


QoS-aware Flow Monitoring and Event Creation in Heterogeneous MPLS-based Wireless Mesh Networks supporting Unidirectional Links

Mathias Kretschmer, Christian Niephaus
 Fraunhofer FOKUS
 Sankt Augustin, Germany
 mathias.kretschmer@fokus.fraunhofer.de
 christian.niephaus@fokus.fraunhofer.de


 Gheorghita Ghinea
 Brunel University
 London, United Kingdom
 george.ghinea@brunel.ac.uk

Abstract—Monitoring is a crucial task in QoS-aware networks since it provides statistics to verify that the network performs within the committed QoS parameters. It is especially important in a resource-constrained Carrier-grade Wireless Mesh Access Network (CG-WMAN) in order to monitor a node's neighborhood, established links as well as MPLS QoS-traffic flows, so-called Label-Switched Paths (LSPs). In this paper, we present a monitoring architecture for LSPs in a heterogeneous CG-WMAN, where configurable Rating Agents perform adaptive per-LSP event creation based on monitoring statistics, QoS-requirements and overall network state. Keeping the footprint of the monitoring mechanism at a minimum, our approach is based on quasi-passive monitoring minimizing the transmission of extra frames. To support unidirectional links as well as 1-to-N multicast trees, a receiving side feedback-free mechanism is proposed which can be extended with transmitting side functionality. Initial results obtained in our testbed show that we can reliably detect under-performing links according to the QoS requirements of the payload.

Keywords Heterogeneous Wireless Mesh, QoS, Monitoring, Unidirectional Links

I. MOTIVATION

The visibility and success of Wireless Mesh Network (WMN) deployments has raised interest among commercial operators in this technology. A WMN-type architecture considered as an alternative for an operator access network must meet similar requirements such as guaranteed Quality of Service (QoS) and high availability in order to allow for provisioning of triple-play services. Thus, CG-WMANs can be compared to typical operator access network with two major limiting factors: the severe capacity constraints due to scarce wireless spectrum resources and the volatile link conditions. The heterogeneous CG-WMAN developed by the CARrier grade wireless MESH Network (CARMEN)[3] consortium is based on a concept which combines and adapts technology independent Multi Protocol Label Switching (MPLS)-based Traffic Engineering[2], IEEE 802.21 command and event services as well as a model to address the potentially shared frequency spectrum resources of wireless links. LSP are used at an aggregate level to separate traffic classes with different QoS requirements and to support Mobile Terminal (MT) mobility through Proxy Mobile IP

(PMIP)[6].

Detailed wireless link and LSP monitoring is a difficult task due to the dynamic nature of wireless links caused by temporary fading and interferences, but also due to often very dynamic per-frame transmitter configurations. A *link* in the context of this work refers to a bidirectional or unidirectional association among two wireless interfaces of neighboring nodes. The wireless technologies considered in our CG-WMAN range from satellite (i.e. DVB-S) over 3GPP to IEEE 802.16 and 802.11. A typical scenario with multiple LSP and different QoS requirement sharing the same physical links is depicted in Figure 1. A backup LSP has been pre-configured to allow for an instant fail-over in case of a breakage of the protected path segments.

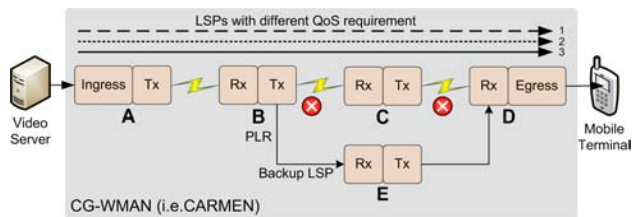


Fig. 1. Typical MPLS network with LSPs carrying different QoS payload and a pre-configured backup LSP

While the fail-over action needs to be performed quickly in order to avoid service interruptions, the decision needs to be carefully considered since existing traffic on the underlying links might be impacted and mis-configured trigger might cause network instability or even oscillation. Since overall network optimization is a complicated and relatively slow process, it can not react immediately on each LSP breakage. Configuring the local criterion function according to the overall network state is the task of a network management component which has the complete view of the network and can therefore compute an optimized set of rules. Once configured, the criterion function will make quick decisions based on local knowledge only, which it gathers from evaluation of throughput, activity, loss, forwarding latency and signal quality statistics related to an LSP.

Link breakage can be detected by technology specific

mechanisms. But depending on the QoS requirements of an LSPs, such mechanisms might not be suitable and a more adaptable and differentiated solution is needed. This solution may take one or multiple LSP statistics into account to determine when to create a *REROUTE* event. For example, a VoIP LSP might tolerate some loss but require a low packet delay variation, while regular web traffic would be much more tolerant. Like all criterion functions, the *REROUTE* criterion function could be seen as a plug-in, chosen for a specific technology or payload.

Active *ALIVE* messages to detect a wireless link breakage consume precious link resources due to the Media Access Control (MAC) overhead, in particular on shared channels. Depending on the technology they might even cause an *ACK* frame to be returned. Thus, passive means of link breakage detection or prediction should be preferred. Where active signaling is necessary, existing technology-inherent mechanisms should be utilized whenever applicable. Our LSP monitoring solution is designed to also support unidirectional technologies such as Digital Video Broadcast (DVB) or the transmission of, for example, low-delay VoIP traffic using the IEEE 802.11e *NOACK* policy. For stable, stationary long-distance links, *ACKs* might also have been disabled, due to the increased latency introduced by a per-frame Automatic Repeat reQuest (ARQ) mechanism. Therefore, we propose a passive feedback-free mechanism located at the receiving side of a link. Additionally, transmitting side monitoring should be performed where supported by the underlying technology. Data that could be gathered on the transmitting side includes queuing or traffic shaper delay and overruns, packet loss or bandwidth statistics.

This paper is organized as follows. In the next section we discuss related work regarding wireless network and flow monitoring. The following section describes our approach, an integrated solution for LSP monitoring as well as an adaptive rating agent for LSP related event creation. In the 'Validation' section we present initial measurement results obtained in our testbed. Concluding, we summarize our contribution and give an outlook on future work.

II. RELATED WORK

Traffic Engineering (TE) relies on monitoring data for proactive off-line and reactive dynamic approaches[1]. The TE concepts relying on MPLS have mainly been developed for wired networks with orthogonal point-to-point links based on reliable technologies such as optical fiber or Ethernet. The breakage of such a medium can quickly be detected and fail-over times of about 50ms are typical in Synchronous Optical Networking (SONET) networks. Multiple schemes have been proposed to allow MPLS Fast Reroute (FRR)[11] to provide similar fail-over times[13].

In the context of wireless networks, the definition of a broken link is rather fuzzy and very technology or even implementation dependent. Hence additional parameters

need to be considered in order to reliably evaluate link quality and reliability and in the literature a plethora of schemes have been studied, such as [10], [14] and [9]. Often, the proposed solutions combine analysis with event creation. Our work provides a framework that separates link analysis and statistics gathering from interpretation and adaptable overall network state aware event creation. Additionally, multiple criterion functions could be deployed interchangeably depending on specific technology or payload characteristics.

IPFix[12] defines a protocol to export traffic IP flow information generated by metering processes which is usually collected by external processes[5] to serve as a basis for further analysis. In the context of this work we focus on fast local event creation based on local metering data and pre-configured thresholds. The IPFix concept could however be applied for longer term traffic analysis within a CG-WMAN.

III. APPROACH

Monitoring in a CG-WMAN is a complex task that operates at multiple network stack layers, from the Physical Layer to the MPLS layer, which is often referred to as Layer 2.5. The monitoring module performs the following tasks:

- Neighborhood monitoring and per-frame analysis
- Maintenance of neighboring node statistics
- Creation of link level *up* or *down* events
- Provision of LSP end-to-end performance statistics
- Creation of QoS & network state aware LSP events

In this paper we present the Technology Independent Monitoring (TIM) component to separate the tasks of measuring LSP per-hop and end-to-end statistics from adaptable per-hop LSP-specific events creation. Figure 2 depicts the architecture of our monitoring architecture where TIM is located above a link monitoring component. The *Rating Agent* component is located on top of TIM. It operates on the LSP statistics gathered by TIM but is controlled by and performs tasks related to the network management or path computation components. The communication between the monitoring subsystem and the network management components is implemented via extended IEEE 802.21 Command and Event Services which are already used extensively throughout our CG-WMAN. While multiple types of events could be created, in this paper we focus on a *REROUTE* event which can be issued at each hop on a per LSP basis taking the individual QoS requirements, technology-specific characteristics and overall network state into account.

A. Receiving and Transmitting Side Monitoring

A link can be monitored from the transmitting side, the receiving side or from both. The data measured, its accuracy and interpretation as well as the possible events that could get triggered vary depending on the underlying technology. Hence, certain data should be monitored on a particular side of a link. For example, a periodic or

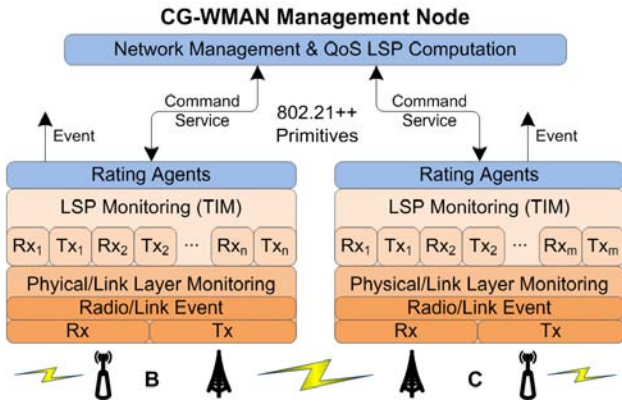


Fig. 2. The TIM Monitoring Architecture uses 802.21++ primitives for its local and remote messaging

constant signal needs to be present on a link in order for the receiving side to detect that a transmitter is alive. Figure 3 depicts one-hop LSP segment sharing a physical link and the parameters that can be measured on the transmitting side or receiving side of each LSP segment.

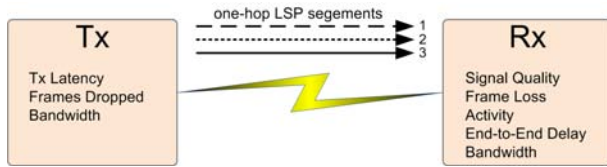


Fig. 3. Possible transmitting and receiving side monitoring parameters per LSP segment

As suggested in RFC 3272[2] our CG-WMAN performs end-to-end monitoring of individual LSP statistics. In addition to the actual bandwidth utilization, we also maintain loss, signal quality, delay and activity statistics which can indicate wireless link stability with a varying significance depending on the QoS requirements of the payload. This receiving side monitoring measures the actual end-to-end characteristics of a LSP and is therefore mandatory to verify if an LSP receives the agreed end-to-end QoS handling. The per-LSP QoS requirements are installed at each node on the path during the LSP setup procedure together with the LSP forwarding state. This information is therefore available to transmitting as well as receiving side monitoring.

Transmit side monitoring can provide valuable information about the per-hop QoS handling of an LSP. Depending on the wireless technology a node can detect on the transmitting side if the forwarding latency of a frame is within the guaranteed bounds or if frames are dropped due to traffic shaper policies. Also, it can measure the burst and average bandwidth utilization over various intervals. However, transmitter side loss monitoring relies on receiver feedback via, for example, a Link Layer ARQ mechanism. Therefore it can not detect transmission errors when frames are sent with a unidirectional link configuration. This includes multicast or broadcast frames

since they are usually sent without any *ACK*.

If the *rating agent* creates a *REROUTE* event, it needs to be signaled to the upstream Point of Local Repair (PLR) (node B in Figure 1) so that it redirects the traffic onto a pre-configured backup LSP. Ensuring the delivery of the *REROUTE* event to the PLR can be a difficult task in a situation of unstable or natively unidirectional links. The proper calculation of backup LSPs and provision of reliable signaling paths is part of the path computation component of the CG-WMAN and out of the scope of this document.

In the special case of node B, the transmit side of the link could be the ideal place to create and react upon *REROUTE* events, since event creation and reaction would be node local procedures.

As detailed above, end-to-end receiving side monitoring is mandatory to assess the QoS handling an LSP receives. Optionally, transmitting side monitoring can be used to gather additional node-local data regarding an LSP which can help with anomaly detection and faster *REROUTE* event delivery.

B. Technology Independent LSP Monitoring

Our monitoring approach, TIM, provides loss, delay, activity and signal quality statistics per LSP or its segments over physical links implemented by heterogeneous technologies. This data is evaluated by *Rating Agents* to create LSP-specific events. In order to reduce wireless resource consumption, TIM tries to minimize the number of extra frames being sent or the header overhead introduced by aggregating LSP measurements and exploiting technology-specific features where possible.

TIM defines a header which can be seen as a technology independent extension of the MPLS shim header in order to provide a protocol, payload and technology independent mechanism to perform feedback-free end-to-end loss and delay measurements per LSP. As depicted in Figure 4, the TIM header is 32 bits wide and is always sent after the MPLS label stack, which in the CG-WMAN context usually only consists of one label, unless temporary backup paths via tunneling are in affect. Hence, the header parsing complexity per hop is minimal.

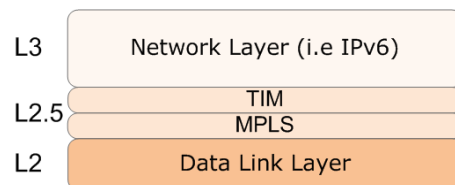


Fig. 4. Position of the TIM header in the protocol stack *extending* the MPLS header

The TIM header as depicted in Figure 5 is inserted at the MPLS ingress node and thus is sent piggy-back along the LSP and removed at the egress router together with the MPLS label stack. Should multiple MPLS labels be added to the stack due to FRR or other means of traffic

engineering, the TIM header remains untouched in order to still allow for end-to-end LSP measurements.

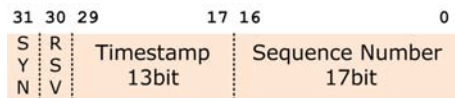


Fig. 5. The TIM header is 32 bits wide

The ingress node maintains a 17bit wide cyclic *sequence number* per outgoing LSP, which is copied into the TIM header of each outgoing packet of the LSP. The *sequence number* wraps around after 131072 frames per LSP which can cover a sufficiently long period to detect packet loss or reordering. To identify even larger burst losses, a correlation with the time stamp field can be used to still detect the loss, while a precise quantification is no longer possible. Packet reordering should not occur since forwarding strictly follows the LSP, but might occur for short periods during a LSP fail-over process. Therefore, reordering-aware loss calculation algorithms should be used and the degree of acceptable reordering for a specific LSP should be derived from its QoS requirements. Longer periods of packet reordering would indicate a network misconfiguration, a misbehaving link or node.

The 13 bit wide *time stamp* field is filled with the current time of the ingress node when sending out the packet. The resolution is 1ms and thus allows for a maximum delay of 8192 ms to be measured. This is sufficient to even cover, for example, shared Digital Video Broadcast - Satellite (DVB-S) satellite return links with a typical latency between some hundred milliseconds and multiple seconds. The *SYN* bit is used to indicate that the ingress nodes uses a clock synchronized to a global time base such as Global Positioning System (GPS) and that the implementation guarantees an accuracy of $< 1\text{ms}$. If the egress node's clock is also synchronized to the same time base, the time difference between the *time stamp* and the egress node's clock can be assumed to be the actual packet end-to-end forwarding delay with a $\pm 2\text{ms}$ tolerance. If the clocks are not synchronized, the delay variation of subsequent packets can be interpreted. RFC3393[4] provides further details regarding Packet Delay Variation (PDV) measurements with unsynchronized clocks.

Bandwidth measurements can be performed on an LSP basis by calculating, for example, a sliding average of the actual bandwidth consumption of the LSP. Signal quality and activity analysis could be performed similarly to the bandwidth analysis by just interpreting frames of a specific LSP. This approach would ignore valuable information, since here we are only interested in information regarding the state of the underlying link regardless of the LSP a frame belongs to. Hence, in Figure 3, any frame sent from node A for any LSP that is received by node B, can be interpreted as activity. Also, the signal quality and radio parameters of such a frame can be evaluated. Care needs to be taken if dynamic transmitter configurations,

for example, regarding the transmit power or Modulation and Coding Scheme (MCS) are in being used by the transmitting node. Activity and signal quality analysis are mainly of node-local importance for the *Rating Agent* to evaluate link reliability.

Intermediate MPLS nodes may examine the TIM header similarly to the egress node to maintain loss and delay statistics between the ingress node and themselves. Those statistics could be evaluated by *Rating Agents* or explicitly queried for debugging purposes to locate under-performing segments. Likewise, the TIM header may be evaluated by each node in MPLS 1-to-N multicast trees to determine loss and delay between itself and the root.

C. Rating Agent

The *Rating Agent* can be seen as a plug-in and consists of a list of dynamically chosen and individually configured criterion functions which can create arbitrary events related to an LSP and its statistics such as such as exceeded burst bandwidth, signal quality degradation, inactivity or loss above a certain threshold. *Rating Agents* are invoked upon processing of each frame by TIM or the expiration of an inactivity timer to ensure timely event creation.

D. Adaptive LSP REROUTING Events

In the context of this work we focus on *REROUTE* events which trigger a two-fold recovery procedure. As a quick and temporary fail-over solution, the use of a precomputed MPLS FRR backup path will be signaled to the node upstream of the under-performing link. In parallel, the mesh area coordinator will receive an event about this incident. Using its more complete topology knowledge, it will compute and install a new primary LSP as well as a backup LSP. Once the new LSPs have been set up, the traffic is routed onto this new path. The route computation module relies on feedback from established LSPs as well as basic link monitoring to maintain overall network link state and utilization.

IEEE technologies such as 802.11 or 802.16 determine a link to be *up* by monitoring the channel for periodically broadcasted frames, such as beacon frames or super frames. Broadcast technologies such as DVB permanently send out a carrier which receiving nodes acquire and maintain a *lock* on. If no actual data is available, so-called *stuffing frames* are transmitted, but are usually filtered out by the receiving hardware and can therefore not be used to detect transmitter liveliness. In the case of DVB, regularly broadcasted mandatory tables such as the Network Information Table (NIT) could be seen as the equivalent of a beacon and longer periods without a received NIT would indicate a broken or flaky link. In both cases the detection process might be too slow or not accurate enough for a CG-WMAN, since it might take one second or longer until the upper layers of a node are informed about a link breakage. Additionally, the threshold when a link is considered *down* depends heavily on the QoS requirements of the affected LSPs.

Although the transmission of extra *ALIVE* frames to determine the link state should be avoided due to the additional overhead they are still necessary in some cases. Especially when monitoring the availability of an idle LSP. The number of such frames should be minimized by taking into account existing traffic and by aggregating the *ALIVE* frame interval, so that it covers all LSP in questions. In Figure 6 different *ALIVE* intervals for the active LSPs have been configured. The actual *ALIVE* interval used is the smallest one among all intervals. The default *ALIVE* interval is initially determined by a fixed value per traffic class. It can be adjusted by the management component to optimize overall network performance.

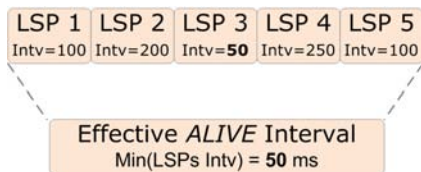


Fig. 6. Individual per-LSP and effective *ALIVE* Interval

Most recent wireless technologies support the use of different MCS configurations per destination. For multicast or broadcast frames, typically the most robust MCS is used to ensure that all nodes can receive such frames. For that reason, *ALIVE* frames are sent as broadcast frames. When interpreting regular data frames as an aggregated *ALIVE* indication, it needs to be ensured, that such frames are sent using an MCS that can be decoded by all receiving nodes.

IV. VALIDATION

The implementation of the monitoring component within our CG-WMAN testbed is a work-in-progress. We have implemented the major components and present initial results confirming TIM delay and loss measurements as well as event creation by *Rating Agents* indicating an under-performing link.

A. Scenario

Our software is built upon our C++ Simple and Extensible Network Framework (SENF)[8] framework which also provides a network emulator supporting the mixed use of emulated and real hardware interfaces. This allows us to evaluate the same source code on emulated nodes, real Linux-based nodes or a combination of both while using proven measurement tools such as *mgen*[7] for validation.

The scenario depicted in Figure 7 consists of four mesh nodes running on a multi-core Linux PC as well as two Linux PCs running *mgen*. The links between nodes A and B and nodes C and D are emulated, while the link between nodes B and C is made up of two real 802.11a interfaces in ad-hoc mode. To verify the TIM measurement results, we have introduced a fixed delay of 5ms and 2ms respectively as well as an average loss of 2% on the emulated links.

Three different flows are sent via separate LSPs, a 64kbps VoIP flow, a 2Mbps video flow and an ICMP flow created by a *flood-ping*.

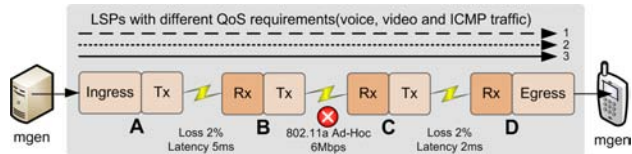


Fig. 7. Three-hop LSPs with different QoS parameters and receiver side monitoring

B. Results

The upper part of Figure 8 depicts the TIM delay measurements of the video LSP obtained at the intermediate MPLS nodes as well as end-to-end, while the lower part depicts the corresponding loss figures. The result for the VoIP and ICMP LSP are similar and have been omitted to avoid cluttering the graph.

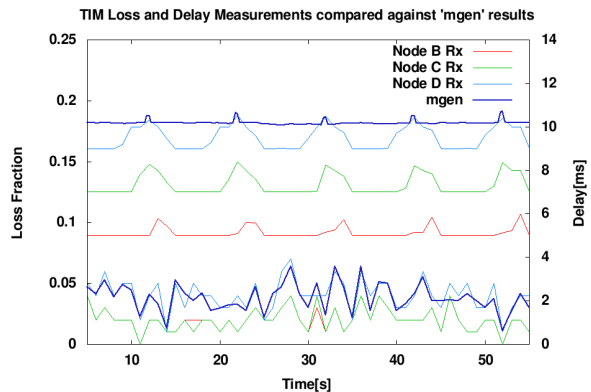


Fig. 8. TIM receiver side measurements at nodes B, C and D compared to end-to-end 'mgen' results

The graph shows that TIM in clock-synchronized mode accurately captures loss and delay introduced by the emulated links AB and CD, as well as a 2ms delay introduced by the almost loss-free 802.11a link. The TIM end-to-end measurements represented by the thin blue lines are confirmed by the *mgen* results represented by the thick blue lines. Note that *mgen* was run on external PCs connected via Ethernet. Hence the average latency measured is slightly higher.

Figure 9 depicts the inactivity per LSP on the 802.11a link. The two thick lines represent the period between the last activity seen and the time when the *Rating Agents* have created inactivity events. Different per-LSP inactivity thresholds have been configured: 100ms for the VoIP flow, 1000 ms for the video flow and 5000ms for the IGMP flow.

After we disabled the 802.11a link at time $t=34s$, the two inactivity events for the Voice-over-IP (VoIP) and the video flow have been triggered after 100ms and 1000ms respectively. We re-enabled the link right after

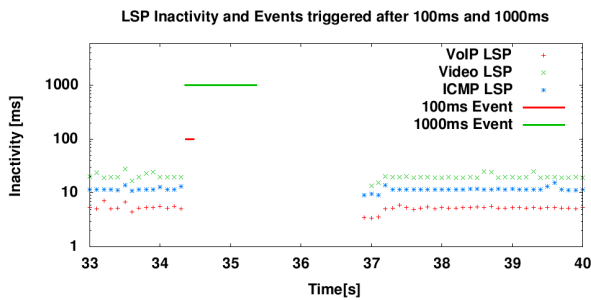


Fig. 9. per-LSP Inactivity and triggered events

these events, and regular activity has resumed after about 3000ms, hence the third event did not get triggered.

C. Performance

In our current prototype implementation the MPLS forwarding module including the monitoring component is executed in user space. All meta information such as the Linux RadioTap header, timestamps and the TIM header is inspected on a per-packet basis and measurement data aggregation is performed. Forwarding packets between two WLAN interfaces is CPU bound and the system can sustain a throughput of about 10 Mbps on a 400MHz embedded AMD Geode system. Using plain kernel space Internet Protocol (IPv4) forwarding or Ethernet bridging the same system can easily saturate the wireless link at about 30Mbps. In both cases, no measurements or aggregations are performed. Existing MPLS implementations neither support multicast forwarding nor FRR and have therefore not been considered. If available, though, kernel space MPLS forwarding should be about as efficient as Ethernet bridging. We're aware of optimization potential in the SENF framework as well as in the measurement and aggregation code. Those optimizations should speed up the user space implementation significantly. Moving the most critical code segments into kernel space should improve the performance even more and might be considered once the overall CG-WMAN architecture design has matured.

V. CONCLUSION AND FUTURE WORK

We have introduced an architecture for technology independent monitoring of LSPs as well as configurable per-LSP event creation. TIM allows for feedback-free monitoring of LSPs in a CG-WMAN. Adaptable *Rating Agents* can create events based on multiple gathered statistics supporting the optimization goals of the overall CG-WMAN management component.

To reduce the overhead introduced by the TIM header, it could only be sent at Poisson distributed intervals, as suggested, for example, in [4]. This could be signaled using one of the experimental bits in the MPLS header, but might complicate tunneling external MPLS traffic.

The *Rating Agents* allow the event creation tasks to be broken down into smaller problems and we will look into

integrating existing more optimized criterion functions for the various events of interest in a CG-WMAN. The potential presence of *Rating Agents* at each hop of an LSP could cause event storms since an incident occurring upstream might cause all downstream *Rating Agents* to trigger similar events. To address this issue we're studying a hierarchical structure among the various *Rating Agents* and a possible optimization of our 802.21++ message transport.

ACKNOWLEDGMENT

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 214994. The views and conclusions contained here are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the CARMEN project or the European Commission.

REFERENCES

- [1] A. H. Asgari, P. Trimintzios, M. Irons, R. Egan, and G. Pavlou. Building quality-of-service monitoring systems for traffic engineering and service management. *J. Netw. Syst. Manage.*, 11(4):399–426, 2003.
- [2] D. Awduche, A. Chiu, A. Elwalid, I. Widjaja, and X. Xiao. Overview and Principles of Internet Traffic Engineering. RFC 3272 (Informational), May 2002. Updated by RFC 5462.
- [3] A. Banchs, N. Bayer, D. Chieng, A. de la Oliva, B. Gloss, M. Kretschmer, S. Murphy, M. Natkaniec, and F. Zdarsky. Carmen: Delivering carrier grade services over wireless mesh networks. In *Proc. IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications PIMRC 2008*, pages 1–6, Sept. 15–18, 2008.
- [4] C. Demichelis and P. Chimento. IP Packet Delay Variation Metric for IP Performance Metrics (IPPM). RFC 3393 (Proposed Standard), Nov. 2002.
- [5] F. Fatemipour and M. H. Yaghmaee. Design and implementation of a monitoring system based on ipfix protocol. In *Proc. Third Advanced International Conference on Telecommunications AICT 2007*, page 22, 2007.
- [6] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil. Proxy Mobile IPv6. RFC 5213 (Proposed Standard), Aug. 2008.
- [7] <http://pf.itd.nrl.navy.mil/mgen/mgen.html>. Accessed 17-jul-2009.
- [8] <http://senf.berlios.de>. Accessed 22-apr-2009.
- [9] S. Jiang, D. He, and J. Rao. A prediction-based link availability estimation for routing metrics in manets. *IEEE/ACM Trans. Netw.*, 13(6):1302–1312, 2005.
- [10] V. Mhatre and K. Papagiannaki. Using smart triggers for improved user performance in 802.11 wireless networks. In *MobiSys '06: Proceedings of the 4th international conference on Mobile systems, applications and services*, pages 246–259, New York, NY, USA, 2006. ACM.
- [11] P. Pan, G. Swallow, and A. Atlas. Fast Reroute Extensions to RSVP-TE for LSP Tunnels. RFC 4090 (Proposed Standard), May 2005.
- [12] J. Quittek, T. Zseby, B. Claise, and S. Zander. Requirements for IP Flow Information Export (IPFIX). RFC 3917 (Informational), Oct. 2004.
- [13] A. Raj and O. C. Ibe. A survey of ip and multiprotocol label switching fast reroute schemes. *Comput. Netw.*, 51(8):1882–1907, 2007.
- [14] M. Rondinone, J. Ansari, J. Riihijärvi, and P. Mähönen. Designing a reliable and stable link quality metric for wireless sensor networks. In *REALWSN '08: Proceedings of the workshop on Real-world wireless sensor networks*, pages 6–10, New York, NY, USA, 2008. ACM.