Wireless Mesh Networks in the IEEE LMSC

Guido R. Hiertz[*], Sebastian Max[*], Thomas Junge[*], Lars Berlemann[*],
Dee Denteneer[†], Stefan Mangold[‡], Bernhard Walke[*]
[*]Chair of Communication Networks, Faculty 6, RWTH Aachen University, Aachen, Germany
[†]Philips, Eindhoven, The Netherlands
[‡]Swisscom Innovations, Bern, Switzerland

***Abstract*— On March 13th 1980, the Computer Society of the *Institute of Electronics and Electrical Engineering (IEEE)* approved project 802. IEEE 802 is led by the *LAN/MAN Standards Committee (LMSC)*. Until today, 22 *Working Groups (WGs)* mainly define standards for the lowest two layers of the ISO/OSI reference model in the 802. For wireless communication, 802.11 WG defines the *Wireless Local Area Network (WLAN)*, 802.15 WG defines the *Wireless Personal Area Network (WPAN)*, and 802.16 WG defines the *Wireless Metropolitan Area Network (WMAN)* standard. With *Multiple Input/Multiple Output (MIMO)*, *Ultrawideband (UWB)* and sensitive *Modulation and Coding Schemes (MCSs)*, latest developments in the 802 enable data rates beyond 500 Mb/s for new applications of wireless communication. Similar to preceding wireless technologies, data rate slows down by increase in distance of the communication entities. However, demands for new applications emerge that need high data rates regardless of distance. To overcome the link speed limitation, dense deployment of wireless networks is needed. *Wireless Mesh Networks (WMNs)* help to overcome current dependencies of wireless communication systems on wired backbones. Thus, they enable cheap deployment and rapid roll-out for a new generation of wireless services. As active participants of 802 meetings, the authors are deeply involved in standardization since 2003. In this paper we provide insight to current standardization activities of the LMSC on WMNs.**

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

I. Introduction

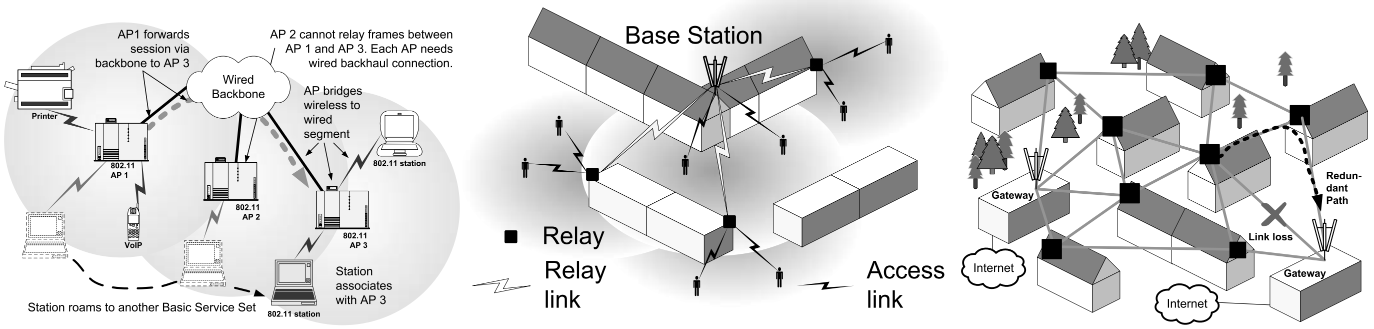
All current wireless standards in the IEEE *LAN/MAN Standards Committee (LMSC)* use physical and/or logical star topologies [1]. 802.11 *Wireless Local Area Networks (WLANs)* use an *Access Point (AP)* that forms a local *Basic Service Set (BSS)*. The 802.15.3 *Wireless Personal Area Network (WPAN) Medium Access Control (MAC)* defines a centralized scheme. A *Piconet Controller (PNC)* controls the *Wireless Medium (WM)*. *Wireless Metropolitan Area Networks (WMANs)* based on 802.16 rely on central *Base Stations (BSs)* that schedule access to the WM. For the support of handover, roaming, frame forwarding, interconnection of wireless entities and many more, central entities need to be interconnected. Furthermore, the interconnection of the central entities provides access to other networks and forms a broadband backbone. Currently, this backbone is based on wired technology, e. g. the central entity operates as a bridge to an Ethernet (802.3) segment. The density of central wireless entity deployment essentially influences the provided data rate. The higher the data rate that shall be supported, the higher *Signal to Interference plus Noise Ratio (SINR)* is needed. Since SINR sharply decreases with increasing distances, central entities need to be densly deployed to sustain a sufficient SINR over the area that shall be covered. Therefore, with tight deployment of central wireless entities, the wired networks must be widely available too. However, wired infrastructure is expansive to deploy. To overcome this cost barrier, central entities have to interconnect wirelessly: *Wireless Mesh Networks (WMNs)* provide the solution.

A. Wireless Mesh Networks - Evolution of Wireless Networks

Current wireless communication systems form isolated, stand-alone networks, see Fig. 1(a). Each AP, PNC or BS serves its associated entities only. The wireless link is used for transmission between the central entity and its associated clients. The wired backbone provides any other service. Thus, an important aspect of the central entity is bridging between the wireless and the wired network. Unlike the wired Internet, wireless networks have not connected yet. *Wireless Relay Networks (WRNs)* are the first step towards a wireless Internet. In a WRN, relay entities behave as proxy of the central entity, see Fig. 1(b). They help to increase the range of the central entity. As intermediate entities, they forward frames and operate on behalf of the central entity. With increased capability of the relaying entity, a WMN can be formed. In a WMN, each entity operates independently of its neighbors. Comparable to the wired Internet, the WMN consists of wireless routers. Path selection methods help to find the next suitable hop, see Fig. 1(c). Well known algorithms identify the optimal path. However in WMNs, the term optimum is related to more than hop count only. Spontaneous ad-hoc WMNs may be decentralized, can operate autonomously and can be easily deployed. The capability to forward frames and to overcome range limitations enables new services unknown from traditional wireless networks. Due to the complexity involved, new issues emerge too.

B. Challenges in Wireless Mesh Networks

The radio spectrum is a shared medium. Depending on the SINR at the receiver side, no other transmission may occur concurrently in the neiborhood of a transmitting entity. While in traditional single-hop wireless networks at least the central AP, PNC or BS is a common element that forms the intersection of the neighborhood sets of all entities, such common element does not exist in WMNs. In WMNs, each entity has a different set of neighboring entities. Therefore,


AP1 forwards session via backbone to AP 3
AP 2 cannot relay frames between AP 1 and AP 3. Each AP needs wired backhaul connection.
Wired Backbone
AP bridges wireless to wired segment
Printer
802.11 AP 1
802.11 AP 2
802.11 AP 3
802.11 station
VoIP
Station associates with AP 3
Station roams to another Basic Service Set
802.11 station
Base Station
Relay
Relay link
Access link
Gateway
Redun- dant Path
Link loss
Internet
Internet
Gateway

(a) Single hop WLAN (b) Wireless Relay Network (c) Wireless Mesh Network

Fig. 1. (a): The wired backbone interconnects different APs. Each AP operates as bridge between the wired and the wireless broadcast domain. Roaming and session forwarding services are provided with the help of the wired network. (b): In WRNs, relaying entities operate slave to a central master. It has full control over the WM. (c): A WMN is fully decentralized. Each entity operates as wireless router that forwards frames based on local path selection decisions.

the hidden and exposed entity problems are more severe. In many cases, the set of neighbors' neighbors consists of more elements than the set of neighbors. Since the interference range exceeds the reception range, precaution in the set of neighbors' neighbors against mutual interference must be taken. To allow for sufficient performance, the MAC layer must be specifically adopted for operation in WMNs topology, see [2], [3].

Current wireless networks form a single-hop topology. The central entity operates as bridge to other networks and is the gateway for any non-local traffic. Thus, the current 802 wireless standards form single logical broadcast segments. WMNs extend the range of the broadcast segment. Although frames may be relayed over multiple hops, the WMN shall transparently operate to higher layers. As *Address Resolution Protocol (ARP)*, *Dynamic Host Configuration Protocol (DHCP)*, *Internet Protocol (IP)* and other protocols shall seamlessly work in WMNs, an efficient support for broad- and multicast traffic is needed, see Fig. 2.

To comply with transparent operation of the WMN, all path selection decisions need to be hidden from higher layers. With multiple hops in WMNs, demand for tight coupling of path selection with the MAC emerges. For each local link, information about *Modulation and Coding Scheme (MCS)*, transmission power, noise level, interference situation, congestion status and many more characteristics is available in the MAC layer. In contrast to IP based Mesh routing defined by [4], WMNs can use the MAC layer information as additional metrices in the path selection decision. Thus, a best Mesh path does not necessarily consist of the concatenation of the *Mesh Links (MLs)* with highest link speed.

Security is another aspect, affected by WMNs. In WRNs, customer owned entities may become an active part of the wireless networks. The entities operate as relays that forward frames to and from other customers. Besides privacy related issues, integrity of *Authentication, Authorization and Accounting (AAA)* services can be threatened too. Since wireless routers operate idependently, path selection information needs to be secured to avoid malicious attacks in WMNs. Furthermore, end-to-end security may be requested even when untrusted entities form a joint WMN.

C. Outline

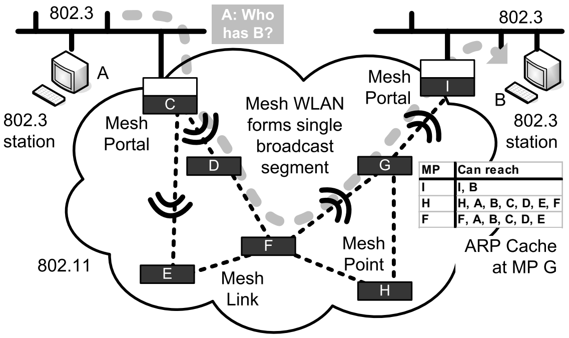
In section II we give an overview of the current 802 *Working Groups (WGs)* that develop standards for WRNs or WMNs. Section III introduces enhancements to the specific MAC layers of each WG. Path selection in WMNs is presented in section IV. An overview to security risks is given in section V. Section VI concludes our paper.

II. IEEE 802 WGs DEFINING WMNs

The initial 802.16 standard was released in 2001. Its revision in 2004 [5] is the first 802 standard that introduces a Mesh topology. Since 2006, 802.16 works on an amendment for *Wireless Relay Networks (WRNs)*. In 2004, interests in *Wireless Mesh Networks (WMNs)* led to establishment of new *Task Groups (TGs)* in 802.11 and 802.15.

A. 802.11s

Prior to the formation of the TG, 802.11 started the "*Extended Service Set (ESS)* Mesh networking" *Study Group (SG)* in 2003. The SG developed the *Project Authorization Request (PAR)* and *Five Criteria (5C)* documents that describe the scope of 802.11 TG "s". The current Mesh *Wireless Local Area Network (WLAN)* draft [6] defines a transparent ESS that operates as a *Distribution Service (DS)* for the *Access Points (APs)*. A *Mesh Point (MP)* is an entity that is able to forward frames and participates in the formation of the Mesh WLAN. An MP that furthermore provides the association service is dentoed as *Mesh Access Point (MAP)*. Stations associate with MAPs and use all services known from existing WLAN. The Mesh WLAN operates transparently. It behaves not different than today's Ethernet backbones that are most often used to interconnect APs. In contrast, Lightweight MPs do not provide any service. They operate as Mesh stations that benefit from participation in the Mesh WLAN but have no forwarding capability.



MP	Can reach
I	I, B
H	H, A, B, C, D, E, F
F	F, A, B, C, D, E

Fig. 2. Here, the Ethernet (802.3) station A wants to communicate with station B. It sends out an ARP request to resolve B's address. Both 802.3 segments are transparently intereconnected via a Mesh WLAN. The MPPs operate as bridges. In the Mesh WLAN MPs need to keep adress table for path selection and frame forwarding.

B. 802.15.5

802.15.5 became TG in January 2004. It defines a recommended practice for Mesh *Wireless Personal Area Network (WPAN)*. Although the PAR considers high (e. g. 802.15.3) and low rate (e. g. 802.15.4) WPANs, responds for the *Call for Applications (CFA)* and *Call for Proposals (CFP)* were driven by demands for high rate Mesh WPAN. Therefore, the current focus of 802.15.5 is on range extension and convenient coverage in the home environment. In consideration of the special requirements of Mesh WPAN, 802.15.5 forms an independent TG and target on not an amendment to existing standards. However, the annex of 802.15.5 provides guidelines how to implement a Mesh WPAN with current WPAN standards. Thus, 802.15.5 may work independent or in coexistence with other 802.15 non-Mesh WPAN.

Association of Legacy *Devices (DEVs)* with a Mesh-*Piconet Controller (PNC)* is possible. However, Mesh-WPANs co-located with a "Legacy PNC" need to support coexistence, because PNCs rely on exclusive spectrum usage. In addition, TG5 introduces the concept of Light-Mesh-PNCs. A Light-Mesh-PNCs does not provide association service to any DEV. It forwards data and participates in the formation of a Mesh WPAN, thus supporting other Mesh-PNCs in the formation of the Mesh WPAN. The most simple type of entities is a Mesh-DEV. It has the capability to associate with multiple PNCs. However, it fully relies on a PNC. It cannot forward frames or participate in the Mesh WPAN.

C. 802.16

The current 802.16 standard [5], [7] describes *Point-to-Point (PtP)*, *Point-to-Multipoint (PMP)* and Mesh mode operation. In non-Mesh mode, any traffic is sent to or from the *Base Station (BS)*. *Subscriber Stations (SSs)* exchange frames via the central BS only. In an 802.16 Mesh, SSs mutually forward traffic and communicate directly. According to the frame based approach of 802.16, a *Wireless Metropolitan Area Network (WMAN)* is always synchronized. In contrast to the PtP or PMP mode, the Mesh WMAN solely supports *Time Division Duplex (TDD)*. In an 802.16 Mesh, SSs are denoted as nodes. To account for the difficult interference situation in WMNs, 802.16 provides definition for neighborhood and extended neighborhood. All nodes in a nodes's communication range belong to its neighborhood. The extended neighborhood forms the set of nodes that are two hop away from a node's point of view. 802.16 Mesh foresees the usage of omnidirectional antennas. Only nodes at the edge of the Mesh may use directional antennas.

1) 802.16j: At the end of March 2006, the Relay TG (TG "j") was formed by approval of the PAR, which the *Mobile Multihop Relay (MMR)* SG developed. 802.16j works on WRNs. WRNs form a sub-set of WMNs. While each entity in a WMN has forwarding capability, a WRN bases on a master-slave architecture. In 802.16j, the BS has full control over the WMAN. Relay SS forward data on request of the BS. 802.16j distinguishes three different types of relay entities [8]. A *Fixed Relay Station (FRS)* is immobile. The *Nomadic Relay Station (NRS)* has fixed location for periods comparable to a user session. The *Mobile Relay Station (MRS)* forwards data even when being in motion.

III. MAC Enhancements for WMNs

Independent frame transmissions in *Wireless Mesh Networks (WMNs)* cannot be mutually decoupled. Each frame transmission affects the neighborhood of the transmitting device, emits interference to the direct and indirect neighborhood and mandates no harmful concurrent transmission in the surroundings of the receiving entity. As the wireless 802 standards are very different, so are their approaches to deal with the harsh environment. Table I provides an overview.

A. 802.11s

The basic Mesh *Wireless Local Area Network (WLAN)* is unsynchronized and uses *Enhanced Distributed Channel Access (EDCA)* [9] as *Coordination Function (CF)*. Since EDCA cannot prioritize *Access Points (APs)* over stations, in many scenarios the *Mesh Access Point (MAP)* relies on two radios. One transceiver is used for the Mesh WLAN while the other provides the AP functionality. As an 802.11 WLAN can be easily congested, the current draft introduces an optional congestion control mechanism. Each *Mesh Point (MP)* monitors its in- and out-going traffic rate. With the help of an *Information Element (IE)* broadcasted in the beacon frame, the MP signals its congestion status to its neighborhood. Additionally, an MP may send a unicast frame to request throttling of frame transmissions of its neighbor MP.

For increased efficiency, the current draft describes *Common Channel Framework (CCF)* and *Mesh Deterministic Access (MDA)* as optional CFs. Both, MDA and CCF rely on the optional synchronization mechanism. The CCF foresees channel frequency switching. MPs periodically tune their radio to the common channel. There they exchange short *Request to Switch (RTX)*/*Clear to Switch (CTX)* messages to negotiate on a different frequency channel that is used for data frame exchange. MDA works as reservation based access mechanism that schedules transmissions and provides contention

TABLE I

OPERATION MODES IN *LAN/MAN Standards Committee (LMSC)* WMNS

	synchronized	unsynchronized
centralized	802.16	
decentralized	802.11, 802.15, 802.16	802.11

free access to the *Wireless Medium (WM)*, see Fig. 3. MDA divides the Mesh superframe into slots of 32 µs. Each *MDA Opportunity (MDAOP)* consists of several slots. At the beginning of MDAOPs that an MP has reserved, all neighboring MDA capable MPs preset their *Network Allocation Vector (NAV)*. Thus, the MDAOP has highest priority in channel access.

B. 802.15.5

In its current form, *Task Group (TG)* 5 defines a decentralized, synchronized WMN. A Mesh wide superframe is divided into *Medium Access Slots (MASs)*. Some MASs in the beginning of each superframe are reserved for transmission of beacon frames. These frames synchronize the Mesh *Wireless Personal Area Network (WPAN)*. As option, Mesh entities may choose to distribute their beacon transmission over the superframe. Although such scheme may be easier to implement, it is less efficient as entities need to switch at arbitrary times from sleep to awake state to be able to receive their neighbhors' beacons. All mesh capable entities use a reservation based protocol [10]–[14] to access the WM. It guarantees collision free transmission. Under consideration of the information provided by neighboring beacons, entities choose MASs that are currently unused in their neighborhood. With adaptive selection algorithms, interference can be furthermore limited. Reservation of the WM may be indicated using relative timing (offset from now in µs) or with the help of the MASs. The latter one involves less overhead since the granularity is higher.

The beacon frames are protected from neighboring interference. Neighboring entities mark MASs used for beacon transmission as occupied. Thus, neighbors' neighbors will not reuse a beacon MAS. While neighbors can receive and decode the beacon information, indirect neighbors can measure its signal strength. Informed by intermediate entities about the beacon MAS owner, indirect neighbors can detect their mutual signal strength. Thus, entities may set-up an internal interference graph that allows them to identify opportunities for spatial frequency reuse.

C. 802.16

Due to its frame based concept an 802.16 Mesh always operates synchronously. *Subscriber Stations (SSs)* synchronize to the *Base Station (BS)* or the neighboring SS that is closest to the BS. In an 802.16 Mesh *Wireless Metropolitan Area Network (WMAN)*, medium access may be either de- or centrally coordinated. Using the centralized Mesh mode, a single Mesh BS coordinates access to the WM. It schedules transmissions and has full control over the WM like a BS in a non-Mesh WMAN. With centralized scheduling, the Mesh BS collects the schedules of all nodes and grants or denies access to the WM based on the unified schedule. Intermediate SSs forward requests of other SSs that are out of range of the BS. The BS broadcasts the amount of resources a link may use (schedule assignment and configuration). Again, SSs forward the information to other SSs. With the help of a common algorithm, all Mesh SS compute the same schedule as the BS and translate it into the according *Uplink (UL)* and *Downlink (DL)* subframe timing. With decentralized scheduling, each node broadcasts its schedule in the extended neighborhood. Therefore, it periodically dissemeniates a *Mesh Distributed Schedule (MS-DSCH)* message. Each node is responsible to ensure collision-free operation. Thus, a node needs to look for unused resources in the UL and DL subframes in the two-hop neighborhood. *Physical Slots (PSs)* of a frame that are not used by any other burst may be claimed for its own transmissions. To compete on PSs, SSs may optionally a use random access channels as in *Point-to-Multipoint (PMP)* mode. As third approach, a Mesh WMAN may use a combination of de- and centralized scheduling.

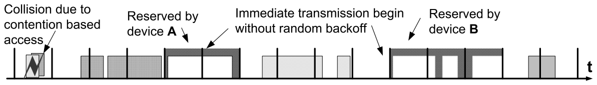

Collision due to contention based access
Reserved by device A
Immediate transmission begin without random backoff
Reserved by device B
t

Fig. 3. The optional MDA in 802.11s and 802.15.5 use a slotted superframe to negotiate on reservation based access. 802.15.5 negotiates on the reservation of MASs with the help of beacon frames. MDA uses explicit messages for reservation agreements. Unreserved MASs may be reused with contention based medium access.

1) 802.16j: Due to its centralized structure, the *Wireless Relay Network (WRN)* approach of 802.16j foresees introduction of BS functionality in the *Relay Station (RS)*. The RS partially operates as BS to other *Mobile Stations (MSs)* and SSs. Current 802.16 supports a variety of *Physical Layer (PHY)* technologies. However, 802.16j foresees *Orthogonal Frequency Division Multiple Access (OFDMA)* only. As the RS may serve several other entities, it shall support aggregation of traffic that is received via *Point-to-Point (PtP)* and PMP connections. Depending on its capabilities, the RS may handle uni- and broadcast traffic.

IV. PATH SELECTION IN WMNS

The concatenation of *Mesh Links (MLs)* defines a Mesh path. Depending on the network topology, several Mesh paths may be available from a source to the destination entity. Path selection algorithms select the best Mesh path. Since the *Wireless Medium (WM)* is a harsh environment, quality of a ML constantly changes. To achieve the best path selection decision, the ML metrices need to be quickly adapted, see Fig. 4. Furthermore, path selection algorithms ensure loop-free operation of the *Wireless Mesh Network (WMN)*. Especially multi- and broadcast frame distribution is difficult to handle. Application of spanning tree related protocols is not sufficient.

A. 802.11s

The current draft [6] defines *Hybrid Wireless Mesh Protocol (HWMP)* as the default path selection mechanism. It combines aspects of reactive (on-demand) and proactive routing protocols. In its basic form, HWMP reuses concepts proposed by *Ad-hoc On-demand Distance Vector (AODV)* [15]. *Mesh Points (MPs)* periodically broadcast beacon frames. The beacon frames carry path selection and topology information. On-demand *Route Request (RREQ)* frames may be transmitted when needed. In addition to the AODV concepts, HWMP provides a tree based approach. If a root MP is available, HWMP uses on-demand routing mechanisms. In many cases the *Mesh Point colocated with a Mesh Portal (MPP)* will be configured as root MP. An MPP is an MP that bridges the Mesh *Wireless Local Area Network (WLAN)* with non-802.11 networks. All MPs proactively maintain a path to the root MP. Other MPs rebroadcast the root annuncement message to allow neighboring MPs to discover the root MP and to calculate the distance in terms of hops.

B. 802.15.5

The proposed path selection scheme [16] in 802.15.5 uses a method referred to as *Meshed Adaptive Robust Tree (MART)*. It provides a path selection scheme for *Low Rate (LR)* Mesh-*Wireless Personal Area Network (WPAN)*. Due to the current scope of *Task Group (TG)*5 MART is adapted to the needs of *High Rate (HR)* Mesh-WPAN. Each Mesh-*Piconet Controllers (PNCs)* forms the root of a tree. Neighboring Mesh-PNCs treat each other as child or leaf node in the local routing tree. With the tree's help, each Mesh-PNC decides on which neighbor to choose as next hop. For unknown destinations, neighboring Mesh-PNCs help to find the optimal path. Their local knowledge may help to reroute. Non-optimal paths must be used when a frame needs to ascend and descend the tree via a different root Mesh-PNC. This intermediate Mesh-PNC has knowledge about paths to Mesh-PNCs, which are mutually unaware. Broadcast RREQs are solely needed for path discovery when no Mesh-PNC in the Mesh WPAN can provide a path. To further reduce the path selection overhead, short tree addressing is proposed. In the general case, full *Medium Access Control (MAC)* addresses identify devices. However in small scale Mesh-WPAN, path selection may benefit from short address. In 802.15.3, each Mesh-PNC has a *Piconet Identifier (PNID)*. It assigns *Device Identifiers (DevIds)* to its associated *Devices (DEVs)*. Together, PNID and DevId uniquely identify a DEV. To ensure non-ambiguous PNIDs, a *Mesh Coordinator (MC)* assigns PNIDs from its pool.

C. 802.16

Since an 802.16 *Wireless Metropolitan Area Network (WMAN)* always includes a *Base Station (BS)*, the logical topology of the WMAN forms a tree. The root node is the BS. Therefore, the current standard does not define any routing algorithms or application thereof.

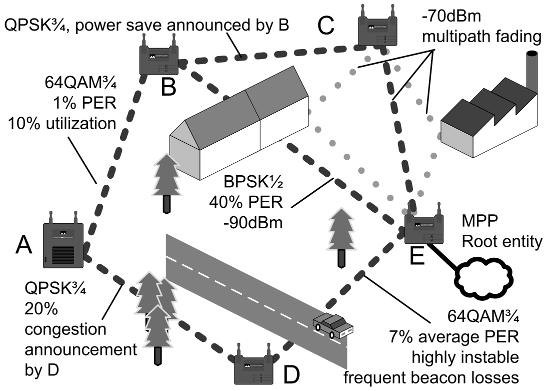


Fig. 4. MLs have several properties that influence the path selection decision. Furthermore, ML properties may depend on the transmissin direction.

1) 802.16j: While routing or path selection mechanisms may not be needed in WMAN, the mobility of *Nomadic Relay Stations (NRSs)* and *Mobile Relay Stations (MRSs)* introduces the thread of looping frames. Depending on the capability of the NRSs and MRSs, direct connection set-up and frame exchange between neighboring entities must be able to detect looping frames and stop to relay them.

V. Security Improvements for WMNs

Current standards for wireless networks in the 802 secure frames at the link layer. Presently, only 802.16 provides tunneling concepts for end-to-end security over multiple hops. Besides confidentiality of messages, enforcement of *Authentication, Authorization and Accounting (AAA)* services and prevention of *Denial of Service (DoS)* attacks are issues in public *Wireless Mesh Networks (WMNs)* also.

A. 802.11s

Security in 802.11s uses the mechanisms defined in [17]. Thus, the current approach provides no end-to-end security. Based on 802.1X [18] the extensions support centralized or distributed authentication and key management. Using decentralized security scheme, *Mesh Points (MPs)* mutually authenticate. Thus, two handshakes appear. With centralized security model, the authenticator operates as proxy between the supplicant and the *Authentication Server (AS)*. MPs serve as authenticator, when a new MP request access to the Mesh *Wireless Local Area Network (WLAN)*.

B. 802.15.5

802.15.5 received a security proposal that bases on pre-distributed keys. Each Mesh-*Piconet Controller (PNC)* in the network receives several keys during set-up. Within the Mesh *Wireless Personal Area Network (WPAN)* two and only two Mesh-PNCs hold a common pair of keys K_x and K_y. Other entities in the Mesh WPAN may have either K_x or K_y but not both. Then, the hash function of the keys provides a unique key that is used for secure communication. Details can be found in [16], [19].

C. 802.16

Security in 802.16 provides encapsulation of encypted data and a *Privacy Key Management (PKM)*. The mandatory *Base Station (BS)* in each *Wireless Metropolitan Area Network (WMAN)* serves as AS. The BS grants or denies access to the WMAN. It provides keys and enforces encyption in the network. However, in Mesh mode some *Subscriber Stations (SSs)* are out of range of the BS. Then, intermediate SSs need to encrypt transmissions on their neighboring links. For each of its neigbhors, a SSs negotiates on a separate encryption key. To prevent session timeout, each SS regularly renews keys with its neighbors. Data is encrypted either in *Cipher Block Chaining (CBC)* or *CTR mode with CBC-MAC (CCM)* mode.

1) 802.16j: As *Wireless Relay Network (WRN)*, 802.16j relies on the central BS and the mechanisms introduced in the base standandard. Extensions to the current security framework need to consider customer owned and operated SSs or *Mobile Stations (MSs)* that operate as *Relay Stations (RSs)* for the WMAN provider. As the RS potentially forwards other customers data, integrity and confidentiality of the relayed information is needed. Also, the RS shall not be able to compromise the WMAN. During association with the WMAN, the BS must ensure that the data provided for log-in via the RS is valid and hidden to RS.

VI. Conclusions

802.11s provides the most advanced *Wireless Mesh Network (WMN)* concept in the *LAN/MAN Standards Committee (LMSC)*. In its present form, 802.11s covers all aspects of of WMNs. Its usage scenarios foresee highly mobile applications (military and public safety users), enterprise networks and home environment. Due to its wide range of applications, several companies have announced future products to be compliant with 802.11s.

802.15.5 is more ambitious. The current proposal optionally foresees highly efficient spatial frequency reuse. With its new approaches for medium access, exploitation of the capacity of the *Wireless Medium (WM)* becomes possible. Furthermore, the current *Medium Access Control (MAC)* approach offers efficient power save mechanisms.

Although 802.16 is the first standard in the LMSC to introduce concepts for WMNs no products are available currently. Due to rather vague description, the concept is not mature. Therefore, 802.16j is more likely to be successfully deployed in the market. The *Fixed Relay Station (FRS)* concept offers the possibility to cheaply increase the *Base Station (BS)*'s range. *Nomadic Relay Station (NRS)* and *Mobile Relay Station (MRS)* may less likely be introduced in the market.

References

[1] G. R. Hiertz, S. Max, Z. Yuneng, L. Stibor, and H.-J. Reumerman, "IEEE 802 Wireless Mesh Networks (802.0 Submission)," Online, IEEE LMSC (LAN MAN Standards Committee), Vancouver, Canada, Tech. Rep. 11-05-1163-00-0000, Nov. 2005, IEEE 802.0. [Online]. Available: http://www.comnets.rwth-aachen.de

[2] G. R. Hiertz, S. Max, E. Weiß, L. Berlemann, D. Denteneer, and S. Mangold, "Mesh Technology enabling Ubiquitous Wireless Networks," in *Proceedings of the 2nd Annual International Wireless Internet Conference (WICON)*, Boston, USA, Aug. 2006, Invited Paper, p. 11.

[3] B. Walke, S. Mangold, and L. Berlemann, *IEEE 802 Wireless Systems - Protocols, Multi-Hop Mesh/Relaying, Performance and Spectrum Coexistence*. Wiley, Sept. 2006, to appear.

[4] "Mobile Ad-hoc Networks (MANET) Working Group," The Internet Engineering Task Force (IETF). [Online]. Available: http://www.ietf.org/html.charters/manet-charter.html

[5] *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.

[6] *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.

[7] *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.

[8] R. B. Marks, M. Nohara, J. Puthenkulam, M. Hart, and et al., "802.16 Mobile Multihop Relay," Online, IEEE LMSC (LAN MAN Standards Committee), IEEE 802 Tutorial IEEE 802.16mmr-06/006, Mar. 2006. [Online]. Available: http://ieee802.org/16/sg/mmr/docs/80216mmr-06_006.zip

[9] *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.

[10] G. R. Hiertz, Y. Zang, J. Habetha, and H. Sirin, "IEEE 802.15.3a Wireless Personal Area Networks - The MBOA Approach," in *Proceedings of 11th European Wireless Conference 2005*, vol. 1. Nicosia, Cyprus: Microsoft Innovation Center Europe, ATHK CYTA, Apr. 2005, pp. 204–210. [Online]. Available: http://www.comnets.rwth-aachen.de

[11] G. R. Hiertz and J. Habetha, "A new MAC Protocol for a wireless multi-hop broadband system beyond IEEE 802.11," in *Wireless World Research Forum, 9th Meeting in Zurich, Switzerland*, July 2003.

[12] G. R. Hiertz, Y. Zang, J. Habetha, and H. Sirin, "Multiband OFDM Alliance - The next generation of Wireless Personal Area Networks," in *Proceedings of the 2005 IEEE Sarnoff Symposium*, Princeton, New Jersey, USA, Apr. 2005, p. 7. [Online]. Available: http://www.comnets.rwth-aachen.de

[13] G. R. Hiertz, J. Habetha, P. May, E. Weiss, R. Bagul, and S. Mangold, "A Decentralized Reservation Scheme for IEEE 802.11 Ad Hoc Networks," in *The 14th IEEE 2003 International Symposium on Personal, Indoor and Mobile Radio Communications*, Sept. 2003. [Online]. Available: http://www.comnets.rwth-aachen.de

[14] G. R. Hiertz, Y. Zang, S. Max, and H.-J. Reumerman, "Mesh PAN Alliance (MPA) (IEEE 802.15 Proposal Submission)," Online, IEEE LMSC (LAN MAN Standards Committee), Cairns, Australia, Tech. Rep. 15-05-0247-00-0005, May 2005, IEEE 802.15, Task Group 5, Mesh WPAN. [Online]. Available: http://www.comnets.rwth-aachen.de

[15] C. Perkins and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," RFC 356, Mobile Ad-hoc Networks (MANET) - The Internet Engineering Task Force, July 2003. [Online]. Available: http://ietf.org/rfc/rfc3561.txt

[16] J. Zheng, C. Zhu, M. Wong, and M. Lee, "IEEE 802.15.5 WPAN Mesh Networks," Online, IEEE LMSC (LAN MAN Standards Committee), Cairns, Australia, Tech. Rep. 15-05-0256-01-0005, May 2005. [Online]. Available: http://802wirelessworld.com

[17] *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 6: Security Enhancements*, IEEE Amendment to IEEE Std 802.11, 1999 Edition (Reaff 2003) IEEE Std 802.11i-2004, July 2004.

[18] *IEEE Standard for Local and metropolitan area networks - Port-Based Network Access Control*, IEEE Computer Society IEEE Std. IEEE Std 802.1X-2004, Dec. 2004, sponsored by the LAN/MAN Standards Committee.

[19] G. R. Hiertz, Y. Zang, L. Stibor, S. Max, H.-J. Reumerman, D. Sanchez, and J. Habetha, "Mesh Networks Alliance (IEEE 802.11 TGs Proposal submission)," Online, IEEE Computer Society, San Francisco, California, USA, p. 57, July 2005. [Online]. Available: http://www.comnets.rwth-aachen.de