Quality of Service Networking for Smart Grid Distribution Monitoring

Wei Sun*†, Xiaojing Yuan†, Jianping Wang*, Dong Han† and Chongwei Zhang*
*School of Electrical Engineering and Automation, Hefei University of Technology, Hefei, China 230009
†University of Houston, Houston, USA 77004
Email: sw8207@gmail.com,xyuan@central.uh.edu,donny@cs.uh.edu

Abstract—**In order to realize the Smart Grid vision, it is necessary to have guaranteed Quality of Service (QoS) for the communication and networking technology used in various stages of the Smart Grid, ranging from power generation, transmission, distribution, to the customer applications. The low cost wireless protocols such as Zigbee (using IEEE 802.15.4 defined physical and MAC layer) and Bluetooth (IEEE802.15.1) are especially useful for the power distribution system monitoring and customer applications. However, they do not support QoS and typically have a short propagation distance. In this paper, we propose to add the QoS into these low cost protocols by providing differentiated service for traffic of different priority at the MAC layer and use Zigbee as an example. Our analytical delay model and simulation results show that the proposed QoS enhancement can improve the delay and goodput of the network, thus ensuring the reliability, availability, and performance of a Smart Grid distribution monitoring and control.**

I. INTRODUCTION

In the United States and around the world, modernization of the electric power grid is central to national efforts to increase energy efficiency, transition to renewable energy sources, reduce greenhouse gas emissions, and build a sustainable economy that ensures prosperity for current and future generations. An advanced Smart Power Grid for 21st century hinges on successfully adopting, integrating, and advancing existing communication and computing technologies with the power-delivery infrastructure [1], [2]. The core technological challenge to realize the Smart Grid vision is the development of integrated information and communication/networking technologies for monitoring and control of the power devices. The enabled "real time" bi-directional information flow will ensure quick response to and restoration from any local scale power outage to prevent it exacerbating to large scale blackouts such as the ones in North America and Europe [2], [3].

As the "last mile" connection, power distribution system is a major part of power grid. With the increase in the electricity demands and the development of Smart Grid, the amount of data and information needed to be communicated through the monitoring network also increases significantly. Such demand cannot be satisfied by existing power system networking strategies. In addition, due to their exposure in hazardous environment, the electronic power devices vulnerability to failure has been identified as the major cause of several large-scale blackout [2], [3] in the North America and Europe. Networking technology to ensure real-time, reliable, efficient, and effective bidirectional data/information flow for power grid monitoring and control is one of paramount importance for failure detection, diagnosis and responses in the Smart Grid. The power distribution system monitoring had not been feasible [2], [4] because of the overhead involved in installing and maintaining a traditional wired communication (such as those through as Fiber, Ethernet, RS485/232, etc.), the numerous variety of electronic power devices, and the complex terrain they locate. Power line carrier (PLC) technology had been explored to support the data transmission. However, the data transmitted through power line tends to be interfered by the power load [5]. The operation of switching devices such as a High Voltage Direct Current (HVDC) transmission line and an Uninterrupted Power Supply (UPS) also interfere with the PLC communication[6]. The wireless communication technology also provides a feasible option for reliable bi-directional networking along the power distribution system. Many power distribution companies have already utilized public cellular wireless network (GPRS/CDMA/3G)[7], [8] to monitor the power distribution devices. Besides the high cost, the two major technological challenges of such approach for power distribution monitoring are (1) *network security*: how to manage and mitigate malicious cyber attacks; and (2) *guaranteed QoS*: how to ensure the monitoring data, emergency response and control command can be reliably delivered within required time frame, but would not be affected by the number of cell phone customers and their data traffic. To tackle these two technological challenges, we propose to use a private wireless network dedicated for power distribution system monitoring and describe in detail in this paper, and we present how we enhance the QoS for a low-cost wireless protocol, Zigbee (using IEEE 802.15.4 defined physical and MAC layer), by adding a priority handling mechanism at its MAC layer.

The remainder of this paper is organized as follows. In Section II we review the basics of IEEE802.15.4 and relevant research in network QoS. In Section III, we present the delay model of the QoS-MAC for IEEE802.15.4. Section IV presents the experimental setup and the performance results of our QoS-MAC with respect to end-to-end network delay, goodput [1], and collision probability. In Section V, we summarize the results of this paper and point to future directions in protocol

---

[1] We consider goodput as the ratio of achieved throughput and the traffic arrival rate in this paper.

978-1-4244-6511-8/10/$26.00 ©2010 IEEE

development for Smart Grid realization.

II. REVIEW OF IEEE802.15.4 AND RELATED WORK IN NETWORK QOS

Researchers have been studying the opportunities and challenges using the wireless sensor network technology. Gungor[2] reviewed WSN applications in electrical power system and summarized the statistical characterization of the wireless channels used in various electrical power systems. Leon[9] proposed a novel conceptual design to improve the observability and reliability of power systems by assessing the structural health of transmission lines using WSN technology. Nordman[10] proposed a failure detection method based on the system level characteristics of power distribution system based on measurements from wireless sensor nodes. He conducted feasibility analysis of retrofitting existing electrical distribution devices with wireless sensor network technology for monitoring purpose. Most of these research focus on the Zigbee (IEEE802.15.4) [11] networking protocol, which is a short-transmission-range protocol used in wireless personal area networks (WPANs). From the hardware perspective, such communication module can be easily added to the power distribution device at reasonable cost, making it a WSN node. Nodes can communicate with each other in a simple and efficient manner based on Zigbee. Additional features such as QoS, self-healing, and self-organization, from networking perspective, can be added by modifying the networking protocols (software) at each node. In addition, low-cost relaying wireless communication nodes can be used to increase the communication range and improve the reliability and fault tolerance of the power distribution monitoring system. Our contribution here is one of the first steps that makes the real-time monitoring and response of the power distribution network based on wireless sensor network technology feasible.

In this paper, we advance the research by enhancing the QoS support to the IEEE802.15.4 to make the real-time feedback control of the power distribution device feasible. Current Zigbee protocol may result in serious malfunction and service degradation of the Smart Grid as more stations, devices, and consumer appliances are brought online and the traffic increases multiple folds. Without loss of generality, we consider two types of traffic used in the power distribution network: the ***operational*** data provides periodic measurements of device condition and power quality like 1, 2, 3, etc.; and the ***emergency*** data is triggered by any detected failure in the system. Even though the operational data should be transmitted reliably at all time ideally, it is generally agreed that the emergency data should be able to preempt any operational data waiting for service so that any failure can be addressed immediately to prevent possible catastrophic event. From the networking perspective, we assign the emergency data higher priority at the MAC layer so that it will be given preferred service at all time.

IEEE802.15.4 MAC layer supports two medium access modes: the ***slotted*** mode (beacon-enabled mode) and ***unslotted*** mode (nonbeacon-enable mode). In the ***slotted*** mode, the MAC layer accesses the medium using a beacon-based superframe structure. Such mode is not effectible enough for real time data communication. In the ***unslotted*** mode, arbitration of medium access of distributed wireless nodes is achieved by the carrier-sense multiple-access/collision-avoidance (CSMA/CA) scheme [11] . Unlike the popular WiFi (IEEE802.11), in which the backoff value (backoff period, BP) counts down only when the channel is idle [11], [12], the IEEE 802.15.4 counts down BP regardless of the channel status.

Wang[13] compared the slotted and unslotted CSMA in IEEE802.15.4, and found that unslotted CSMA has better throughput and higher probability of successful transmission than slotted CSMA. Kim[14] modeled the unslotted CSMA/CA using M/G/1 queue to obtain performance measures such as delay and throughput and analyzed the collision between two nodes performing CCA. Yu-Kai[15] presented a comprehensive performance analysis based on the analytical model and ns2 simulation of slotted mode with respect to the queuing drop rate, goodput, and power consumption. From these results, it is clear that both slotted and unslotted modes of IEEE 802.15.4 MAC cannot satisfy the latency and reliability requirements of the power distribution monitoring system. However, the unslotted mode is more scalable and more suitable to be used for monitoring power distribution system. Although network QoS had been extensively researched for Wifi, resulting in QoS protocols such as IEEE802.11e and IEEE802.16e [16], [17], [18], the current literature for IEEE802.15.4 QoS support is limited to the guaranteed timeslots as described above. In this paper, we present the analytical model and performance analysis of a QoS enhancement to the Zigbee unslotted MAC.

III. QOS-MAC FOR IEEE 802.15.4

To support reliable bi-directional communication in the Smart Grid, it is of paramount importance that the reporting time is within a guaranteed bound. The MAC delay is one of the primary components of the overall network latency. In this section, we present a new QoS-MAC to enhance the QoS for IEEE 802.15.4. We also will derive the QoS-MAC delay model that captures the delay suffered by a single application frame for successful one-hop channel transmission for both high and low priority data traffic. The system level performance such as network delay, goodput and collision probability follow naturally. Important symbols and notations used in the model are listed in Table 1. Other symbols will be introduced in the text.

A. QoS-MAC for IEEE 802.15.4

We introduce the QoS support for IEEE 802.15.4 by the differentiated service for data traffic with different priority. Additional queues are used in the MAC to store different priority traffic. The high priority data will not only have higher probability of channel access, but also can interrupt the service to the low priority traffic by forcing it to backoff.

Assume we have N sensor nodes that monitor power distribution devices and report back to a coordinator using IEEE

TABLE I
NOTATIONS IN ANALYTICAL MODEL

Symbol	Discription
n_0	Number of nodes with High-priority package
n_1	Number of nodes with Low-priority package **only**
n_2	Number of nodes with **no** package in MAC queue
T_s	Service time of a package
b_m	Average backoff time of the mth stage
T_{tx}	Average transmission time of a packet
K	The max backoff stage of High-priority packet
P_i	The probability a channel is idle when CCA is performed
$P_{i\|i}$	The probability a channel is idle in two consecutive CCA
τ	The probability of CCA detection
p^0	The probability of a node with High-priority package
p^1	The probability of a node with **only** Low-priority package
p^2	The probability of a node with **no** package
m_0	The buffer size of High-priority package
m_1	The buffer size of Low-priority package
Q_{n_0,n_1}	The probability of having n_0 with High-priority packet and n_1 nodes with Low-priority packet in a node

802.15.4 protocol. All the nodes are within the hearing range of each other. When abnormality is detected on a device, the measurements will be sent as emergency data via the communication module. When operational data arrives at any node, it will be pushed into the queue at MAC layer if there is a packet in service. When the emergency data arrived, it will be queued in the high priority queue if there is high priority packet in service. Otherwise, it will interrupt the service of an operational data packet. No operational data will be serviced until the emergency data queue is empty.

The data arrival rates are λ_0 and λ_1 for emergency and operational data respectively. The size of the queue is m_0 for high priority data and m_1 for low priority data. The nodes having high priority packets($(\cdot)^0$) are high priority nodes [2], and the nodes with ***only*** low priority packets ($(\cdot)^1$) are low priority nodes. In the following sections, we will derive the models for the QoS-MAC delay, channel service time, and the goodput.

B. Delay Model of QoS-MAC

We model the delay of QoS-MAC and the backoff process using the Markov Chain queue model for two classes of traffic, as shown in Fig.1. Each state is represented by a vector $\langle k, \lambda, \mu, p\rangle$, in which the k_0 and k_1 represent the number of packets in the queue; λ_0 and λ_1 are the arrival rate; μ_0 and μ_1 are the service rate; and p_{k_0,k_1} denotes the probability of having k_0 high priority packets and k_1 low priority packets in the queue in the current state. Equ.1 describe the Markov Chain in Fig.1, from which we can solve the probability p_{k_0,k_1} under the conditions of statistical equilibrium [19].

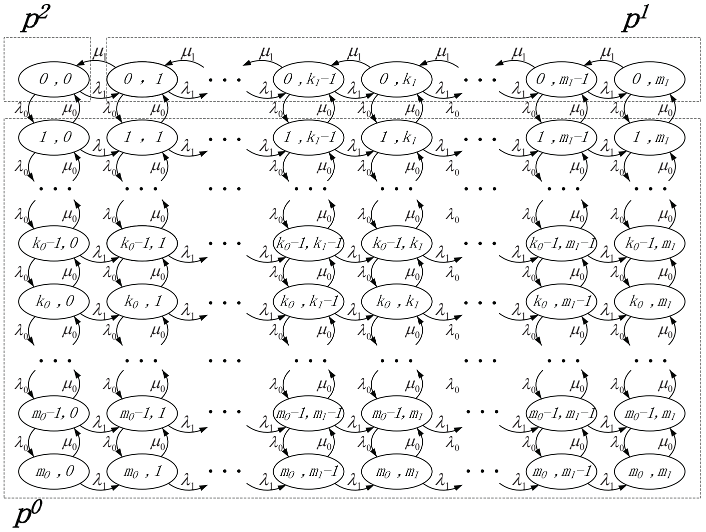

Fig. 1. Markov chain model of buffer

$$\begin{cases} p_{0,0} = \dfrac{\mu_0}{\lambda_0+\lambda_1}\cdot p_{1,0} + \dfrac{\mu_1}{\lambda_0+\lambda_1}\cdot p_{0,1} \\ p_{k_0,0} = \dfrac{\lambda_0}{\lambda_0+\lambda_1+\mu_0}\cdot p_{k_0-1,0} + \dfrac{\mu_0}{\lambda_0+\lambda_1+\mu_0}\cdot p_{k_0+1,0} \\ p_{0,k_1} = \dfrac{\lambda_1}{\lambda_0+\lambda_1+\mu_1}\cdot p_{0,k_1-1} + \dfrac{\mu_1}{\lambda_0+\lambda_1+\mu_1}\cdot p_{0,k_1+1} \\ \qquad + \dfrac{\mu_0}{\lambda_0+\lambda_1+\mu_1}\cdot p_{1,k_1} \\ p_{k_0,k_1} = \dfrac{\lambda_1}{\lambda_0+\lambda_1+\mu_0}\cdot p_{k_0,k_1-1} + \dfrac{\lambda_0}{\lambda_0+\lambda_1+\mu_0}\cdot p_{k_0-1,k_1} \\ \qquad + \dfrac{\mu_0}{\lambda_0+\lambda_1+\mu_0}\cdot p_{k_0+1,k_1} \\ p_{m_0,0} = \dfrac{\lambda_0}{\lambda_1+\mu_0}\cdot p_{m_0-1,0} \\ p_{m_0,k_1} = \dfrac{\lambda_0}{\lambda_1+\mu_0}\cdot p_{m_0-1,k_1} + \dfrac{\lambda_1}{\lambda_1+\mu_0}\cdot p_{m_0,k_1-1} \\ p_{0,m_0} = \dfrac{\lambda_1}{\lambda_0+\mu_1}\cdot p_{0,m_1-1} + \dfrac{\mu_0}{\lambda_0+\mu_1}\cdot p_{1,m_1} \\ p_{k_0,m_1} = \dfrac{\lambda_0}{\lambda_0+\mu_0}\cdot p_{k_0-1,m_1} + \dfrac{\mu_1}{\lambda_0+\mu_0}\cdot p_{k_0,m_1-1} \\ \qquad + \dfrac{\mu_0}{\lambda_0+\mu_0}\cdot p_{k_0+1,m_1} \\ p_{m_0,m_1} = \dfrac{\lambda_0}{\mu 0}\cdot p_{m_0-1,m_1} + \dfrac{\lambda_1}{\mu 0}\cdot p_{m_0,m_1-1} \end{cases} \tag{1}$$

As shown in Fig.1, all the states in the model can be classified as states that have: (1) at least one high priority packet in queue (p^0); (2) no high priority packet in queue (p^1), i.e., all packets are low priority data; and (3) no packet in queue (p^2). They can be determined based on the current states of the network (Equ.2).

$$p^0 = \sum_{k_0=1}^{m_0}\cdot\sum_{k_1=0}^{m_1} p_{k_0,k_1}; p^1 = \sum_{k_1=0}^{m_1} p_{0,k_1}; p^2 = p_{0,0} \tag{2}$$

---

[2] it can also have low priority packets

The probability of n_0 nodes having high priority packets and n_1 nodes having low priority packet in queue, Q_{n_0,n_1}, can be determined by Equ.3.

$$Q_{n_0,n_1} = \frac{N!}{n_0! \cdot n_1! \cdot n_2!} \cdot (p^0)^{n_0} \cdot (p^1)^{n_1} \cdot (p^2)^{n_2} \qquad (3)$$

C. Channel Service Time Model

To model the channel service time to be used in network delay and the goodput, we use following parameter setup. We adopted the time unit 'symbol'($1symbol = 16ns$) as in IEEE802.15.4 MAC, and use the data rate of 250kbps as in 2.4G PHY. The default value of *aUnitBackoffPeriod*[3] is 20 symbols. The default value of the interval between the transmission (TX) frame and the Acknowledgement (ACK) frame, *aTurnaroundTime*, is 12 symbols. To avoid interruption of the ACK frame, we limited the duration for CCA detection to *aUnitBackoffPeriod* (i.e., 20 symbols).

Consider two continuous time units in the channel, $P_i = P_{i|i} \cdot P_i + P_{i|b} \cdot (1 - P_i)$, in which the $P_{i|b}$ or $P_{i|i}$ is the conditional probability that the channel is idle in the second time unit given it is busy or idle during the first time unit. Using the result from [15], i.e., $P_{i|b} = 1/\overline{T_{tx}}$, where $\overline{T_{tx}}$ is the average transmission time of a package, we can compute the probability of the high priority and low priority nodes detecting the idle channel for the packets in queue as:

$$P_i^0 = 1/[1 + \overline{T_{tx}} \cdot (1 - P_{i|i}^0)] \qquad (4)$$

$$P_i^1 = 1/[1 + \overline{T_{tx}} \cdot (1 - P_{i|i}^1)] \qquad (5)$$

If a node performs CCA in the first time unit when the channel is idle, it will send the data during the second time unit, making the channel busy. Only when no node performs the CCA in the first time unit, the probability of the channel being idle in both time units, $P_{i|i}$, will be nonzero. For high priority node, the probability of channel idle in two successive time units ($P_{i|i}^0$) is all high priority nodes and all low priority nodes did not perform CCA in the first time unit (Equ.(6)).

$$P_{i|i}^0 = \sum_{n_0=1}^{N} \sum_{n_1=0}^{N-n_0} \big[\frac{Q_{n_0,n_1}}{Q_0} \cdot (1 - \tau^0)^{n_0 - 1} \cdot (1 - \tau^1)^{n_1}\big] \qquad (6)$$

where $Q_0 = \sum_{n_0=1}^{N} \sum_{n_1=0}^{N-n_0} Q_{n_0,n_1}$. In Equation (6), the fraction in bracket is the probability of there are n_0 high priority nodes and n_1 low priority nodes (Q_{n_0,n_1}) in the network when there is at least ONE high priority node(Q_0). Similarly we can get $P_{i|i}^1$ as:

$$P_{i|i}^1 = \sum_{n_0=0}^{N} \sum_{n_1=1}^{N-n_0} \big[\frac{Q_{n_0,n_1}}{Q_1} \cdot (1 - \tau^0)^{n_0} \cdot (1 - \tau^1)^{n_1 - 1}\big] \qquad (7)$$

where $Q_1 = \sum_{n_0=0}^{N} \sum_{n_1=1}^{N-n_0} Q_{n_0,n_1}$

The probability of a node performing CCA detection per symbol for high priority data (τ^0) or low priority data (τ^1), in Equ.6 and Equ.7 can be calculated using Equ.8 and Equ.9 respectively:

$$\tau^0 = \sum_{n=0}^{K^0-1} \frac{(1 - P_i^0)^n \cdot P_i^0 \cdot (n+1)}{\sum_{m=0}^{n}(b_m^0 + 1) + T_{tx}^0} + \frac{(1 - P_i^0)^{K^0} \cdot K^0}{\sum_{m=0}^{K^0-1}(b_m^0 + 1)} \qquad (8)$$

$$\tau^1 = \sum_{n=0}^{K^1-1} \frac{(1 - P_i^1)^n \cdot P_i^1 \cdot (n+1)}{\sum_{m=0}^{n}(b_m^1 + 1) + T_{tx}^1} + \frac{(1 - P_i^1)^{K^1} \cdot K^1}{\sum_{m=0}^{K^1-1}(b_m^1 + 1)} \qquad (9)$$

The first term is the average CCA detection probability when the packet is transmitted successfully, in which T_{tx}^0 denotes successfully transmit duration time of the packet, b_m^0 is the average backoff time of the m-th backoff stage, and the digital 1 is one unit time for CCA detection; the second term represents the case when all service attempts fail.

A packet is serviced either when the packet is transmitted successfully or when the packet is dropped due to CCA detection failure and the maximum backoff time has been reached. The service time of high priority packet can then be computed as Equ.10.

$$\begin{aligned} T_s^0 = &\sum_{n=0}^{K^0-1} (1 - P_i^0)^n \cdot P_i^0 \cdot \Big[\sum_{m=0}^{n}(b_m^0 + 1) + T_{tx}^0\Big] \\ &+ (1 - P_i^0)^{K^0} \cdot \sum_{m=0}^{K^0-1}(b_m^0 + 1) \end{aligned} \qquad (10)$$

The first term is the sum of the time it takes to transmit a packet within the n backoff stages: the probability that the packet is transmitted successfully times the sum of the transmission time of the packet. The second term in Equ.10 is the time spent when the packets failed to transmit. Similarly, the service time for low priority packets can be calculated using Equ.11.

$$\begin{aligned} T_s^1 = &\sum_{n=0}^{K^1-1} (1 - P_i^1)^n \cdot P_i^1 \cdot \Big[\sum_{m=0}^{n}(b_m^1 + 1) + T_{tx}^1\Big] \\ &+ (1 - P_i^1)^{K^1} \cdot \sum_{m=0}^{K^1-1}(b_m^1 + 1) \end{aligned} \qquad (11)$$

D. MAC Delay, Goodput and Collision Rate

In this section, we derive the three performance measures we are using in the paper for both emergency and routine optional data: the MAC delay, the goodput, and the collision rate.

The MAC delay is defined as the time taken from the packet entering the MAC layer queue to it being serviced, i.e, either transmitted successfully or dropped. Given the channel service time, we can calculate the MAC delay of the high priority packet as shown in Equ.12. It includes the time for the current incoming packet to be serviced and all the packets in the queue before it being serviced. The fraction in Equ.12 is the probability of having k_0 high priority packets in the queue (including the current packet).

$$T_d^0 = \sum_{k_0=1}^{m_0} \sum_{k_1=0}^{m_1} \big(\frac{p_{k_0,k_1}}{\sum_{k_0=1}^{m_0} \sum_{k_1=0}^{m_1} p_{k_0,k_1}} \cdot k_0 \cdot T_s^0\big) \qquad (12)$$

---

[3] the number of symbols forming the basic time period in CSMA/CA mechanism

Similarly, the MAC delay of the low priority packet includes the time for the high priority packets queued (first term in Equ.13) or incoming (third term in Equ.13) being serviced, and the time for other low priority and current packets being serviced (second term in Equ.13).

$$\begin{aligned} T_d^1 = \sum_{k_1=1}^{m_1} \Big[\sum_{k_0=0}^{m_0} & \frac{p_{k_0,k_1}}{\sum_{k_0=0}^{m_0}\sum_{k_1=1}^{m_1} p_{k_0,k_1}} \cdot k_0 \cdot T_s^0 \\ & + \frac{p_{0,k_1}}{\sum_{k_0=0}^{m_0}\sum_{k_1=1}^{m_1} p_{k_0,k_1}} \cdot k_1 \cdot T_s^1 \Big] + T_d^1 \cdot \lambda_0 \cdot T_s^0 \end{aligned} \tag{13}$$

Solving Equ.13, the MAC delay of the low priority packets is:

$$\begin{aligned} T_d^1 = & \frac{1}{1-\lambda_0 \cdot T_s^0} \sum_{k_1=1}^{m_1} \Big[\sum_{k_0=0}^{m_0} \frac{p_{k_0,k_1}}{\sum_{k_0=0}^{m_0}\sum_{k_1=1}^{m_1} p_{k_0,k_1}} \cdot k_0 \cdot T_s^0 \\ & + \frac{p_{0,k_1}}{\sum_{k_0=0}^{m_0}\sum_{k_1=1}^{m_1} p_{k_0,k_1}} \cdot k_1 \cdot T_s^1 \Big] \end{aligned} \tag{14}$$

The goodput of the network for either high or low priority traffic is another important network performance measure. The goodput of periodic operational data through the network indicates whether the monitoring data of the electronic power devices can be reliably transmitted during the normal operation. Likewise, the tradeoff of the operational data goodput and the bursty emergency data goodput is important to determine the network characteristics of the Smart Grid. We solve the goodput of high priority packet (G_0) (Equ.15) and low priority packet (G_1) (Equ.16) based on the given network parameters.

$$G_0 = \frac{\sum_{n_0=0}^{N}\sum_{n_1=0}^{N-n_0} Q_{n_0,n_1} \cdot \left(n_0 \cdot \frac{[1-(1-P_i^0)^{K_0}]\cdot L_0}{T_s^0} \right)}{N \cdot \lambda_0} \tag{15}$$

$$G_1 = \frac{\sum_{n_0=0}^{N}\sum_{n_1=0}^{N-n_0} Q_{n_0,n_1} \cdot \left(n_1 \cdot [\frac{1-(1-p_i^1)^{K_1}]\cdot L_1}{T_s^1} \right)}{N \cdot \lambda_1} \tag{16}$$

In the Smart Grid, the packet transmission failure rate indicates the reliability of the periodic operational data communication. Ideally, all operational data should be transmitted even though it may be delayed when bursty emergency traffic occurs. Given the network parameters, we can compute the failure rate for high priority packet (Equ.17) and low priority packet (Equ.18).

$$F_0 = (1 - P_i^0)^{K_0} \tag{17}$$

$$F_1 = (1 - P_i^1)^{K_1} \tag{18}$$

IV. EXPERIMENT SETUP AND RESULTS

To validate the performance of our QoS-MAC enhancement to the IEEE802.15.4, we simulate a cluster of wireless sensor network monitoring operation and power quality around a substation with 10 wireless sensor nodes and one coordinator connecting to wired backbone and power source. The packet size is 50 bytes and the transmission time (including acknowledgement and IFS(Inter Frame Space)) is 157 symbols(2512 μs). The packet arriving rate for all nodes are the same. We set the maximum number of Backoff Stage (BN) as 5, the value of the Backoff Exponent (BE) for high priority traffic ranges from 0 ∼ 3 and for low priority data ranges from 2 ∼ 5. The queue size is six packets (300 bytes) for both high and low priority traffic.

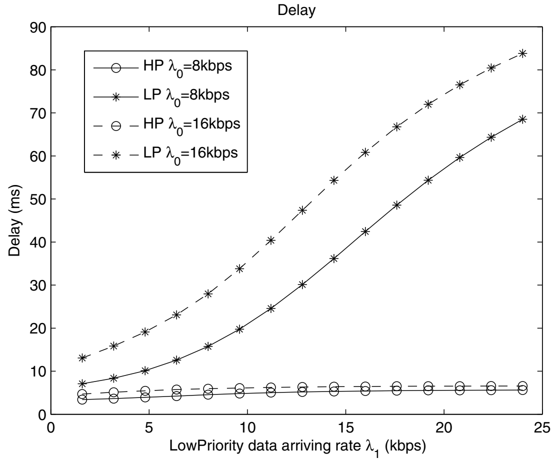

Fig. 2. Delay

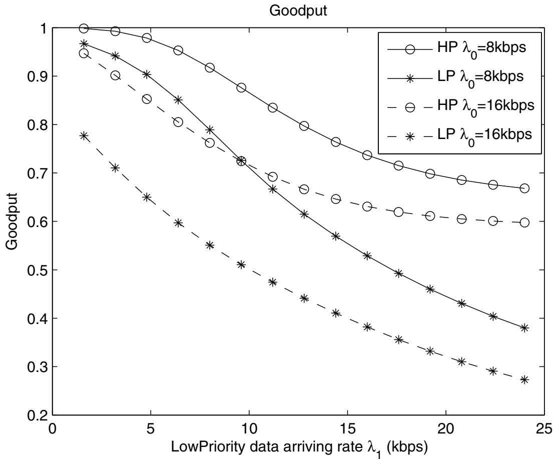

Fig. 3. Goodput

In the simulation, we tested two scenarios: setting the packet arriving rate for high priority data[4] at (1) 8 kbps and (2) 16 kbps while increasing the arrival rate of the low priority data from 0.4 kbps to 24 kbps. Such scenarios allow us to study the network behavior with more than enough bandwidth to with saturated bandwidth—when the quality of service will have impact on all performance measures.

Fig.2 shows the results of network delay of high and low priority data in both cases. We observe that (1) the delay of high priority data is almost invariant with increased arriving rate of low priority data; (2) the delay of high priority data is much less than that of the low priority data because they have

---

[4] We consider the high priority traffic bursty.

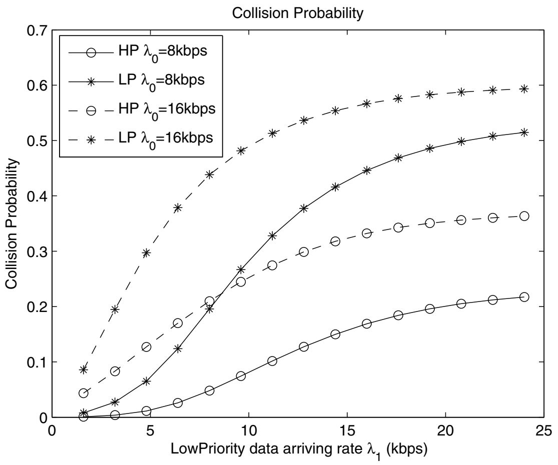

Fig. 4. Collision rate

preemptive priority and higher channel access probability.

The goodput for both scenarios are shown in Fig.3. It is clear that the goodput of low priority data dropped sharply while the goodput for high priority data degraded a little. When the traffic is very heavy, less than 30% low priority data will be transmitted successfully, while more than 60% emergency data transmitted successfully. It clearly demonstrates that the QoS-MAC ensures differentiated service for different traffic.

Fig.4 shows the collision rate in CSMA/CA after the maximum backoff stage is reached and the packet is dropped. When the traffic is light, the collision rate of both priority packets is small (less than 10%). When the traffic increases, the collision rate for both priority data increases because the channel is busy. However, the collision rate for the high priority data increases much slower than that of the low priority data, demonstrates the preemptive property of the high priority data over low priority data.

V. CONCLUSION AND FUTURE DIRECTION

In this paper, we enhanced the QoS support of the low cost wireless protocol IEEE802.15.4 at the MAC layer to support reliable networking and communication of the power distribution systems. Our vision is to develop network model and middleware to enhance the quality of service communication used by the Smart Grid that collects voluminous data from wireless sensor networks. Such reliable, efficient, robust, and secure communication will enable active and effective participation from consumers and distribution system in the power grid operation. Our contribution in the paper is one of the first steps that makes the real-time monitoring and response of the power distribution monitoring system based on wireless sensor network technology feasible. After presenting a Markov Chain based mathematical model we developed to model the MAC behavior of the Zigbee for two classes of power grid traffic: Operational and Emergency data, we derived three performance measures used in our performance analysis: network delay, goodput and collision rate for both types of traffic. The experiment results from two testing scenarios show that in our QoS enhanced MAC protocol, the network performance is much better for the high priority packets than that of the low priority packets. In addition, the network delay, goodput, and the collision rate for high priority data reached a boundary while that of the low priority data do not as the traffic in the network increases to saturation.

Future research include (1) simulate more realistic networking scenario for smart grid application; and (2) develop cross-layer networking protocol such as integrate the network layer and MAC to ensure the end-to-end communication performance of smart grid distribution monitoring system.

REFERENCES

[1] *NIST Smart Grid Standards*, National Institute of Standards and Technology Working Draft Proposed Standard, Rev. Rlease 1.0, 2009.
[2] V. C. Gungor, B. Lu, and G. P. Hancke, “Opportunities and Challenges of Wireless Sensor Networks in Smart Grid - A Case Study of Link Quality Assessments in Power Distribution Systems,” *IEEE Transactions on Industrial Electronics*, vol. pp, pp. 1–1, 2010.
[3] J. W. Bialek, “Recent blackouts in us and continental europe: is liberalisation to blame?” *Cambridge Working Papers in Economics*, 2004.
[4] W. Sun, J. Wang, C. Zhang, and Z. Qian, “Research on the wireless Ad-hoc network for power distribution network communication in medium-small cities,” in *International Conference on Sustainable Power Generation and Supply, 2009. SUPERGEN ’09.*, 2009.
[5] J. Misurec, “Interference in data communication over narrow-band PLC,” *International Journal of Computer Science and Network Security*, vol. 8, Nov. 2008.
[6] S. Mahmod, N. F. Mailah, and M. Radzi, “Effects of high power converter on power line carrier signal,” in *4th National Conference on Telecommunication Technology*, 2004.
[7] P. K. Lee and L. L. Lai, “A Practical Approach to Wireless GPRS On-Line Power Quality Monitoring System,” in *Power Engineering Society General Meeting*, 2007.
[8] A. J. Wilson, “The use of GPRS technology for electricity network telecontrol,” *Computing & Control Engineering Journal*, 2005.
[9] R. A. Leon, V. Vittal, and G. Manimaran, “Application of sensor network for secure electric energy infrastructure,” *IEEE Trans. on Power Delivery*, vol. 22, pp. 1021–1028, 2007.
[10] M. M. Nordman and M. Lehtonen, “A Wireless Sensor Concept for Managing Electrical Distribution Networks,” in *Power Systems Conference and Exposition, 2004. IEEE PES*, 2004.
[11] *Wireless Medium Access Control and Physical Layer Specifications for Low-Rate Wireless Personal Area Networks* , IEEE Std. 802.15.4, 2003.
[12] J. C.Y., H. H.Y., S. D.K., and H. G.U., “Enhanced Markov Chain Model and Throughput Analysis of the Slotted CSMA/CA for IEEE 802.15.4,” *IEEE Trans. on Vehicalar Technology*, vol. 58, pp. 473–478, 2009.
[13] F. Wang, D. Li, and Y. Zhao, “ Analysis and Compare of Slotted and Unslotted CSMA in IEEE 802.15.4,” in *Wireless Communications, Networking and Mobile Computing, 2009. WiCom ’09. 5th International Conference*, 2009.
[14] T. O. Kim, J. S. Park, H. J. Chong, and K. J. Kim, “Performance Analysis of IEEE 802.15.4 Non-beacon Mode with the Unslotted CSMA/CA,” *Communications Letters, IEEE*, pp. 238–240, 2008.
[15] Y.-K. Huang, A.-C. Pang, and H.-N. Hung, “A Comprehensive Analysis of Low-power Operation for Beacon-Enabled IEEE802.15.4 Wireless Networks.” *IEEE Transactions on Wireless communications*, pp. 5601–5611, 2009.
[16] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: MAC Quality of Service Enhancements*, IEEE Std. 802.11e, 2005.
[17] (2005, Dec.) DISTRIBUTED MEDIUM ACCESS CONTROL (MAC) FOR WIRELESS NETWORKS. WiMedia Alliance Inc. [Online]. Available: http://www.wimedia.org
[18] *Physical and MAC Layers for Combined Fixed and Mobile Operation in Licensed Bands*, IEEE Std. 802.16e, 2005.
[19] B. I. Marks, “State Probalilities of M/M/1 Priority Queues,” *Operat Res*, vol. 21, 1973.