Enhanced Radio Access and Data Transmission Procedures Facilitating Industry-Compliant Machine-Type Communications over LTE-Based 5G Networks

Massimo Condoluci[1,2], Mischa Dohler[2,3], *Fellow IEEE*,
Giuseppe Araniti[1], Antonella Molinaro[1], Joachim Sachs[4]

[1]University Mediterranea of Reggio Calabria, Italy
[2]King's College London, UK
[3]Worldsensing, UK & Spain
[4]Ericsson, Sweden

Abstract. Priority alarm messages for machine-type communications (MTC) in industry applications require guaranteed delays of a few dozen milliseconds only, with super-critical applications even calling for below-10ms access. With the best state-of-the-art cellular systems being barely able to meet below 50ms delays, we propose in this paper some important improvements to the 3GPP MTC access procedure allowing to significantly boost performance for alarm messages. Notably, the first method encompasses an SMS (Short Message Service)-like approach where the alarm is transmitted in a secure and backwards-compatible form over the connection-establishing access channel, thus allowing to terminate the data transmission significantly earlier and to support emerging critical alarm messages (CAMs). The second method uses a secure and prior-agreed sequence of random access codes to convey super-critical alerts within a few milliseconds, thus able to support emergency alarm messages (EAMs). Both methods not only achieve control-compliant access delays but are also highly energy efficient, thus allowing for long battery lifetimes and hence quicker uptake by the industry.

1. Introduction

Machine-to-machine (M2M) refers to the paradigm of having machines (sensors, actuators, etc.) connected and communicating without (or with a minimal) human interaction [1]. Apart from autonomous operational requirements, M2M also puts constraints on energy efficiency of battery-powered machines, computational efficiency of low-complexity embedded devices, low cost deployment to facilitate scaling, and low latency to support industry-compliant critical control applications [2].

M2M applications vary enormously [2], examples range from smart cities where sensors report status updates (on, e.g., air quality, parking occupancy, lightening conditions) to health care where sensors report blood pressure, well-being, glucose levels, etc. Other examples are related to the monitoring of industrial sites, pipes, valves, etc.; in this case, access delays of a few milliseconds are desirable to allow closed control-loop applications [2], where e.g. a phasor sensor detects instabilities in the grid requiring parts of a substation to be shunned.

Traditionally, these industrial control applications were powered by wired M2M solutions (e.g., field buses and Industrial Ethernet). Then, with the ratification of e.g. WirelessHART and ISA100.11a, low power wireless solutions started to be used in the industry. Whilst offering long lifetimes, these solutions fall short in range due to low transmission powers. This requires mesh networks to be used, which, even with the best design available today, seriously jeopardize end-to-end reliability and delay [3].

The third Generation Partnership Project (3GPP) machine-type communications (MTC) potentially circumvent these problems, where a viable cellular M2M solution ought to be of low complexity, low cost, low energy consumption and short access delays to be of interest to the industrial ecosystem. Various industrial and academic efforts [4][5][6] are thus in place to address these issues. Focus is on the Random Access (RA) in the uplink of the machine which dictates energy consumption, delay, and complexity. To date, the evolutionary approaches (among them, e.g., the prioritized random access [7]) are generally 3GPP backwards compatible but not able to go below 50ms [8]. The revolutionary approaches (e.g., [9]), on the other hand, meet the industrial delay requirements but are not backwards compatible or they are based on assumptions that limit their effectiveness in real-world settings (e.g., fixed packet size and modulation/coding scheme).

By following the evolutionary path, we introduce in this paper two approaches, largely backwards-compatible with current 3GPP designs and thus pave the way for successful industry-compliant MTC uptake in 5G networks, whose design is expected to be aligned with the large and ubiquitous deployments of Long Term Evolution (LTE) system expected in 2020. The prime design goal is to lower the access delay, which consequently also helps with the energy budget. Both methods allow the standard RA and data transmission procedure, a typical 4-message handshake followed by data transmission over dedicated resources, be terminated quicker. The first method mimics the Short Message Service (SMS) by transmitting encrypted alarms already in the access channel, piggybacked in RA *Msg3*; the second method relies on a secure sequence of preambles to allow the base station (BS, a.k.a. eNodeB) to identify alarm messages almost immediately.

In the remainder of the paper, we describe our proposed methods facilitating critical alarm messages (CAMs) and emergency alarm messages (EAMs); simulation results are also provided. Finally, architectural discussions and conclusions are drown.

2. Critical Alarm Messages (CAMs)

Special classes of MTC applications, with great interest to control industries, deal with critical alarm messages (CAMs) [1][2], i.e., high-priority trigger-based data transmitted by MTC devices (usually fixed) in case of alerts (e.g., overheating, pressure overflow). The design of an effective RA procedure plays a crucial role to fulfill the strict requirements of CAMs: reliability and security/authenticity.

2.1 State-of-the-Art in 3GPP Random Access for MTC

The 3GPP contention-based RA mechanism for small data transmission [10] (left-side hand of Figure 1) consists of a four-message handshake between the MTC User Equipment (UE) and the BS.

The procedure starts with the *Preamble Transmission* (Msg1) on the Physical Random Access Channel (PRACH), a sequence of time-frequency resources (a.k.a. RA slots) the periodicity of which is broadcasted by the BS in the PRACH Configuration Index. In the first available RA slot, the MTC device transmits a preamble randomly chosen within a set of orthogonal pseudo-random preambles. A collision occurs if two or more MTC devices transmit the same preamble in the same RA slot.

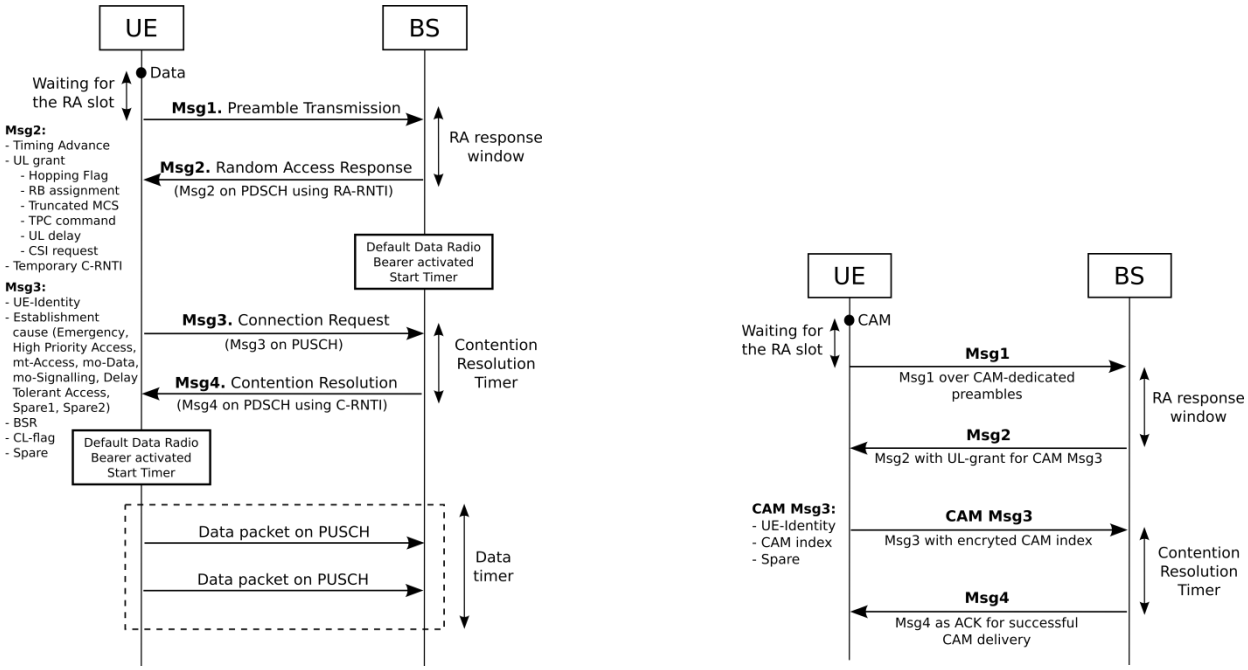

Figure 1. Standard 3GPP RACH-based Small Data Transmission (left) and the proposed SMS-like CAM RACH (right).

If Msg1 is successfully decoded, the BS sends the *Random Access Response* (Msg2) that contains information about the detected preamble and the grant for the transmission of the *Connection Request* (Msg3) on the Physical Uplink Shared Channel (PUSCH). Finally, a *Contention Resolution* message (Msg4) terminates the RA procedure and confirms the grant (according to the buffer state report in Msg3) for the subsequent data transmission on PUSCH.

An undetected Msg1 collision, could also involve a Msg3 collision; each colliding device will retransmit Msg3 until the maximum number of allowed attempts before scheduling a new RA attempt after a random backoff time.

Due to the ALOHA-based preamble transmission and to the use of random backoffs in the case of failure, the RA performance is heavily constrained in the case of delay-constrained access requests from thousands of MTC devices. The attempts to improve the RA performance are not satisfactory in terms of access delays. This inspired us to propose a 3GPP-compliant method which terminates a secure CAM transmission significantly quicker than the 3GPP RACH. Our proposal, namely the *SMS-like CAM RACH*, takes inspiration from the method used to transmit SMSs by exploiting control-plane connections.

2.2 The SMS-like CAM RACH solution: Secure Data in Msg3

The SMS-like CAM-RACH scheme is an enhancement of the RACH-based standard procedure for secure CAM transmission. Our proposal, which is compliant with the 3GPP RA procedure, introduces the following novelties with respect to legacy 3GPP RACH:

- *CAM-dedicated preamble set*. To guarantee low-latency accesses, a subset of preambles is reserved to CAMs.
- *Pre-defined CAM types.* To reduce the overhead, the network defines different CAM types; the MTC device only transmits the *index* of the relevant CAM, instead of the whole data packet. This saves time, network, and battery resources.
- *CAM Msg3*. The legacy Msg3's reserved bits are used to convey the encrypted MTC device

identity and the CAM index.

In the proposed solution, the eNodeB first broadcasts the information about the CAM-dedicated preamble set and the pre-defined CAM types. When a device has to transmit a CAM, it sends a randomly selected CAM-dedicated preamble (right-side hand of Figure 1). By receiving a CAM-dedicated preamble, the eNodeB is aware of the incoming CAM and sends in Msg2 the grant for the new defined *CAM Msg3*, which contains the CAM index encrypted with the device's personal key, to guarantee security and authentication[1].

Once Msg3 is received, the eNodeB uses the transmitting device's key to derive the CAM type. The procedure is then terminated with the Msg4 (uplink grants are not assigned since the alarm was already notified in the CAM Msg3). If the MTC device detects a CAM RACH failure, it schedules a novel procedure after a backoff period of 10ms.

It is fair to assume a negligible preamble collision rate for CAM-related MTC devices: by assuming 10 devices transmitting CAMs in an interval of 100ms and a RACH periodicity of 5ms, we obtain a CAM transmission every two RA opportunities, i.e., the collision probability per RA slot is negligible even when few preambles are reserved for CAM RACH.

Upon receiving the alarm type notification with CAM Msg3, the BS directly transmits the predefined CAM to the final destination (e.g., remote server, actuator). The address translation is achieved through the cloud-based radio access network (RAN) according to the identity of the transmitting MTC device and the CAM type.

2.3 Simulations & Discussion

An analysis of the proposed **encrypted CAM transmission** in the CAM-RACH scheme is reported here to assess the achievement of: *(i)* **low-latency** CAM delivery; *(ii)* **reduced energy consumption**; *(iii)* **no negative impact** on non-CAMs.

The simulation campaign has been carried out through a 3GPP-calibrated 5MHz TDD simulator; cell layout, channel model, and power levels are set according to [8][9][10][11]. MTC devices are located in the central cell of our scenario, while neighboring cells (with background full-buffer traffic so as to act as interfering cells) are located with an inter-site distance of 500m (macro-cell case 1 in [11]).

We analyze two scenarios: *Case A*, where MTC devices are attached to a macro BS (macro-cell system parameters are set in accordance to [11]); *Case B*, where a small-cell handles MTC traffic. This latter case is a further innovative proposal to manage machines located in challenging positions by using different 3GPP small-cell solutions [5]. We consider a small-cell deployed through one femto-cell (with system parameters set as in [5]).

We address a typical industrial scenario, where indoor MTC devices (UE settings in accordance to [11]) are located in a restricted area (50x50m), with a mean distance from the macro BS equal to 300m; all devices are in the femto-cell coverage area. We consider a frequency-separated [13] deployment (2GHz for macro BS and 3GHz for femto-cell) to avoid inter-cell interference; interfering femto-cells are not considered in our simulations (in multi femto-cell deployment, interference can be mitigated by proposals in literature as [15]).

[1] The MTC device derives the 128bit-long security key, K_{CLT} [4][10], through a *nonce* generated by the Mobility Management Entity (MME). The eNodeB requests the MME to derive and pass the K_{CLT} by providing a token sent the by device with the first data transmission.

Ten randomly chosen terminals transmit CAMs, while the other MTC devices transmit one 200 bytes long data message [10][11]. Arrival rates of non-CAM devices are uniformly distributed over 20s. Within this interval, the arrival rates of CAM-related devices are uniformly distributed over 100ms. The PRACH periodicity is set to 5ms (PRACH configuration index 6) [10][11], other PRACH parameters are set as in [9]; 5 CAM-dedicated preambles are reserved among the 54 contention-based ones. Finally, the CAM index is composed by 8 bits while the legacy CAM size is 128 bits.
Simulation results are shown in Figure 2 when increasing the MTC load. The delay (left-hand plot) between the CAM generation at the MTC device and its reception by the BS increases with the number of MTC devices due to the higher RA congestion. In Case A (i.e., macro BS), the delay increases up to 500ms by considering 15k devices, then it grows up to about 14s and 13s for the 3GPP and CAM-RACH schemes, respectively. This increase for the CAM-RACH procedure is given by the PUSCH overload in scenarios with large number of MTC devices. For Case A, the proposed CAM-RACH guarantees a delay reduction from 10% (at high load) to 50% (at low load).

The use of small-cells (i.e., Case B) introduces meaningful delay saving compared to Case A due to the short distance (up to 25m) between the femto-cell and the MTC devices: the higher signal-to-interference-plus-noise ratio (SINR) increases the probability of a successful preamble reception at the first attempt (on the contrary, further retransmissions are necessary to overcome the limitation of higher interference in macro-cell scenarios). In detail, our CAM-RACH achieves a delay equal to 20ms up to 15k devices, then it grows up to 500ms in the heavy load of 30k terminals. The delay reduction w.r.t. the 3GPP RACH ranges from 50% (at high load) to 70% (at low load), thus testifying once more the effectiveness of the proposed solution for low-latency CAM transmission.

The energy consumption is analyzed in Figure 2 (right-hand plot). The proposed CAM-RACH saves the device's (LTE class 3 UE, 23dBm maximum transmission power [8][9]) battery by reducing the period spent in transmitter, receiver and fine clock states. Further energy reduction is obtained in Case B, where the short distance between femto-cell and MTC devices limits preamble retransmissions compared to the macro-cell case. In the heavy load scenario with 30k MTC devices, our proposed CAM-RACH in Case B guarantees an energy reduction close to 95% compared to Case A of 3GPP RACH.

We further consider the impact of having CAM-dedicated preambles on non-CAM MTC traffic. In our analysis (five out of 54 preambles reserved for CAM-RACH), the delay of non-CAM MTC traffic is only influenced by a factor of less than 6% in the worst-case scenario (i.e., 30k devices). This result underlines that the proposed CAM-RACH procedure can effectively handle low-latency CAM transmission without significant impacting the performance of other MTC devices.

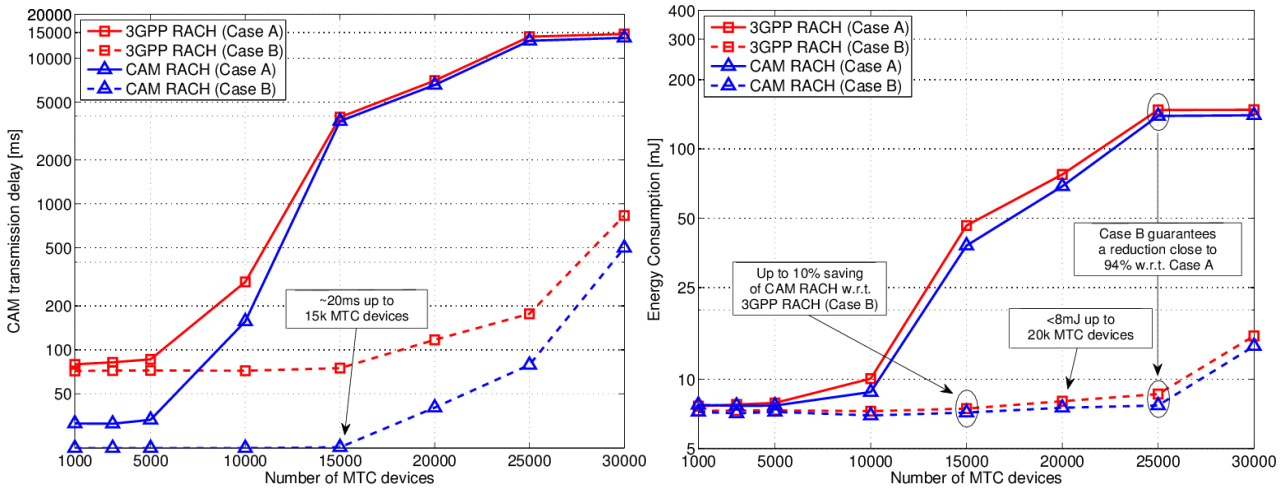

Figure 2. Performance of CAM RACH vs. 3GPP RACH-based data transmission. CAM transmission delay (left) and energy consumption (right).

3. Emergency Alarm Messages (EAMs)

Another big challenge for cellular network providers comes from the management of emergency alarm messages (EAMs) [1][2], which carry trigger-based alerts (usually sent by fixed sensors) requiring immediate action (for instance, to solve industry chain instabilities) and have more stringent delay requirements (expected to be about a few milliseconds) than CAMs. Solving this issue would enable the design of effective industrial MTC business models. With this aim, we propose a novel 3GPP-compliant RA mechanism that exploits secure sequence of access preambles, generated according to the device's cyphering key for EAM transmission.

3.1 State-of-the-Art in 3GPP Preambles

Preambles are orthogonal codes which allow multiple devices to start the RA procedure. Since the available preambles are limited, collisions occur when a massive number of terminals accesses the network in the same RA slot. Therefore, research studies mainly focus on increasing the number of devices that successfully complete the RA. Among those, in [12] is proposed a *code-expanded* RA scheme that significantly increases the amount of contention resources without requiring additional preambles: this is accomplished by using access codewords (i.e., MTC devices transmit orthogonal preambles in a group of consecutive RA slots) instead of a single preamble, and the RA capacity increases due to the availability of a larger codeword set compared to the legacy 3GPP RACH.

In this paper, we extend the idea in [12] by associating the EAM transmission to a secure access sequence of L preambles. In this way, an MTC device just needs to transmit its own access sequence to transfer the EAM to the BS, without any data transmission on the PUSCH, with a consequent drastic delivery delay and energy consumption reductions.

3.2 The EAM-RACH solution: Secure Data in Msg1

The *EAM-RACH procedure* is designed for EAM transmissions with a very low-latency and energy consumption through a 3GPP-compliant *two-message handshake* between the device and the BS. The proposed solution is based on the novel idea of delivering EAMs through an **authorized sequence of access preambles**, generated based on the device's private key. The main novelties of the EAM-RACH are:

- The adoption of *RACH configuration index #14* (PRACH periodicity of 1ms) to allow a quicker preamble transmission. Techniques such as the *dynamic TDD* [13] can be used to

dynamically change the PRACH configuration when, based on some target values measured by sensors, the probability of having an EAM transmission increases.

- The use of an ***EAM preamble sequence s***, generated through a hash function *H* according to the device's key K_{CLT} and – if added security is needed – a timestamp *t* [14]. The generated sequence is composed of *L* different preambles chosen from those (already) reserved for non-contention based access.
- The use of a constantly updated ***hash table HT*** at the BS to store the mapping between a given preamble sequence and the related UE-identity. The frequency of HT update increases if the timestamp *t* is used with the hash function.

The EAM-RACH scheme works as follows (Figure 3). The BS stores in the *HT* the sequence of each device associated to its cell. When an MTC device has to send an EAM, it consecutively transmits in the next *L* RA slots the preambles in the access sequence *s*. When a sequence of *L* different preambles is received, the BS performs the authentication check by comparing it with the *HT*. In the case of success, it means that the access sequence was transmitted by an authorized MTC device with a given probability *p* (refer to the following of this section for more details), and the BS transmits the Msg2 to the temporary address relevant to the last preamble in the sequence. If the device receives Msg2 within the waiting window, it declares the EAM success; otherwise a new EAM-RACH procedure is scheduled after a backoff interval of 10ms. Once an EAM reception (or several unauthorized attempts), the security keys ought to be updated for security reasons.

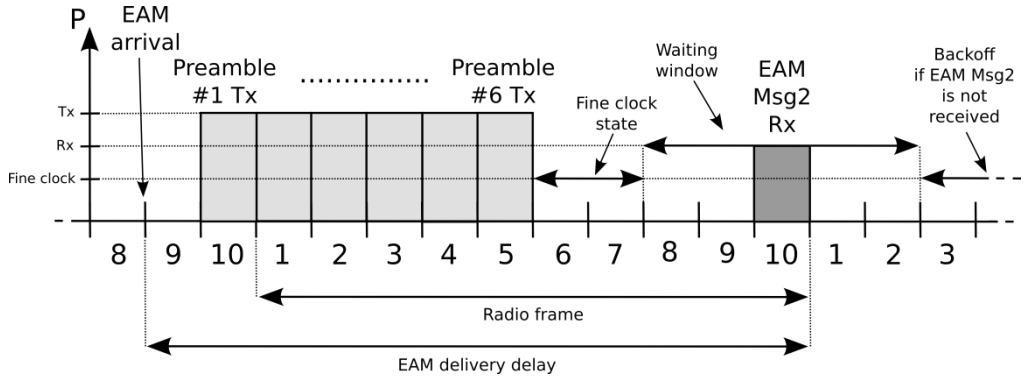

Figure 3. Time diagram designed for our proposed EAM-RACH procedure (preamble sequence length *L*= 6).

3.3 Simulations & Discussion

A simulation campaign has been carried out to assess the expected benefits of our proposed EAM-RACH. The same simulation settings reported in Section 2.3 are used, except for the RACH configuration index; we considered 10 preambles for non-contention based access and a preamble sequence length *L* equal to 6 (this setting guarantees an adequate trade-off between security and transmission delay; lower length values decrease the security of EAM-RACH while higher length values increase the transmission delay without significantly increasing the security). Finally, we consider that only one MTC device transmits EAMs in the whole simulation period.

We compared the access delay of the proposed EAM-RACH scheme with the 3GPP- and CAM-RACH procedures (Figure 4).

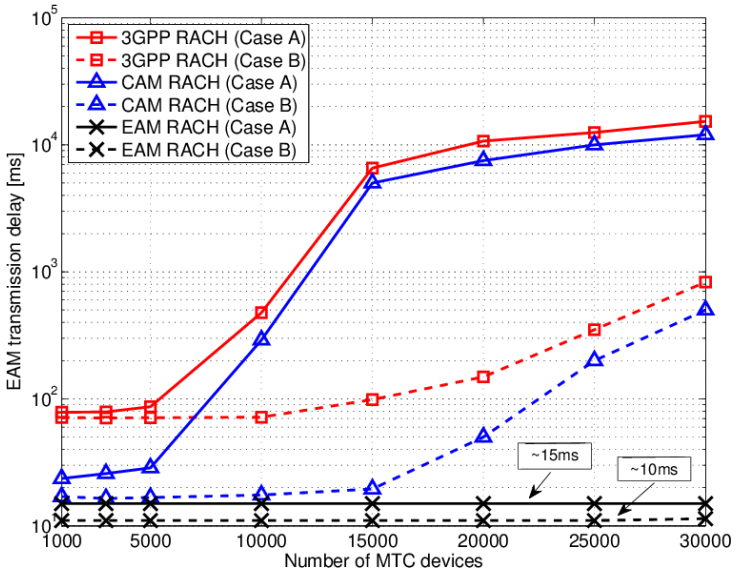

Figure 4. Transmission delay of EAMs by varying the MTC load.

The results of 3GPP and CAM-RACH schemes in Case A (macro cell scenario) and in Case B (small-cell scenario) are similar to those in Figure 2. Indeed, since the 3GPP RACH does not offer priority differentiation, EAMs experience delay values equal to those in Figure 2. Concerning the CAM-RACH, the PUSCH overload in case of huge MTC load influences the EAM delivery delay in a similar trend as for the CAM analysis. In detail, the performance drastically deteriorates when the number of MTC devices is larger than 5k and 15k for Case A and B, respectively. The novel EAM-RACH scheme, which does not require any PUSCH resource, guarantees the lowest delay. In case of success at the first attempt, the EAM transmission takes approximately 10ms (in both Cases A and B). In case of failure, an additional delay (up to 26ms in the worst case) is introduced for every EAM sequence retransmission. In Case A, as devices are located indoor at the cell-edge, the larger coupling losses decrease the SINR and, as a result, the decoding probability of the first EAM sequence is only 80% (so, the success probability per preamble is close to 96%). This leads to an average EAM delay of 15ms caused by occasional retransmission in the macro-cell. As also stated in [5], the use of small-cells (Case B) leads to small coupling losses and more than 99% decoding probability of the EAM preamble sequence. This results in a low average delay of about 10ms.

It is also worth noticing that the delay for the EAM-RACH scheme, which exploits a code-expanded approach to reduce the access collision probability and does not exploit PUSCH resources, is not influenced by the MTC load in the cell. This demonstrates that the proposed mechanism is able to fulfill the delay requirements of critical EAMs without performance degradation for high traffic load.

We now analyze the security issues of the proposed EAM-RACH method to demonstrate its robustness. There are three possible ways for an intruder to transmit an authorized preamble sequence:

- *Generate an authorized key K_{CLT}:* The intruder can derive an allowed preamble sequence if it generates the key of a trusted MTC device. With a 128-bit key, the probability p to generate an authorized key is inversely proportional to the overall number of possible 128-long keys. This probability is thus very low (for instance, order of magnitude of 10^{-35} for 30k devices).

- *Generate a random preamble sequence:* If the intruder tries to randomly generate an authorized preamble sequence, the probability of achieving an allowed sequence is $p=n \cdot \frac{1}{10} \cdot \frac{1}{9} \cdot \ldots \cdot \frac{1}{5}$ (where n is the number of EAM-related devices associated to the BS), thus fairly low. As additional protection, furthermore, the system ought to rekey in the case of detected unauthorized attempt(s).
- *Exploiting a hash collision:* The intruder could generate an allowed access sequence from a non-trusted key (i.e., hash collision). By assuming that the hash function H distributes hash values evenly across the available range of preamble sequences, the hash collision probability, given n authorized MTC devices plus one intruder and N admissible preamble sequences, is $p = 1 - \frac{N-1}{N} \cdot \frac{N-2}{N} \cdot \ldots \cdot \frac{N-(n+1)+1}{N}$, where $N=1.512 \cdot 10^5$ in our scenario. Again, the probability is reasonably low.

4. Architectural challenges

The proposed access schemes with the joint use of small-cells [5] also call for architectural improvements to allow signaling and network overload reduction by avoiding the transmission of full IP headers. An example of the enhanced architecture is illustrated in **Error! Reference source not found.**, where small-cells are embodied by femto-cells. As motivated by the above simulation results, MTC devices communicate with femto-cells, a.k.a. Home-eNodeBs (HeNBs), which in turn directly exchange control traffic via the *X2* interface. Femto-cells are connected to the 3GPP core network via the HeNB-GW, which concentrates control and data traffic and thus reduces the core network overload by minimizing the number of signaling connections towards the core network also when the number of connected femto-cells is huge. Indeed, this solution exploits only one Stream Control Transmission Protocol (SCTP) association between the HeNB-GW and the core network in the control plane as well as only one GPRS Tunneling Protocol (GTP) connection in the user plane.

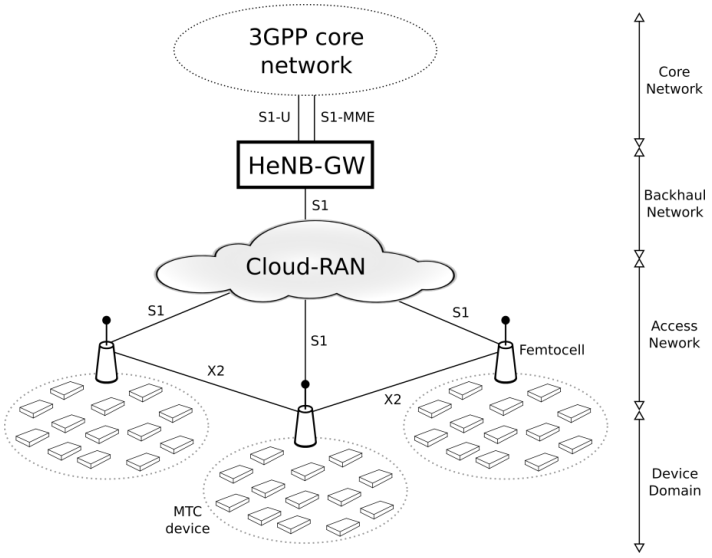

Figure 5. Enhanced cloud-RAN architecture for MTC access via femto-cells to the 3GPP core network.

The use of a cloud-RAN architecture yields several advantages: avoiding the transmission of full robust header compression (ROHC) header in the data packets by storing a Network Address Translation (NAT) list for each MTC device (the cloud-RAN performs NAT procedure by considering the UE-identity of the transmitting device and the data type); avoiding CAM & EAM

data transmission by storing connection-related parameters; allowing dynamic network configuration by tuning the TDD & RA parameterizations according to the traffic measurement monitored by the cloud-RAN; exploiting caching to store and process information for signaling minimization and reliability maximization.
Further solutions are currently under investigation, as [16] where a *flexible* network architecture is proposed allowing to run core network functions at (or close to) the BS sites. Thus, system functionalities can be flexibly allocated to different execution nodes through Software Defined Network (SDN) and Network Functions Virtualization (NFV) approaches.

5. Concluding Remarks

We presented and assessed the effectiveness of two novel RA schemes handling time-critical alarm messages sent by fixed MTC sensors over future cloud-RAN enabled 3GPP networks; their performance characteristics are summarized in Table 1.
Focusing on the CAM transmission, the proposed solution allows significant delay and energy savings by transmitting CAM data in Msg3 of the RA procedure, thus reducing the PUSCH overload and increasing the number of supported devices. Concerning the EAM management, we presented a novel approach where EAM data is directly transmitted through a secure preamble sequence, which allows the BS to quickly identify the EAM without the need of any data transmission by the terminal.
The detailed design and protocol optimization of the cloud-RAN architecture is left for future work.

Table 1. Comparison of the proposed CAM-RACH and EAM-RACH procedures w.r.t. the 3GPP RACH-based small data transmission.

	3GPP RACH	CAM-RACH	EAM-RACH
Delay	• >60ms • < 100ms until 5k devices (Case A) • < 100ms until 15k devices (Case B) • Up to 15s (Case A) • Up to 850ms (Case B)	• >20ms • <100ms until 5k devices (Case A) • ~20ms until 15k devices and <100ms until 25k devices (Case B) • Up to 13s (Case A) • Up to 500ms (Case B)	• ~15ms (Case A) • ~10ms (Case B)
Energy consumption	• Up to 148mJ (Case A) • Up to 15mJ (Case B)	• Up to 140mJ (Case A) • Up to 13mJ (Case B)	• Up to 60mJ (Case A) • Up to 10mJ (Case B)
PUSCH load	• PUSCH used for Msg3 • PUSCH used for data transmission	• PUSCH used only for CAM Msg3	• PUSCH is not used
Control overhead	• High overhead (full RACH procedure and successive data transmission)	• Only CAM RACH procedure (data in Msg3) • Reduced Msg3 size • Reduced Msg4 size	• Only EAM RACH procedure (no EAM data transmission) • Reduced Msg2 size • No Msg3 • No Msg4

References

[1] Woon Hau Chin, Zhong Fan, and R. Haines, "Emerging Technologies and Research Challenges for 5G Wireless Networks," *IEEE Wireless Communications*, vol. 21, no. 2, Apr.

2014, pp. 106-112.
[2] K. Zheng, Suling Ou, J. Alonso-Zarate, M. Dohler, Fei Liu, Hua Zhu, "Challenges of massive access in highly dense LTE-advanced networks with machine-to-machine communications," *IEEE Wireless Communications*, vol. 21, no. 3, Jun. 2014, pp. 12-18.
[3] B. B. Olyaei, J. Pirskanen, O. Raeesi, A. Hazmi, and M. Valkama, "Performance comparison between slotted IEEE 802.15.4 and IEEE 802.11ah in IoT based applications," *IEEE 9th WiMob*, Oct. 2013, pp. 332-337.
[4] 3GPP, TR 37.869, "Study on Enhancements to Machine-Type Communications (MTC) and other Mobile Data Applications; Radio Access Network (RAN) aspects," Rel. 12, Sep. 2013.
[5] M. Condoluci, M. Dohler, G. Araniti, A. Molinaro, K. Zheng, "Towards 5G DenseNets: Architectural Advances For Effective Machine-Type Communications over Femtocells," *IEEE Communications Magazine*, vol. 53, no. 1, Jan. 2015, pp. 134-141.
[6] K. Zheng, F. Hu, W. Wang, W. Xiang, and M. Dohler, "Radio Resource Allocation in LTE-Advanced Cellular Networks with M2M Communications," *IEEE Communications Magazine*, vol. 50, no. 7, Jul. 2012, pp. 184-192.
[7] J.-P. Cheng, C. Han Lee, and T.-M- Lee, "Prioritized Random Access with dynamic access barring for RAN overload in 3GPP LTE-A networks," *IEEE Globecom Workshops*, Dec. 2011, pp. 368-372.
[8] A. Laya, L. Alonso, and J. Alonso-Zarate, "Is the Random Access Channel of LTE and LTE-A Suitable for M2M Communications? A Survey of Alternatives," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, Dec. 2013, pp. 4-16.
[9] S. Andreev, A. Larmo, M. Gerasimenko, V. Petrov, O. Galinina, T. Tirronen, J. Torsner, and Y. Koucheryavy, "Efficient Small Data Access for Machine-Type Communications in LTE," *IEEE International Conference on Communications (ICC)*, Jun. 2013, pp. 3569-3574.
[10] 3GPP, TR 38.868, "RAN Improvements for Machine-type Communications," Rel. 11, Oct. 2011.
[11] 3GPP, TR 25.814, "Physical layer aspect for evolved universal terrestrial radio access (UTRA)," Rel. 7, Sep. 2006.
[12] H. Thomsen, N. K. Pratas, Č. Stefanović, and P. Popovski, "Code-Expanded Radio Access Protocol for M2M Communications," *Transactions on Emerging Telecommunications Technologies*, vol. 24, no. 4, Jun. 2013, pp. 355-365.
[13] D. Astely, E. Dahlman, G. Fodor, S. Parkvall, and J. Sachs, "LTE Release 12 and Beyond," *IEEE Communications Magazine*, vol. 51, no. 7, Jul. 2013, pp. 154-160.
[14] A. Bartoli, J. Hernandez-Serrano, M. Soriano, M. Dohler, A. Kountouris, and D. Barthel, "Secure Lossless Aggregation Over Fading and Shadowing Channels for Smart Grid M2M Networks," *IEEE Transactions on Smart Grid*, vol. 2 , no. 4, Dec. 2011, pp. 844-864.
[15] Yanzan Sun, R.P. Jover, Xiaodong Wang, "Uplink Interference Mitigation for OFDMA Femtocell Networks," *IEEE Transactions on Wireless Communications*, vol. 11, no. 2, Feb. 2012, pp. 614-625.
[16] E. Dahlman, G. Mildh, S. Parkvall, J. Peisa, J. Sachs, Y. Selén, and J. Sköld, "5G Wireless Access - Requirements and Realization," *IEEE Communications Magazine*, vol. 52, no. 12, Dec. 2014, pp. 42-47.