

Addressing Network Interoperability in Hybrid IEEE 802.11s/LTE Smart Grid Communications

Nico Saputro, Kemal Akkaya, and Samet Tonyali
 Department of Electrical and Computer Engineering
 Florida International University
 Miami, Florida 33174
 Email: {nsapu002—kakkaya—stony002}@fiu.edu

Abstract—Ensuring network interoperability when IEEE 802.11s-based NAN and LTE-based WAN is deployed for Smart Grid (SG) Advanced Metering Infrastructure (AMI) poses significant challenges. Besides the QoS mismatch between networks, LTE tunneling mechanism becomes an issue when forwarding downlink traffic to IEEE 802.11s network since the gateway of these networks is supposed to be the end device in LTE setup. Yet, inherent security/privacy overhead in SG traffic makes it even more challenging. To address these issues, a novel UE access list is proposed for LTE network to enable the downlink traffic identification to IEEE 802.11s network and accordingly selects the corresponding gateway. For the QoS mismatch, Dual-Queues (DQs) for each Access Category of the underlying MAC protocol, namely Enhanced Distributed Channel Access (EDCA) in IEEE 802.11s network is proposed. By using ns-3 network simulator, extensive performance evaluations under heavy security overhead are conducted to assess the performance of the proposed mechanisms.

I. INTRODUCTION

A smart meter (SM) in Advanced Metering Infrastructure (AMI) can be used for a variety of activities such as [1]: (1) remote meter reading, (2) remote service switching, (3) tamper detection and notification, (4) outage detection and notification, and (5) voltage and power quality monitoring. Each activity may have different Quality of Service (QoS) requirements (e.g., delay and priority [2]) that can be dynamic based on certain conditions [3]. The heterogeneity of two-way QoS traffic are augmented when security and privacy mechanisms are implemented, in particular on the increase of the data size [4] [5] and additional traffic related to the key management [6].

Typically, a multi-tier communications network that consists of Home Area Network (HAN), Neighborhood Area Network (NAN), and Wide Area Network (WAN) [7] is used for AMI. Each network tier may use different communication technologies. For instance, a hybrid wireless network and Long Term Evolution (LTE) cellular network is widely studied as the NAN and WAN respectively in recent years [8] [9] [10] [11]. However none of them investigated the interoperability issues in these hybrid networks. Typically, they make a straight assumption about the connectivity between network tiers and do not consider the issue of varying QoS supports in each network tier. Therefore, there is a need to investigate the interoperability issues in this hybrid network for ensuring the desired performance.

In this paper, we first pointed out two network interoperability issues when an IEEE 802.11s [12] and LTE cellular network [13] are deployed as the NAN and WAN of AMI network respectively. Then, two proposed approaches to address these issues were discussed and implemented in ns-3 network simulator. Performance evaluation under heavy security traffic overhead was conducted. The simulation results indicate that the proposed approaches can solve these issues without any significant impact on the network performance. However, security overhead may impede the gains in QoS performance.

The rest of the paper is organized as follows. Section II describes the system model and network interoperability problems. Section III describes the proposed approaches. In Section IV, we present the evaluation results. Finally, the paper is concluded in Section V.

II. PRELIMINARIES

A. System Model

An IEEE 802.11s multi-hop wireless mesh network and LTE cellular network are deployed for AMI as the NAN and WAN respectively. Each consumer in a NAN is assumed to have an IEEE 802.11s wireless-based smart meter (SM). A gateway with dual interfaces, namely IEEE 802.11s interface and LTE interface, is used to support bi-directional traffic flow between network tiers. For the NAN, the gateway acts as the Mesh Portal Point and the root node for the tree-based routing of Hybrid Wireless Mesh Protocol (HWMP) [12]. As the root node, the gateway periodically broadcasts proactive path request (PREQ) to create and maintain a logical spanning tree rooted at the gateway. In this way, a path to each SM is always available through the gateway and each SM can reach the gateway in multi-hop fashion through other SMs. For LTE network, this gateway acts as a user equipment (UE) and can communicate with utility company through a base station (i.e., eNB) and an evolved packet core (EPC) network that serves as the LTE gateway to external network (i.e., Internet).

B. Problem Motivation and Definition

Extending the UE as the gateway creates an interoperability issue related to downlink traffic intended to any SM in the IEEE 802.11s network due to the used of unidirectional General Packet Radio Service (GPRS) tunneling protocol

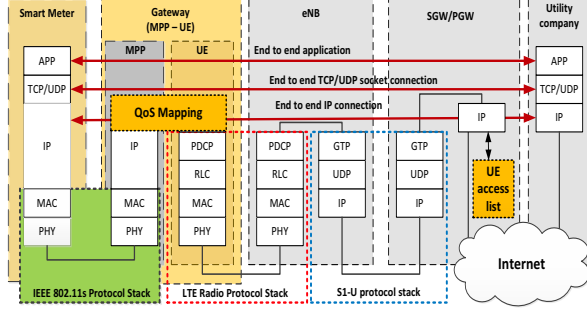


Fig. 1: Proposed Architecture which has an IP access list and a QoS Mapping list.

(GTP) between a base station (i.e., eNB) and the Packet Data Gateway (P-GW) in the EPC access network for packet delivery. For each packet delivery direction (e.g., uplink or downlink), each UE has its own GTP tunnel and this tunnel is uniquely identified using a tunnel identity (TEID). For the downlink traffic, P-GW can find the TEID based on the IP address of the destination UE IP address. When the destination IP in the IP packet is unknown (e.g., the IP address of a SM in the IEEE 802.11s network), P-GW will drop the IP packet since it cannot find the corresponding downlink TEID.

Another interoperability issue is related to the number of QoS classes in each network tier. IEEE 802.11s incorporates IEEE 802.11e standard [14] that supports only four Access Categories (ACs) while LTE supports nine QoS classes. This creates problems when there are many different QoS data flows traveling among these networks. Therefore, in this paper, our goals are twofold: to ensure two-way flow of QoS traffic in SG communications network while providing a flexible QoS mapping between tiers and to devise a new IEEE 802.11s architecture that expands the existing QoS classes to accommodate a wide variety of QoS traffic.

III. THE PROPOSED APPROACHES

Two proposed approaches, namely UE access list and QoS mapping list, are showed in Fig. 1. The UE access list is used for finding the corresponding UE gateway in case of traffic destined to an IEEE 802.11s-based NAN. A UE access list consists of network base address and subnet mask of IEEE 802.11s-based NAN and its corresponding UE gateway IP address that serves this NAN. Instead of discarding a downlink IP packet when the destination IP address is unknown, the P-GW will check the UE access list to see whether this unknown IP address is associated to one of the NANs. The appropriate UE IP address can be retrieved from the UE access list when the IP address is associated to a NAN. The P-GW will use this UE IP address to find the corresponding downlink TEID.

A downlink QoS mapping list at the gateway of the hybrid network is proposed to map downlink QoS traffic from the LTE network to its corresponding QoS class in IEEE 802.11s. Each time the gateway receives a downlink traffic, it will consult this list to determine what would be the appropriate

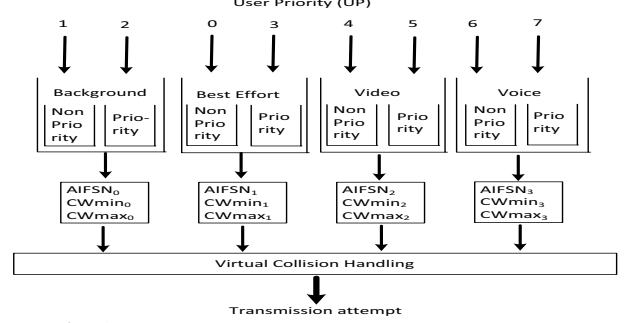


Fig. 2: Proposed EDCA modification with dual queues.

QoS class for the received traffic. This mapping list consists of a pair of quality class identifiers of LTE network and its corresponding QoS class in IEEE 802.11s. When the gateway receives downlink traffic from the LTE network, based on from which bearer this traffic is coming from, the gateway will find the corresponding QoS identifier for IEEE 802.11s in the QoS mapping list. Note that for the uplink traffic from SM(s), the ordinary packet filtering feature at the UE that uses the traffic flow templates to assign the traffic to an appropriate bearer is used.

To address the mismatch between LTE and IEEE 802.11s QoS classes, four ACs in IEEE 802.11s are extended by employing dual queues (DQs), called non-priority and priority queues, for each AC instead of a single queue as defined in IEEE 802.11e standard. The DQs within the same AC have the same EDCA parameters as depicted in Fig. 2. In this way, eight QoS classes will be available in IEEE 802.11s. When an AC has the right to access the medium, the priority queue in this AC will be checked first. When it is not empty, the packet from this priority queue is granted access to the medium. Otherwise, the non-priority queue is given access to the medium.

IV. PERFORMANCE EVALUATION

Three SG applications (outage management system (OMS), grid operations (GO), and demand response (DR)) were used for performance evaluation. Two different encryption mechanisms, AES-128 and Fully Homomorphic Encryption (FHE) [4], were implemented for these applications since the goal is to assess under heavy security/privacy traffic overhead. AES-128 is used for OMS and DR since they do not need any in-network processing while FHE is employed for GO since it needs in-network processing while in-transit. Note that FHE allows computation on encrypted data and is being considered for user privacy in AMI applications. Table I shows the parameters used for each application. The DR is assumed as simple commands to turn on/off appliances and initiated by the utility company to demonstrate the use of UE access list for the downlink traffic delivery to several SMs (e.g., 10% of SMs). These DR commands were sent several time at random. TCP protocol was used for all applications to ensure the reliable data delivery.

The experiments were conducted for varying numbers of SMs. For each node count, 30 random network topologies

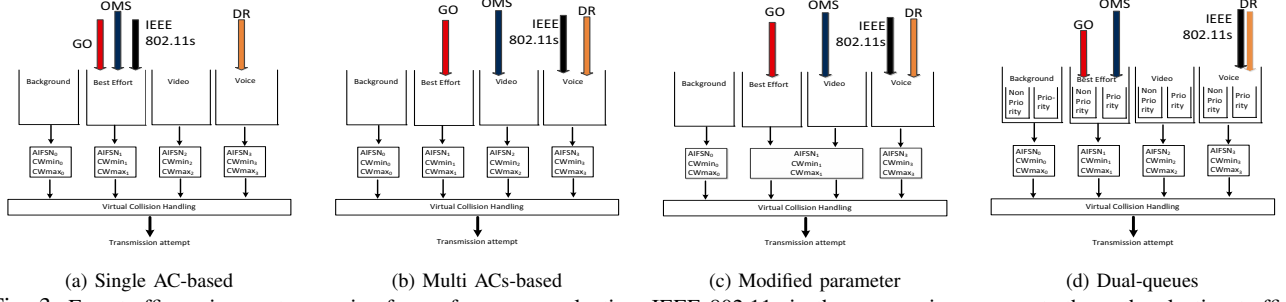


Fig. 3: Four traffic assignment scenarios for performance evaluation. IEEE 802.11s in these scenarios represents the path selection traffic (i.e., HWMP).

TABLE I: SG Applications used for performance evaluation

SG Application	Data size (bytes)		Data sampling	Security
	plaintext	ciphertext		
OMS (from SMs to utility)	64	80	60 secs	AES-128
Grid Operations (GO) (meter usage)	4	12,660	30 secs	FHE
DR (commands to SMs)	4	16	on-demand	AES-128

were created. The end-to-end (ETE) delay and packet delivery ratio (PDR) of each traffic in each network topology were collected. The average of these results for each node count were presented in the graphs. Fig. 3 shows four traffic allocation scenarios for performance evaluation. Fig. 3a shows the baseline where OMS, GO, and IEEE 802.11s traffic are assigned to the best effort AC. The OMS traffic are assumed to have a higher priority than GO traffic. Fig. 3b and Fig. 3c show the same traffic allocations, but instead of different EDCA parameters for every AC, in Fig. 3c best-effort AC and video AC use the same EDCA parameters. We label the OMS and GO traffic in Fig. 3b as OMS-VI and GO-OMS-VI to indicate GO's performance when OMS is using video AC while OMS-VI-mod and GO-OMS-VI-mod for traffic in Fig. 3c. Fig. 3d shows the traffic allocations when DQs are employed. We label the traffic as OMS-DQ-BE-PQ and GO-DQ-BE-NP respectively.

A. Performance Evaluation of Traffic Allocation

Fig. 4 shows some interesting results. When we compare the baseline and OMS-VI, we expect that by assigning to a higher AC and using multiple ACs, a higher PDR and a lower ETE delay can be achieved for OMS traffic. On the contrary, the simulation results show that PDR drops and ETE delay rises as the node count increases. Even worse, the average ETE delay of OMS traffic is higher than that of GO traffic that is assigned to a lower AC.

We speculate that this is due to the traffic characteristics of AMI. Specifically, within the same SM, OMS traffic that has a shorter backoff value than GO traffic may have access to the medium. However, due to the interference from other SMs that transmit GO traffic regularly, that SM will not be able to

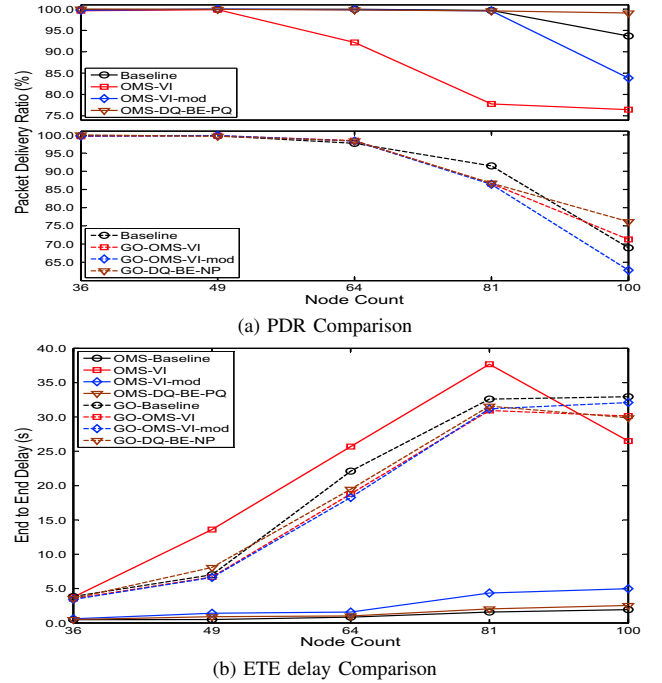


Fig. 4: Performance evaluation of different QoS Class assignments for priority traffic.

transmit since the medium is not idle. As a result, OMS traffic may need to wait even longer (compared to single AC case) in order to access the medium and thus ETE delay increases as shown in Fig. 4. Nevertheless, the PDR for OMS-Baseline is not perfectly high. Therefore, we decided to pursue different means to improve the performance in the case of multiple ACs as detailed next.

1) *EDCA Parameter Tuning*: The above results indicate that the standard EDCA parameters for AC-VI may not be suitable for heavy security overhead traffic. Therefore, tuning the parameters might be an option to improve the performance for such cases. Indeed, when we look at the simulation results for OMS-VI-mod, we can confirm this. Both metrics of OMS-VI-mod are improved significantly when compared to OMS-VI, in particular the ETE delay. Moreover, these improvements

do not have a significant impact on GO traffic. Both PDR and ETE delay of GO-OMS-VI-mod are similar to GO-OMS-VI. However, the results are still short of OMS-Baseline. Further efforts are needed to fine-tune the parameters to improve the performance of the OMS traffic.

2) *Introducing Double Queues:* As mentioned, our proposed approach introduces DQs for each AC. When we compare OMS-VI-mod with our OMS-DQ-BE-PQ approach, we observe that both PDR and ETE delay metrics of OMS-DQ-BE-PQ are better than OMS-VI-mod approach. We attribute this to the fact that when both traffic are present, OMS traffic in DQ approach is guaranteed to have access to the medium first. This is not the case for OMS-VI-mod. Note that in OMS-VI-mod, even though both ACs have the same CW range, the actual CW value selected at a time in each AC may be different due to random CW selection. Moreover, the impact of DQ approach on GO traffic is minimal when compared to OMS-VI-mod. The PDR of GO traffic is even better in DQ approach than that of OMS-VI-mod.

Comparing OMS-DQ-BE-PQ and OMS-Baseline, we see that we were almost able to match ETE values and outperform PDR with respect to OMS-Baseline. Moreover, there is a good performance improvement in GO traffic. The PDR and ETE delay of GO traffic for DQ approach are also outperforming the baseline. Proposed DQs offer flexibility in types of different QoS classes without any additional overhead.

As a result, we can conclude the following: Normally, we expect that multiple queues will be better than single queue carrying all the traffic. However, when we employ FHE, this prevents us achieving improved results with multiple queues. This is because FHE creates a lot of retransmissions which does not leave any space for neighboring SMs to access the medium even if their OMS has a higher priority class. With a single queue, the problem is similar in the sense that FHE traffic dominates the medium. However, with single queue, PDRs are worse which causes to slightly reduce the ETE delay. This is an interesting observation that exposes the impact of security mechanisms on the QoS in the context of AMI applications.

V. CONCLUSION

In this paper, we propose two novel approaches to address network interoperability issues when hybrid IEEE 802.11s / LTE network is used for SG Communications Network. A novel UE access list is used to address the downlink traffic transmission issue from LTE network to the final destination in IEEE 802.11s network. A second approach is the use of DQs to extend the available QoS classes of EDCA from four QoS classes to eight QoS classes. A QoS mapping list is then used at the gateway to map QoS Class Identifiers from the LTE network to these new QoS classes to ensure end-to-end QoS within the hybrid network for the downlink traffic intended to SM(s) in the IEEE 802.11s network.

We implemented and successfully demonstrated the two-way communications in this hybrid network for AMI applications. We also evaluated the performance of DQs compared

to existing alternatives under heavy security/privacy overhead. The evaluations indicated that while DQs can provide flexibility in terms of increased QoS classes and improve performance, their benefits are not obvious when FHE-like security overhead exists.

VI. ACKNOWLEDGEMENT

This work is supported by the US National Science Foundation under the grant number CNS-1550313.

REFERENCES

- [1] "Operations and maintenance saving from advanced metering infrastructure - initial results," *US Department of Energy*, December 2012. [Online]. Available: http://energy.gov/sites/prod/files/AMI_Savings_Dec2012Final.pdf
- [2] J. G. Deshpande, E. Kim, and M. Thottan, "Differentiated services qos in smart grid communication networks," *Bell Labs Technical Journal*, vol. 16, no. 3, pp. 61–81, 2011. [Online]. Available: <http://dx.doi.org/10.1002/bltj.20522>
- [3] K. C. Budka, J. G. Deshpande, T. L. Doumi, M. Madden, and T. Mew, "Communication network architecture and design principles for smart grids," *Bell Labs Technical Journal*, vol. 15, no. 2, pp. 205–227, 2010. [Online]. Available: <http://dx.doi.org/10.1002/bltj.20450>
- [4] S. Tonyali, N. Saputro, and K. Akkaya, "Assessing the feasibility of fully homomorphic encryption for smart grid ami networks," in *Ubiquitous and Future Networks (ICUFN), 2015 Seventh International Conference on*, July 2015, pp. 591–596.
- [5] N. Saputro and K. Akkaya, "Performance evaluation of smart grid data aggregation via homomorphic encryption," in *Wireless Communications and Networking Conference (WCNC), 2012 IEEE*, April 2012, pp. 2945–2950.
- [6] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," *Computer Networks*, vol. 57, no. 5, pp. 1344 – 1371, 2013. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S1389128613000042>
- [7] N. Saputro, K. Akkaya, and S. Uludag, "A survey of routing protocols for smart grid communications," *Comput. Netw.*, vol. 56, no. 11, pp. 2742–2771, Jul. 2012.
- [8] G. Rajalingham, Q.-D. Ho, and T. Le-Ngoc, "Evaluation of an efficient smart grid communication system at the neighbor area level," in *Consumer Communications and Networking Conference (CCNC), 2014 IEEE 11th*, Jan 2014, pp. 426–431.
- [9] J. Markkula and J. Haapola, "Impact of smart grid traffic peak loads on shared LTE network performance," in *Communications (ICC), 2013 IEEE International Conference on*, June 2013, pp. 4046–4051.
- [10] F. Koohifar, N. Saputro, I. Guvenc, and K. Akkaya, "Hybrid wi-fi/lte aggregation architecture for smart meter communications," in *Smart Grid Communications (SmartGridComm), 2015 IEEE International Conference on*, Nov 2015.
- [11] N. Saputro, K. Akkaya, and I. Guvenc, "Privacy-aware communication protocol for hybrid ieee 802.11s/lte smart grid architectures," in *Local Computer Networks Workshops (LCN Workshops), 2015 IEEE 40th Conference on*, Oct 2015, pp. 905–911.
- [12] "Ieee standard for information technology–local and metropolitan area networks–specific requirements part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications amendment 10: Mesh networking," *IEEE Std 802.11s-2011*, pp. 1–372, 10 2011.
- [13] 3GPP. General Packet Radio Access (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (3GPP TS 23.401 version 12.8.0 Release 12). [Online]. Available: http://www.etsi.org/deliver/etsi_ts/123400_123499/123401/12.08.00_ts_123401v120800p.pdf
- [14] "Ieee standard for information technology–local and metropolitan area networks–specific requirements–part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications - amendment 8: Medium access control (mac) quality of service enhancements," *IEEE Std 802.11e-2005 (Amendment to IEEE Std 802.11, 1999 Edition (Reaff 2003))*, pp. 1–212, Nov 2005.