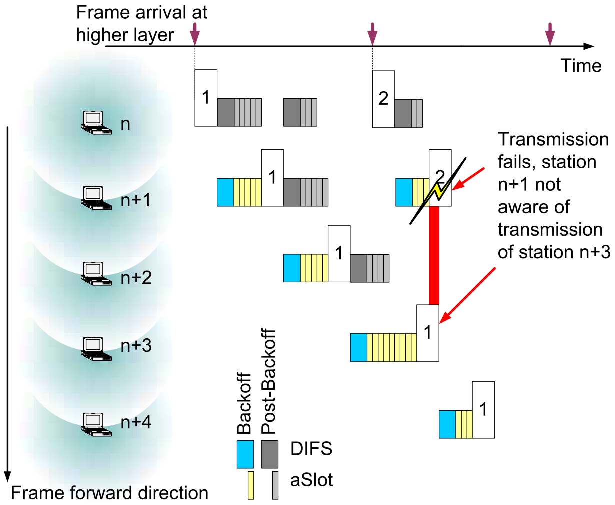

Frame arrival at higher layer
Time
1
2
n
n+1
n+2
n+3
n+4
1
2
1
1
1
Transmission fails, station n+1 not aware of transmission of station n+3
Backoff
Post-Backoff
DIFS
aSlot
Frame forward direction

Fig. 11. IEEE 802.11 WLAN devices use a distributed, decentralized medium access scheme. Between consecutive frames, each device performs backoff regardless if it has frames to transmit or not, see [1]. The backoff has a part that has constant and has a part that has random duration with each transmission attempt. However, such unpredictable medium access prevents prediction of idle WM periods. Hence, with the current IEEE 802.11 access scheme only minor fraction of the capacity of WMNs can be exploited.

enable concurrent transmissions. Furthermore, we will investigate the current IEEE 802.11s proposal and compare *Mesh Deterministic Access (MDA)* and *Common Channel Framework (CCF)* with different *Medium Access Control (MAC)* schemes. More complex scenarios with increased amount of hops per Mesh Path and changing mix of *Uplink (UL)* and *Downlink (DL)* traffic will provide realistic scenarios.

Acknowledgment

The authors would like to thank Prof. Dr.-Ing. B. Walke for his support and friendly advice to this work.

References

[1] *Information Technology - Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications*, IEEE Reaffirmed 12 June 2003 ANSI/IEEE Std 802.11, 1999 Edition (R2003), Oct. 2003.

[2] *IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 15.3: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for High Rate Wireless Personal Area Networks (WPANs)*, IEEE IEEE Std. IEEE Std 802.15.3-2003, Sept. 2003.

[3] *IEEE Standard for Local and metropolitan area networks - Part 16: Air Interface for Fixed Broadband Wireless Access Systems*, IEEE Revision of 802.16-2001 IEEE Std 802.16-2004, Oct. 2004.

[4] *IEEE Standard for Local and metropolitan area networks - Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1*, IEEE Amendment and Corrigendum to IEEE Std 802.16-2004 IEEE Std 802.16e-2005 and IEEE Std 802.16-2004/Cor1-2005, Feb. 2006.

[5] R. Pabst, B. Walke, D. C. Schultz, P. Herhold, H. Yanikomeroglu, S. Mukherjee, H. Viswanathan, M. Lott, W. Zirwas, M. Dohler, H. Aghvami, D. D. Falconer, and G. P. Fettweis, “Relay-based deployment concepts for wireless and mobile broadband radio,” *IEEE Communications Magazine*, pp. 80–89, Sept. 2004.

[6] H. Wijaya, “Interoperability concept for wireless lans,” in *Proceedings of IEEE VTC Fall 2004*, Los Angeles, USA, Sept. 2004, p. 95.

[7] *IEEE Standard for Information Technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 8: Medium Access Control (MAC) Quality of Service (QoS) Enhancements*, IEEE Amendment to IEEE Std 802.11, 1999 Edition (Reaff 2003) IEEE Std 802.11e-2005, Nov. 2005.

[8] S. Mangold, S. Choi, G. R. Hiertz, O. Klein, and B. Walke, “Analysis of IEEE 802.11e for QoS Support in Wireless LANs,” *IEEE Wireless Communications*, vol. 10, no. 6, pp. 2–12, Dec. 2003.

[9] *Draft Amendment to Standard for Information Technology - Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Amendment: ESS Mesh Networking*, IEEE Unapproved draft IEEE P802.11s/D0.02, June 2006.

[10] N. Esseling, B. Walke, and R. Pabst, “Performance evaluation of a fixed relay concept for next generation wireless systems,” in *Proceedings of PIMRC 2004*, Barcelona, Spain, Sept. 2004, p. 9.

[11] R. Pabst, N. Esseling, and B. Walke, “Fixed relays for next generation wireless systems - system concept and performance evaluation,” *Journal of Communications and Networks, Special Issue on "Towards the Next Generation Mobile Communications"*, vol. 7, no. 2, pp. 104–114, June 2005.

[12] B. Walke, H. Wijaya, and D. C. Schultz, “Layer-2 relays in cellular mobile radio networks,” in *Proceedings of IEEE 63rd Vehicular Technology Conference, VTC2006-Spring*, Melbourne, Australia, May 2006, p. 5.

[13] D. Engwer, “"WDS" Clarifications,” IEEE, Submission 802.11-05/0710r0, July 2005.

[14] S. Mangold, S. Choi, P. May, O. Klein, G. R. Hiertz, and L. Stibor, “IEEE 802.11e Wireless LAN for Quality of Service (invited paper),” in *Proceedings of the European Wireless*, vol. 1, Florence, Italy, Feb. 2002, pp. 32–39.

[15] Chair of Communication Networks, RWTH Aachen University, Kopernikusstraße 16, 52074 Aachen, Federal Republic of Germany. [Online]. Available: http://www.comnets.rwth-aachen.de

[16] S. Mangold, S. Choi, and N. Esseling, “An Error Model for Radio Transmissions of Wireless LANs at 5GHz,” in *Proc. Aachen Symposium 2001*, Aachen, Sept. 2001.

[17] I. Periodicals Transactions/Journals Department. (2003, Jan.) IEEE Transactions, Journals, and Letters - Information for Authors. auinfo03.pdf. IEEE. 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331, USA. [Online]. Available: http://www.ieee.org/portal/cms_docs/pubs/transactions/auinfo03.pdf

[18] G. R. Hiertz, L. Stibor, J. Habetha, E. Weiss, and S. Mangold, “Throughput and Delay Performance of IEEE 802.11e Wireless LAN with Block Acknowledgments,” in *Proceedings of 11th European Wireless Conference 2005*, vol. 1. Nicosia, Cyprus: Microsoft Innovation Center Europe & ATHK CYTA, Apr. 2005, pp. 246–252.

[19] P. Gupta and P. R. Kumar, “The Capacity of Wireless Networks,” *IEEE TRANSACTIONS ON INFORMATION THEORY*, vol. 46, no. 2, Mar. 2000.

[20] L. Fu, Z. Cao, and P. Fan, “Spatial reuse in IEEE 802.16 based wireless mesh networks,” in *Communications and Information Technology, 2005. ISCIT 2005. IEEE International Symposium on*, vol. 2, 2005, pp. 1358–1361.

[21] S. Toumpis and A. Goldsmith, “Capacity regions for wireless ad hoc networks,” *IEEE Transactions on Wireless Communications*, vol. 2, no. 4, pp. 736–748, 2003.

[22] C. Seo, E. Leonardo, P. Cardieri, M. Yacoub, D. Gallego, and A. de Medeiros, “Performance of IEEE 802.11 in wireless mesh networks,” in *Microwave and Optoelectronics, 2005 SBMO/IEEE MTT-S International Conference on*, 2005, pp. 363–367.

[23] J. Tao, F. Liu, Z. Zeng, and Z. Lin, “Throughput enhancement in Wimax mesh networks using concurrent transmission,” in *Wireless Communications, Networking and Mobile Computing, 2005. Proceedings. 2005 International Conference on*, vol. 2, 2005, pp. 871–874.

[24] J. Zhu, X. Guo, L. Yang, and W. Conner, “Leveraging spatial reuse in 802.11 mesh networks with enhanced physical carrier sensing,” in *Communications, 2004 IEEE International Conference on*, vol. 7, 2004, pp. 4004–4011.