5G-MLab: Developing a Wireless Reliability Measurement Framework

Matthias Herlich, Thomas Pfeiffenberger, Jia Du, Peter Dorfinger <firstname.lastname@salzburgresearch.at>

***Abstract*—5G, the fifth generation radio access network, is planned to be introduced in the year 2020. With 5G for the first time the emphasis of wireless communication has shifted from high data rates to low latency, scalability, and high reliability. High reliability will allow 5G to be used in safety-critical systems.**

Until now wireless communication has rarely been used for safety-critical communication. In applications such as automated driving, industry 4.0 and smart grids even short losses of the ability to communicate can lead to high costs of repair after accidents, missed production or blackouts. In extreme cases even lives may be at stake. Therefore, it will be necessary to not only trust the network operator to provide high reliability, but to measure and monitor the reliability independently.

The required reliability is usually defined as 99.9% or 99.999%. To detect these small, but important, differences, thousands of measurements are necessary for each location. Additionally, automotive and industrial wireless environments are highly variable in time and space due to moving vehicles and machines. Thus, it is necessary to to make many measurements spread out in space and time. This results in a total number of measurements that is practically impossible to achieve using naive automated measurements. Therefore, no methods have been developed yet that can measure the reliability of wireless communication systems. In this paper we describe how we are developing methods to measure the reliability of wireless communication networks. The goal is to apply the methods to 5G, but the results will be applicable to most other wireless networks (for example IEEE 802.11 WiFi).

First we define two reference scenarios: an automotive and an industrial scenario. The scenarios describe the situations in which we will later demonstrate how our methods measure the reliability of wireless communication. By developing the scenarios with domain experts, we gain insight for which applications reliable communication is most important. This insight allows us to later test and demonstrate the usefulness of our methods in settings where they are most needed.

We develop measurement methods using an incremental approach: (1) Develop a method, (2) test the method, and (3) improve the method or develop a new method. To get an initial feeling how complex the implementation of a measurement method is, we simulate the first steps. Once the initial assessment deems the methods feasible for practice, we implement it in our laboratory setup in later steps. After we refined the methods in the laboratory, we will test how well they perform in the two reference scenarios.

This paper describes our approach to develop methods to measure reliability in wireless systems. Additionally, it provides preliminary results from simulations and laboratory measurements. The methods we will develop using the approach described in this paper will allow measuring and monitoring the reliability of wireless networks. This will increase the trust in wireless communication and thereby allow many visionary uses.

I. Introduction

5G will allow innovative applications and transform industries such as automotive, production, energy, and health. [1] With 5G for the first time wireless communication will not only provide high data rates, but also low latency, scalability, and high reliability.

The reliability of communication will be more important than for example a higher bandwidth in many new use cases for wireless networks. In applications such as automated driving [2], industry 4.0 [3] and smart grids [4] even short losses of the ability to communicate can lead to high costs in form of missed production or blackouts. In extreme cases even lives may be at stake. However, in these extreme cases a single communication failure alone is usually not enough to cause injuries. Still mission critical services usually require a reliability of the wireless communication of at least 99.999%. [1]

Wireless communication has only recently been widely considered for safety-critical communication (in both automotive [5] and industrial scenarios [6]). Moreover, measuring whether a wireless network provides the necessary reliability is complex. Therefore, no methods developed so far can measure the reliability of wireless communication systems.

In future the providers of wireless communication will monitor the reliability of their networks closer. However, it will not be enough to rely on the promise of the providers of networking hardware and infrastructure to provide a reliable service. Independent organizations have to monitor the network to ensure that the network is indeed reliable. This has been standard for safety of vehicles and medical devices and will also be necessary for wireless communication networks.

A. Comparing Wireless and Wired Networks

In the past, transmissions that needed to be reliable used wired networks. Wireless communication has two possible paths to application: First, it can be applied in cases were wired connections are not possible. Second, it can be as reliable as wired connections and replace previously wired connections. Wired connections are usually reliable, but are not 100% reliable. For example, cables break due to mechanical wear. Also, just as wireless networks, wired networks need a given signal-to-noise-ratio to decode transmitted data. If the signal-to-noise ratio is to low, the data cannot be decoded and is lost. Reasons for such a loss can, for example, be thermal noise and interference though badly shielded cables. [7]

Another problem can occur, when network cables have to be connected to moving objects such as robot arms. Here the repeated movement can cause fatigue to the cables and cause them to break.

Last but not least, it is impossible to connect all entities that need to communicate by cables: For example, vehicles

on the road and sensors on rotating machine parts or in sealed containers. In these examples wireless networks are advantageous.

It is easier to provide a reliable network connection using wired networks in most cases, but in future more and more applications will require a reliable wireless communication.

B. Complexity of Multiple Layers

Measuring the quality of a wireless channel is no easy task on its own. However, the end user is not interested in the reliability of the physical channel between two end points. The end user is most likely interested in the reliability on a higher layer, for example, on the IP layer.

The reliability on both layers can be different. For example, even under optimal channels conditions on a shared channel, multiple packets can overlap at the receiver depending on the Medium Access Protocol. Another example is a data packet that has to be delayed due to lower layer transmissions with higher priority (channel state information, keep-alive, time-sync or other background activity). This delay might rarely happen, but if it is long enough to make the packet miss its deadline it will reduce the reliability.

A relatively unreliable physical channel can, however also still serve as basis for a more reliable IP layer, when, for example, packet retransmission is used (assuming the deadline allows for retransmits).

More complexity arises, because effects on multiple layers can interact. For example, a packet is late for delivery, only if it is delayed because of a higher priority transmission *and* it is then lost and has to be retransmitted. As such effects cannot be assumed to be statistically independent, they cannot simply be measured individually and combined analytically. It is necessary to measure all effects and their interactions together.

Companies and projects in the past have focused on the pure physical layer transmission. While this is the most important piece, it is not enough to determine the reliability that an application on a higher layer is exposed to.

C. Goal of the 5G-MLab

The goal of the 5G Measurement Lab (5G-MLab) is to develop methods to measure the reliability of wireless communication networks. The methods we develop will not be specifically designed for 5G, but should work (with adaptions such as setting parameters) on many wireless technologies. However, we focus on 5G as it will become a major platform for reliable communication.

The main problem to determine the reliability is that many measurements are necessary to determine the reliability. Hence, it is necessary to find methods, which can reduce the number of necessary measurements.

II. Defining Reliability

The general concepts for dependable computation and communication are broad as they cover a wide range of applications. [8]

In accordance with RFC 2330 [9] we define **reliability** as the "packet delivery rate between two end points with a given maximum transmission duration". That is, the reliability is the rate with which data packets sent from the source host arrive at the destination host. Additionally, we set out an upper time limit after which data packets are considered lost. In this project we consider transmission on the Internet Protocol (IP) Layer.

Our goal is to measure the reliability as close as possible to the reliability that the user of a technology is experiencing. This includes using end systems that are as close as possible to the systems the end user uses. For example, using high-quality antennas on a measurement system and low-quality antennas in the actually used systems, might reduce reliability and thus give a wrong impression to the end user.

Additionally, we want to make as few assumptions as possible, as each assumption has a chance to be wrong. However, we will consider measurement methods that make assumptions to reduce the complexity of the necessary measurements. In this case it is necessary to check the assumptions in detail and highlight them in the results.

Our focus is on measuring transient non-malicious faults in the wireless channel. However, as these faults can interact with other layers (Hybrid automatic repeat request (HARQ), timing) it might not be enough to consider only the wireless channel. As the IP Layer is the most universal, we consider this as the target of our measurements. However, defining reliability on other layers is also possible. [10]

We consider human introduced faults only in so far as humans change the environment, but we will not consider misconfiguration of devices (neither during initial configuration nor during reconfiguration).

Aviziensis et al. [8] distinguish between availability (readiness for correct service) and reliability (continuity of correct service). We do not consider this distinction, but depending on the resolution our definition of reliability can match either from Aviziensis. The reliability based on packet transmission, as we define it, needs a continuity of correct service for the duration of the packet for a correct transmission. And, thus, fits Aviziensis definition of reliability for a fine-grained view. On a lower time resolution each transmission of a packet only needs correct service at the time of transmission of the packet and continuity of service from one packet to the next is not needed. On this coarse view of time, our definition fits to Aviziensis definition of availability.

For a meaningful definition of reliability over the packet loss rate, it is necessary to define a deadline. There are three reasons for this. Firstly, in many applications, there is an upper limit on the allowed latency of data transmission. For example, a vehicular collision warning that arrives after the collision is no longer able to prevent the collision. Secondly, in order to judge whether a packet is no longer important, an upper limit for a waiting time is required, otherwise it would never be possible to decide whether the packet will arrive later. Thirdly, a definition of reliability is useless without an upper limit for the transmission time since the transmission can be made more reliable by repeated transmissions.

For our definition of reliability a correct transmission is a

binary decision. For example, packets that arrive slightly after the deadline are treated the same as packets that do not arrive at all. Note, that we ignore the latency only for the definition of reliability. In the methods we use to measure the reliability we will also consider methods that exploit latency and other non-binary measures of a packet transmission.

Our definition also does not differentiate between reasons a packet was not received: A packet received and dropped due to incorrect CRC is counted the same as a packet received too late. Additionally, we do not distinguish between packet losses that were detected and silent transmission losses.

In our terminology it is only possible to measure the reliability for past time intervals. However, the measured reliability of the past will be the same for the future as long as all relevant parameters stay the same. The problem lies in determining which parameters are relevant and if they have changed. The only way to be sure no relevant parameter has changed, is to remeasure the reliability directly. This, however, is time-consuming. We will consider methods to measure indicators, which can hint at whether the measured reliability of the past is still valid. For example, if the mean signal-to-noise-ratio of a channel changes, it is no longer possible to assume the environment is similar to the one measured earlier. Thus, it is no longer possible to claim that the system has the same reliability as during earlier measurements.

This project will not consider malicious attacks, for example signal jamming. That is, we will not try to predict the probability of human intervention to intentionally reduce the reliability of the system under test.

We distinguish between two forms of reliability. **Periodic** reliability is the packet delivery rate for a stream of packets sent with a constant sending gap in time between them. The periodic reliability is intended for regular transmissions, for example monitoring a temperature.

Poisson reliability is the packet delivery rate for a stream of packets that are generated by a Poisson process [11]. That is, packet transmissions are randomly and independently placed in a given time interval. This is equivalent to the time between two consecutive packet transmission being exponentially distributed. The Poisson reliability is intended for event-triggered transmissions, for example a notification if a temperature crosses a threshold.

Theoretically both types of reliability can be different. For example, a periodic process in a lower layer can lead to delaying of all packets of a periodic stream when the higher layer process period is a multiple of the lower layer process.

Figure 1 illustrates how the latency of consecutive packets with constant intervals can depend on each other. That is, the probability that transmission n collides with another transmission is not independent of the probability that transmission $n+1$ collides with another transmission. Thus, the reliability of a stream of packets can depend on the offset from an arbitrary reference time. However, when averaged over all possible offsets the periodic reliability will be the same as Poisson reliability.

If at least one of the processes is Poisson the probability for two packets to interfere will be independent of the interference of earlier packets. Whether this difference is relevant in practice, and thus, both measures of reliability lead to different results will have to be tested in real measurements.

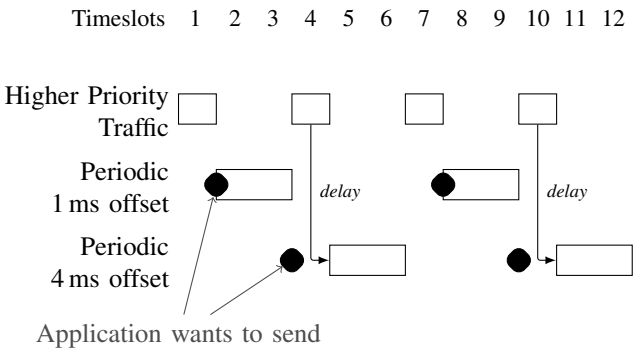

Figure 1. When a periodic process generates packets, the latencies of packets with the same offset are not independent of each other. When averaged over offsets, the probability for a given latency is the same as using a Poisson process. A higher priority transmission can, for example, contain channel state information.

III. Reference Scenarios

To evaluate the measurement methods we develop in the 5G-MLab, we will define two reference scenarios. The goal of the scenarios is to represent the most important scenarios in which reliable wireless communication is needed in the future.

A. Automotive

Future cars will be able to communicate with their surroundings by wireless transmissions. Cars will announce their position, speed, and intention to other cars. A red light will inform approaching cars when it is going to turn green, so the cars can adapt their speed for passenger comfort and efficiency. [2]

This information can be used in cars of different automation levels: it can be displayed to the driver of the car, it can be used by driver assistance systems, and it can be used by fully automated cars. While the benefit of Car-to-Car communication is expected to be greater the more automated traffic becomes, it is also of benefit to human-controlled cars. The biggest challenge in vehicular communication is to achieve reliable wireless communication in the harsh environment [12], [13] inside and outside of vehicles. [14]

Cars will probably not depend on wireless communication for their operation in the near future. This will limit its use to mostly non-safety-critical applications. However, wireless transmission can still increase passenger comfort and efficiency. In the long run, when communication will be necessary for advanced driving features, the reliability will become more important.

To gain most benefits from wireless transmissions the communication must be reliable. For many use cases of wireless communication in the automotive sector the reliability of the wireless transmission is needed to be at least 99.999%. [2]

We are in contact with researchers from the automated driving sector to determine a scenario in which the reliability of wireless transmissions is very important. We will use

this scenario later to evaluate the measurement methods we develop in the project. Examples for such a scenario could be:

- an urban intersection with traffic lights and four lanes on each road,
- a suburban intersection without traffic lights and two lanes per road,
- a section of a highway (either with or without on-ramp or exit).

B. Industrial

A goal of the factories of the future is to be both efficient and flexible. The efficiency will reduce costs. The flexibility will allow adapting to changing demands faster and to highly customize products (lot size one). [15] To achieve this vision both products and machines will need to communicate. With many moving parts it is generally more efficient to use wireless communication. However, an environment with many moving metal machines, is challenging for wireless transmissions.

To develop measurement methods for the reliability of wireless transmissions that are practical useful, we are in contact with machine producers and factory operators. The goal is to determine a reference scenario for industrial communication in which we can evaluate the measurement methods we develop.

IV. Evaluation of Methods

To develop measurement methods for the reliability of wireless networks, we use a cyclic approach shown in Figure 2. We aim to quickly develop measurement methods, which can then be evaluated in setups of increasing complexity and realism.

The setup consists of the selection of the used technology and the environment. The technology selection will use state-of-the-art technologies in the beginning, due to their availability. As soon as more advanced technologies (for example, prototypes of 5G hardware) become available we will switch to those.

The selection of the environment will choose between simulation, lab measurements and real-world measurements.

A. Simulation

The goal of the simulation is to collect experience with the implementation of measurement methods as quickly as possible. This includes data collection, analysis of the measured data, and testing scripts and mathematical tools on simulated results.

We will not use the results of the simulation to determine how reliable a technology is in a given scenario as most simulation models are built to represent the average cases and not the extreme cases that lead to packet loss in rare situations. Thus, we treat the simulation only as a tool to generate lots of data to feed into our measurement tools to determine how well they behave. For example, to determine if the mathematical methods we use, can efficiently handle the number of necessary measurements. Additionally, the simulation will be ideal to quickly change the parameters

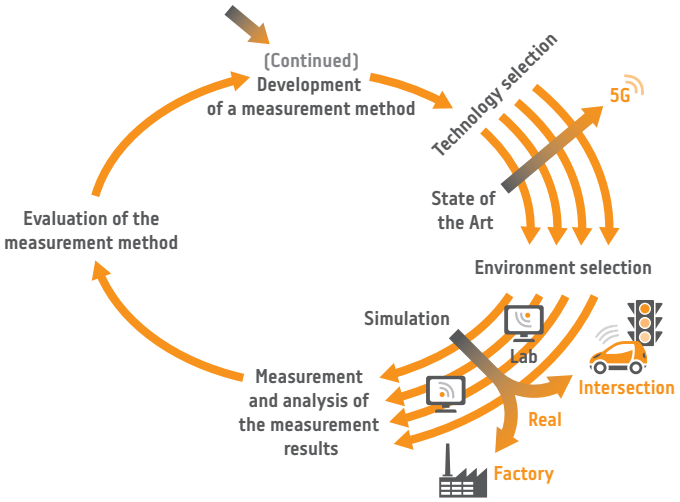

Figure 2. We are using a cyclic approach to develop and evaluate measurement methods. ©Salzburg Research, Fotolia, ecelop

of the measurements (for example, add measurement units, change placement, control movement).

As the goal of the simulation is not to be as realistic as possible, our focus is not to use the latest channel models (such as QuaDRiGa [16]). Instead, we use a multipurpose simulation tool, which covers all layers up to the IP layer.

We selected OMNeT++ 5.1.1 [17][1] as simulation platform. On top of the basic simulator we use the simulte framework [18][2] which depends on the INET framework 3.5.0.[3] For the analysis of the results we use R version 3.2.3 (2015-12-10)[4]. Figure 3 shows a screenshot of the simulation we created based on the SingleCell example from simulte.

We will later publish our source code as open source. However, as the results in this paper are meant to only illustrate our methods, we have not published the source code yet.

B. Lab Measurements

When a measurement method has been sufficiently tested in simulations we will use the same methods (and ideally the same scripts) to gather and analyze data from real hardware in our laboratory.

The goal of this step is to make sure the hardware and measurement scripts are compatible and test whether the algorithms work in principle. While the measurement results provide real results, the reliability we determine in the lab might not be representative of the real-world applications of the technologies. The reason for this is the high number of wireless technology used in office buildings as ours and the lack of large moving machines and vehicles compared to our reference scenarios.

[1] https://omnetpp.org
[2] http://simulte.com
[3] We developed our code based on INET 3.4.0 and OMNeT++ 5.0 first and adapted it as simulte added supported for the newer versions.
[4] https://www.r-project.org

Figure 3. A screenshot of the simulation based on OMNeT++, the INET framework and simulte.

C. Real-world Measurements

To get the most realistic results from our measurement methods we will deploy them in the two reference scenarios described earlier after they have proven feasible in the lab measurements. The goal of the real-world measurements is to determine the reliability of practically relevant scenarios in which wireless communication is applied now or will be applied in the future.

V. Measurement Methods

Our goal is to develop measurements methods and iteratively improve them. Depending on how well the current methods work, we will (in parallel) develop other measurement methods and compare them. This section gives an overview of the first basic ideas we are currently considering.

A. Stationary Measurements

The simplest category of measurements is to use only stationary measurement points. This is easier both in the technical implementation of the measurement and in the analysis. However, it can provide only limited information about other locations, which have not been measured. Note that in the simulation we let even stationary measurement points make small movements (circular movement with 1 cm radius), because stationary nodes have an unrealistic constant Signal-to-Noise-Ratio in the simulation environment we use.

To illustrate the methods described in this paper we use an artificial scenario based on the SingleCell simulation from simulte (see Figure 3). A single user equipment is at a distance of 100 m from a base station. It sends UDP payloads of 8 Byte to a server over the mobile network with exponentially distributed intervals with an average of 10 ms. A packet that arrives at the server not later than 100 ms after it was sent is counted as received. Packets received later are discarded. We simulate the network for 1000 s and then analyze the results.

1) Direct Measurement Method: The direct method to determine the reliability is to count arrived packets a and sent packets s. The ratio $\frac{a}{s}$ is a point estimate of the reliability. However, this point estimate is not informative, especially if all sent packets arrive and thus the reliability is estimated as 100% independent of the number of sent packets.

A more informative estimate is the (95%) binomial proportion confidence interval for the reliability. [19] It determines a confidence interval for the success of a repeated experiment with only two outcomes (success and failure). In our case these two outcomes are "packets received" and "packet not received". To determine the reliability the lower bound of the confidence interval is usually more interesting than the upper bound.

There are multiple ways to calculate such a binomial proportion confidence interval. We will not describe the advantages and disadvantages of each of them, but it is necessary to select a way that holds for asymmetric proportions. Because the reliability we will analyze is mostly close to 1, the estimation should not perform badly in this region. Thus, interval estimators based on a normal approximation of the binomial distribution are not useful. We use the Clopper–Pearson method (also known as the exact binomial test). Other methods exist, but we have not evaluated them for use in this project.

A quick estimate for the lower bound of the 95% confidence interval with only successes is the rule of three [20]. With n successes during n experiments, the lower bound for the 95% confidence interval is $1-\frac{3}{n}$. For example, with 300 successful measurements the lower bound for the 95% confidence intervals is $1-\frac{3}{300}=99\%$.

In our example from 100117 sent packets a total of 99587 were received. That results in a 95% confidence interval of $[0.9942371, 0.9951463]$.

We measured the reliability for exponentially distributed inter-packet times. This is representative for packets, which are sent based on external events, which have the same probability to occur at each time in the interval. However, if the network has state that depends on the past this might change the results. For example, the network might keep awake during frequent measurements, but might go to sleep and take longer to wake up during productive use (when fewer packets are sent).

To determine the reliability in a practical setup the standard Linux `ping` tool[5] defined in RFC792 [21] is not enough. First, it can only set the timeout (using the `-W` parameter) to integer values in seconds. It might be possible to fix this problem, but the second problem is more fundamental. Second, a ping measures a round-trip and, thus, a packet has to travel over the wireless link two times (once up and once down). A better approach is to use the one-way delay as defined in the IP Performance Metrics (IPPM) in RFC7679 [22].

In a first basic test in our lab we transmitted 10 000 packets over a WiFi Link. All packets were successfully received. Using the exact binomial test implemented in `R` as `binom.test(a,b)` this gives a 95% confidence interval

[5]https://sourceforge.net/projects/iputils/

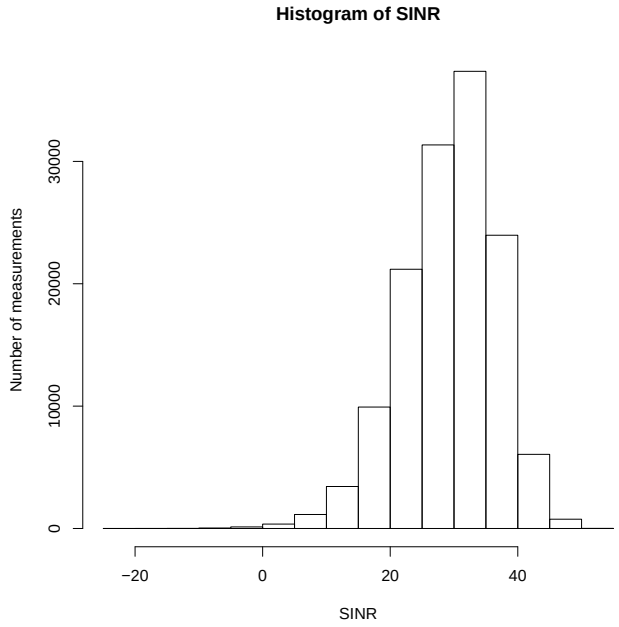

Figure 4. The histogram of the signal-to-noise-ratio of all *received* PDUs on the Physical layer of the base station could provide information that can be used to determine the reliability of the wireless link. In this case SINR equals SNR as no interference exists in the simulation.

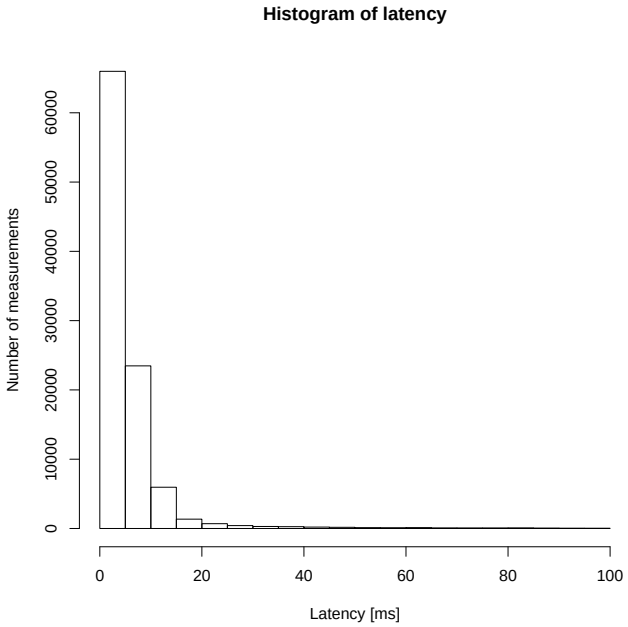

Figure 5. The histogram of all *received* packets at the server on the physical layer of the base station shows that the latency of packets is small most of the time. Some packets arrive with a high latency, but so few that they cannot be seen in the histogram (see Table II)

Table I
SUMMARY OF THE SINRS OF RECEIVED PDUS

	Min.	1st Qu.	Median	Mean	3rd Qu.	Max.
SINR	-20.10	24.58	30.04	29.26	34.56	50.61

Table II
SUMMARY OF THE LATENCY OF RECEIVED PACKETS

	Min.	1st Qu.	Median	Mean	3rd Qu.	Max.
Latency [ms]	4.00	4.38	4.76	6.60	5.57	99.74

for the reliability of $[0.99963, 1.00000]$. All following measurement methods have only been run in the simulation at the moment.

2) SINR Distribution: The direct measurement receives only a single bit of information about every transmitted packet (received or not received). The signal-to-interference-plus-noise ratio (SINR) provides more information. This information could be used to reduce the number of packets to determine the reliability or increase the precision of the reliability calculation with the same number of measurements. This method will however, only be able to detect reduced reliability from a low SINR. Thus, it alone cannot prove that the reliability is high, because it does not account for other reasons for packet loss.

Intuitively, the packet-loss probability is low when the average SINR is high and the packet-loss probability is high when the SINR is low. Thus, it might be possible to estimate the reliability when not even a single packet is lost.

We collected the SINRs of all Protocol data units (PDUs) sent in the simulation. Figure 4 shows a histogram of all *received* PDUs. Table I shows the summary of the recorded SINRs. In the simulation there is no single cut-off SINR for a packet to be received, but the probability of packet loss increases with lower SINR. In the future we will analyze how well the SINR can be used to determine the reliability. The most important question is how well this works in reality and not in the simulation, because the simulation models are usually optimized for average cases and not rare cases that are important to determine reliability.

3) Latency Distribution: A failed transmission from a low SINR usually leads to a retransmission. As long as the retransmission is successful and the deadline for the packet has not been reached the packet is not lost. Hence, the distribution of the latency of received packets also contains more information about the reliability than just the received/not-received distinction. Intuitively, packets that arrive long before the deadline have a lower probability to arrive late and thus the connection has a higher reliability.

Figure 5 shows the histogram of the latency of the received packets. Table II provides a summary of the same data. Note that also packets with latency higher than 100 ms were received, but ignored as of our definition of reliability. In general high latency is rare, but does occur due to, for example, transmission failures and retransmits.

The next step is to determine the reliability from the distribution of the latency. Following this we will compare whether using the SINR or the latency determines the reliability with less data. Also possible is to combine both latency and SINR measurements to determine the reliability.

B. Mobile Measurements

Until now, all measurements have been stationary. This is well as long as the location at which the measurements are made is the same as the location of interest. However, in many applications of reliable wireless communication, mobility of the devices is an important asset. Hence, it is necessary to determine the reliability not only for a single location, but for the complete area in which the sender can be.

As long as the device does not move more than the coherence distance, the properties of the wireless environment stay the same. The simplest (but probably very inefficient) way to determine the reliability for a given area is to split the area in sectors that are smaller than the coherence distance and measure the reliability in each of them. It might be necessary to determine the coherence distance practically and not derive it from theoretical calculations.

More complex but also more efficient methods to determine the reliability could be mobile robots. They could focus measurements of channel quality where it is necessary instead of make the same number of measurements at all locations.

VI. Conclusion

As wireless networks become more wide-spread over time and the dependency on them increases, their reliability should increase, too. In this paper we described how we will develop methods that can determine the reliability of wireless networks. The methods we analyze will be based on stationary and mobile measurement devices and analyze data such as SINR and latency. The algorithms we develop will help to determine where wireless networks are reliable and can be depended upon.

Acknowledgments: The 5G-MLab is funded by the Austrian Federal Ministry of Transport, Innovation and Technology (BMVIT) and the Austrian state Salzburg.

References

[1] 5G-PPP, "5G Empowering Vertical Industries," 2016.
[2] 5G-PPP, "5G Automotive Vision," 2015.
[3] 5G-PPP, "5G and the Factories of the Future," 2015.
[4] ——, "5G and Energy," 2015.
[5] F. Bai and H. Krishnan, "Reliability analysis of dsrc wireless communication for vehicle safety applications," in *Intelligent Transportation Systems Conference, 2006. ITSC'06. IEEE*. IEEE, 2006, pp. 355–362.
[6] J. Åkerberg, F. Reichenbach, and M. Björkman, "Enabling safety-critical wireless communication using wirelesshart and profisafe," in *Emerging Technologies and Factory Automation (ETFA), 2010 IEEE Conference on*. IEEE, 2010, pp. 1–8.
[7] P. L. Martin, *Electronic failure analysis handbook: techniques and applications for electronic and electrical packages, components, and assemblies*. McGraw-Hill Professional Publishing, 1999.
[8] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *IEEE transactions on dependable and secure computing*, vol. 1, no. 1, pp. 11–33, 2004.
[9] V. Paxson, G. Almes, J. Mahdavi, and M. Mathis, "Rfc 2330: Framework for ip performance metrics," 1998.
[10] I. Guvenc, S. Gezici, Z. Sahinoglu, and U. C. Kozat, *Reliable communications for short-range wireless systems*. Cambridge University Press, 2011.
[11] J. F. C. Kingman, *Poisson processes*. Wiley Online Library, 1993.
[12] F. Bai, D. D. Stancil, and H. Krishnan, "Toward understanding characteristics of dedicated short range communications (dsrc) from a perspective of vehicular network engineers," in *Proceedings of the sixteenth annual international conference on Mobile computing and networking*. ACM, 2010, pp. 329–340.
[13] C. F. Mecklenbrauker, A. F. Molisch, J. Karedal, F. Tufvesson, A. Paier, L. Bernadó, T. Zemen, O. Klemp, and N. Czink, "Vehicular channel characterization and its implications for wireless system design and performance," *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1189–1212, 2011.
[14] N. Lu, N. Cheng, N. Zhang, X. Shen, and J. W. Mark, "Connected vehicles: Solutions and challenges," *IEEE internet of things journal*, vol. 1, no. 4, pp. 289–299, 2014.
[15] Industrie 4.0 Working Group, "Recommendations for implementing the strategic initiative INDUSTRIE 4.0," 2013.
[16] S. Jaeckel, L. Raschkowski, K. Borner, and L. Thiele, "Quadriga: A 3-d multi-cell channel model with time evolution for enabling virtual field trials," *IEEE Transactions on Antennas and Propagation*, vol. 62, no. 6, pp. 3242–3256, 2014.
[17] A. Varga and R. Hornig, "An overview of the omnet++ simulation environment," in *Proceedings of the 1st international conference on Simulation tools and techniques for communications, networks and systems & workshops*. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2008, p. 60.
[18] A. Virdis, G. Stea, and G. Nardini, "Simulating lte/lte-advanced networks with simulte," in *Simulation and Modeling Methodologies, Technologies and Applications*. Springer, 2015, pp. 83–105.
[19] L. D. Brown, T. T. Cai, and A. DasGupta, "Interval estimation for a binomial proportion," *Statistical science*, pp. 101–117, 2001.
[20] E. Eypasch, R. Lefering, C. Kum, and H. Troidl, "Probability of adverse events that have not yet occurred: a statistical reminder." *BMJ: British Medical Journal*, vol. 311, no. 7005, p. 619, 1995.
[21] J. Postel *et al.*, "Rfc 792: Internet control message protocol," *InterNet Network Working Group*, 1981.
[22] G. Almes, S. Kalidindi, M. Zekauskas, and A. Morton, "Rfc7679: A one-way delay metric for ip performance metrics (ippm)," Tech. Rep., 2016.