Quantifying Uncertainties of Security and QoS for Design of Power Grid Communications Systems

Yujue Wang  
Washington State University  
ywang@eecs.wsu.edu

Carl Hauser  
Washington State University  
hauser@eecs.wsu.edu

Yiming Wu  
KTH Royal Institute of Technology  
yimingw@kth.se

Abstract

Reliable and secure communication, and high quality of service (QoS) (low latency, high availability, etc.) of data are critical to the successful operation of power systems. However, uncertainties, both aleatory and epistemic, are inherent to the system, which makes it difficult to secure the communication while fulfilling the QoS requirements. Nowadays, the administrators of the power grid's communication system have much flexibility in choosing a specific security scheme but the uncertainties make answering the question "what is the best scheme" or even "what is an adequate scheme" very difficult. Appropriately quantifying uncertainty and its effects on security is a key to choosing a sufficiently secure communication system for power grid while meeting QoS requirements.

In this paper, we model aleatory and epistemic uncertainties using probability distributions and subjective logic respectively. Comprehensive quantification of the uncertainties can greatly sharpen administrators’ understanding of the trade-offs between security and QoS and help them to select the most fitting security scheme to meet the QoS requirements. A case study demonstrates how our method works for two different application scenarios.

1. Introduction

Archetypal power systems are interconnected systems linking distribution systems, transmission systems, and generation units [1]. Reliable operations of the power grid depend on the communications between and within these components. The timely delivery of trustworthy data is critical to the power grid. Therefore, both Qualify of Service (QoS) and security of the communication system should be jointly taken into account to ensure that QoS requirements are met [2] while mitigating malicious attacks [3].

The term “Quality of Service” refers broadly to many aspects of the performance of communication systems. For power system applications, relevant QoS metrics include end-to-end delay, report rate, packet jitter, and packet loss rate [4]. The QoS requirements of power system applications depend on both the applications’ algorithms and their purposes (e.g. protection, control, monitoring).

Uncertainty, however, is inherent to both QoS and security, which makes it very difficult to gain an all-inclusive point of view of QoS and security. For instance, randomness of the system could make it very difficult to measure parameters critical to QoS and security very accurately. Methods for quantifying the uncertainty associated with QoS and security schemes and relating the uncertainty to the performance metrics are needed in order to:

• Understand the correspondence or trade-off between QoS and security;
• Understand the overall trustworthiness of the communication to meet the combined QoS and security requirements.

More specifically, quantifying uncertainties of security and QoS can contribute to power grid in three ways:

• It can improve administrators’ understanding of the trade-offs between security and QoS and the uncertainties pertaining to them;
• It can help the designers of a power system’s communication network choose the most appropriate security scheme considering both the QoS requirements and the security requirements;
• It can be informative for the administrators of the system to monitor and evaluate the security schemes in practice.

Uncertainty can be classified into two types: aleatory and epistemic [5]. Different types of uncertainty originate from different sources and have different characteristics. Thus, they should be handled with different techniques. We make use of probabilistic modeling and subjective logic to handle aleatory and epistemic uncertainty separately and then apply the Monte Carlo method to draw the joint distributions. The joint distributions could provide the administrators
of the system a comprehensive perspective for making better QoS and security decisions.

The remaining sections of this paper are organized as follows: Section 2 introduces the communication model for different application scenarios in power grid. We outline the QoS requirements by investigating communication models in practical power systems. From these requirements, a time allotment for the security scheme is inferred. Different security schemes in practice are shown in Section 3. Section 4 describes the classification of various sources of uncertainty and how to handle each type of uncertainty. The framework for quantifying uncertainty is formally defined in Section 5. Section 6 demonstrates our methods with a case study. Section 7 concludes and suggests directions for future investigations.

2. Power System Communication Models and QoS Requirements

QoS requirements depend in part on the communication model being used for a particular application in the power system. Communication models can be generalized from diverse communication scenarios that are encountered. In this section, different communication scenarios are inspected and further classified into different communication models. The characteristics of each communication model are described. QoS requirements can be estimated by analyzing the communication models.

2.1. Message Delivery Schemes and Communication Modes

Message delivery schemes in power system can be divided into Unicast and Multicast schemes. Unicast means that each message is sent to a single destination. In the power system, for example, communication between Supervisory Control and Data Acquisition (SCADA) systems uses a unicast message delivery scheme. A SCADA system polls measurements from one of its substations at a time. In order to obtain the overall information, it needs to poll every substation one by one. In a similar way, unicast is also employed to obtain measurements from an Intelligent Electronic Device via the Manufacturing Message Specification (MMS) protocol. Multicast means that a message is addressed to a group of receivers concurrently. For instance, a Phasor Measurement Unit (PMU) may send measurements to a few Phasor Data Concentrators (PDCs) using a multicast scheme. Similarly, in a substation, Generic Object Oriented Substation Event (GOOSE) and Sampled Value (SV) messages are delivered using multicast as well.

Based on which device initiates communication, communication modes can be categorized as polling and pushing. From the point of view of data sources, polling is passive: a data source sends measurements or status in response to requests from the data users. Protocols such as IEC60870-5-104, DNP3, and MMS operate in polling mode. The other communication mode, pushing, is initiated by the data source. It sends measurement or status messages by itself, periodically or when events occur. In periodic push mode, for example, a PMU constantly sends data at a rate of $10^{-60}$ messages per second, based on its configured reporting rate. Similarly, SV also works in periodic pushing mode (in IEC61850-9-2, it sends 80 packets per power cycle for protection and 256 packets per power cycle for measurement). In event-driven push mode, for example, an IED can be configured to automatically send messages to data receivers when measurements or status values change. A third configuration of push mode combines periodic and event driven behaviors. As with GOOSE, when no event has occurred, messages are pushed at a slow rate (i.e. 1 message per second depending on configuration). When an event occurs, a large number of messages are pushed in a short period of time (i.e. up to 1000 packets per second, again depending on configuration parameters). The state diagram and work flow of combined periodic and event driven communication pattern can be illustrated in Figure 1 and Figure 2.

![Figure 1 State diagram of combined periodic and event driven communication pattern.](image)

The communication message delivery scheme and communication mode of several major power system communication protocols are summarized in Table 1.

Figure 3 compares behavior of different communication patterns. In this figure, an event is introduced into the system at $0.4$s.

At the top of Figure 3, the periodic communication pattern is illustrated where the report rate is 60 packets per second. The report rate is constant no matter when an event occurs. The middle part of the figure
corresponds to the event driven communication pattern. The measurement or status is updated only after an event occurs. The bottom of the figure illustrates the combined periodic and event driven communication pattern. The report rate increases greatly after an event occurs and remains slow and constant when no event occurs.

Figure 2 Work flow of combined periodic and event driven communication pattern.

2.2. Power System Application QoS

In modern power systems, global data is shared for power system protection, control, and operation. Since these data are delivered via a Wide Area Network (WAN), delivery might suffer unavoidable QoS problems. Such degradation potentially affects the performance of power system applications [6] [7]. In this paper, for QoS requirements related to security, we consider the delay requirement’s affect on the time available for security schemes.

Table 1 Power System Communication Protocol Message Delivery Scheme and Communication Mode

<table>
<thead>
<tr>
<th>Message</th>
<th>Message Delivery Scheme</th>
<th>Communication Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE C37.118 SynchroPhasor Data</td>
<td>Multicast</td>
<td>Periodic Push</td>
</tr>
<tr>
<td>IEC 61850 MMS Server Client</td>
<td>Unicast</td>
<td>Event Driven Poll</td>
</tr>
<tr>
<td>IEC 61850 MMS Report</td>
<td>Multicast</td>
<td>Measurement Event Driven Push</td>
</tr>
<tr>
<td>IEC 61850 GOOSE</td>
<td>Multicast</td>
<td>Combined Periodic and Event Driven Push</td>
</tr>
<tr>
<td>IEC 61850 Sampled Value</td>
<td>Multicast</td>
<td>Periodic Push</td>
</tr>
<tr>
<td>IEEE 1815-2012 DNP 3</td>
<td>Unicast</td>
<td>Event Driven Poll</td>
</tr>
<tr>
<td>IEC 60870-5-104</td>
<td>Unicast</td>
<td>Event Driven Poll</td>
</tr>
</tbody>
</table>

To accommodate the effect of variable QoS performance, researchers have proposed several mechanisms. Firstly, QoS performance can be taken into account in application design. For example techniques such as trajectory extrapolation compensation [8], \( H_\infty \) compensation [9] [10], Fuzzy algorithms [11], and Phase-lead compensation [12] can be used to compensate latency of the data link. Secondly, QoS performance can be ensured by management of communication infrastructure [2]. Another main factor that can affect QoS performance is cyber security schemes, which is our focus here. For example, the computation delay of encryption and authentication are usually not negligible. Depending on which type of security countermeasures are applied, computational delay varies. In order to ensure power system applications work properly, the effects of security countermeasures on QoS must also be considered. In this paper we will illustrate our methods for jointly considering QoS and security by looking specifically at the latency:

\[
T_{\text{latency}} = T_{\text{sec}} + T_{\text{comm}}
\]

where \( T_{\text{sec}} \) is the computational delay introduced by cyber security and \( T_{\text{comm}} \) is the latency introduced by communication path.

The communication delay is normally considered as following equation:

\[
T_{\text{comm}} = T_{\text{trans}} + T_{\text{prop}} + T_{\text{queue}}
\]

where \( T_{\text{trans}} \) is the transmission delay, \( T_{\text{prop}} \) is the propagation delay and \( T_{\text{queue}} \) arises from buffering in the communication system. \( T_{\text{comm}} \) is determined by the application scenario and communication model and \( T_{\text{prop}} \) can be measured. Therefore, \( T_{\sec} \), the time overhead can be utilized by security schemes, can be inferred straightforwardly as \( T_{\sec} = T_{\text{latency}} - T_{\text{comm}} \) once
the latency requirement ($T_{\text{latency}}$) of power system application is determined.


In order to strengthen the reliability of power grid, security schemes are applied to mitigate malicious attacks from external threats. Identical to traditional conceptual features of information security, security objectives of the cyber system of smart grid can be classified as follows [13]:

- **Availability**: to ensure the timely delivery of proper data;
- **Integrity**: protect authentic data from the malicious manipulations;
- **Confidentiality**: only authorized stakeholders could access and interpret the data.

From the perspective of system reliability, availability and integrity are the most important security objectives in the Smart Grid.

3.1. Security Schemes

Cryptographic algorithms and approaches are primary countermeasures against malicious attacks. Encryption algorithms mitigate threats pertaining to confidentiality and cryptographically-based authentication methods aim to deal with attacks against integrity of data [13].

- **Encryption** is an elementary cryptographic method to achieve secure communication and information protection for any information system. In the Smart Grid, most electronic devices are expected to have at least basic cryptographic capabilities, including the ability to support symmetric ciphers.
  - Asymmetric key cryptography requires more computation resources than symmetric key cryptography for long key size (strong security). Thus, the use of asymmetric key encryption, such as RSA, may be limited in embedded computing systems.
  - Symmetric key cryptography such as DES and AES requires approximately constant computational resources regardless of the key size; however, it requires secure exchange and update of secret keys among network nodes, thereby complicating the process of key management.
- **Authentication** is a crucial identification process to eliminate attacks targeting data integrity. Intuitively, design of authentication for the Smart Grid can leverage existing authentication protocols in conventional networks, which have been extensively studied for decades.

4. Uncertainties

The security of communication is critical to the reliable operation of the power grid. Various types of uncertainties, however, are inherent to the power cyber-physical system and make it difficult to ensure the security of the synchrophasor data while meeting Quality of Service requirements.

4.1. Uncertainty Classification

Classification of uncertainty is of great interest to quantify uncertainty as different uncertainties can be quantified in different ways. Generally, there are two types of uncertainty pertaining to a system: the aleatory uncertainty and the epistemic uncertainty [14]:

- **Aleatory uncertainty** is also called variability. It is irreducible and covers uncertainty brought by stochastic behaviors of a physical system or the randomness of the environment under consideration.
- **Epistemic uncertainty** is also termed as reducible uncertainty or subjective uncertainty. Epistemic uncertainty arises from lack of knowledge, i.e. partial information, about the system or the surrounding environment.

Another way to categorize uncertainties depends on the different sources of uncertainties. More specifically, the uncertainty related to security of Wide Area Monitoring and Control (WAMC) originates in several factors:

- **Simplified assumptions**: power systems are very complicated systems. In order to model the system in practice, only the most significant features are modeled and some behaviors of the system are simplified. Modeling abstractions are inherently inaccurate representations of the system and uncertainty arises because of that.
- **Noise in the cyber-physical system**: both cyber and physical components are susceptible to stochastic variations.
- **Human in the loop**: the behavior of human beings is unpredictable. The humans could be operators or malicious attackers. Their actions can bring much variation to the system.
- **Uncertainty in the requirements**: Security is a very expansive concept including several factors. Moreover, there is trade-off between security and performance. So system administrators may NOT
have a precise objective to construct the security scheme.

According to the definitions above, noise of the cyber-physical system and human in the loop can be considered as aleatory uncertainty and other types of uncertainty are epistemic uncertainty. We select different methods to quantify the uncertainties originating in different sources.

There are two kinds of uncertainty quantification problems: forward uncertainty propagation and inverse uncertainty quantification [15]:

- The forward uncertainty propagation problem relies on the observation that independent variables’ uncertainty affects the uncertainty of the function depending on these variables. The propagation of uncertainty refers to the problem of measuring how these variables’ uncertainty influences the uncertainty of the output of the function.

- The inverse problem primarily focuses on inferring the unknown parameters of the mathematical model based on data observed; it estimates the deviation between the experiment and the mathematical model.

What we model lies in the area of uncertainty propagation: we model the uncertainty of the input and show the influence on the choice of the most fitting security implementation. Therefore, quantifying or modeling the uncertainty of the input is of vital importance.

4.2. Tools for Quantifying Uncertainty

Probability distributions are the most common way to describe uncertainty. A probability distribution associates a probability to each measurable subset of the possible outcomes of a stochastic procedure. Details about probability distributions can be found in [16].

Subjective logic is a relatively new genre of probabilistic logic that specifically takes uncertainty and subjective belief into consideration. In general, subjective logic is suitable for modeling and analyzing situations involving uncertainty and incomplete knowledge [17]. A very typical application of subjective logic is to model trust networks [18].

Subjective logic is applied to capture a fundamental uncertainty of human being’s inference on a proposition. In addition, whenever the truth of a proposition is expressed, it is always done by an individual, and it can never be considered to represent a general and objective belief. That is the origin and advantage of subjective logic.

Opinion is the essential concept of subjective logic, which stands for the belief owner’s subjective beliefs on a proposition. A binomial opinion applies to a single proposition, and can be represented as a beta distribution. A multinomial opinion applies to a collection of propositions, and can be represented as a Dirichlet distribution. Through the correspondence between opinions and Beta/Dirichlet distributions, subjective logic provides an algebra for these functions.

5. Quantification Framework

In this section, we use a few equations to describe constraints on security schemes. We denote all of the possible security schemes under consideration as D. One security scheme can be denoted as $d \in D$.

1) Implementation Constraints: Not all of the security schemes are feasible for the QoS requirements of a particular communication model. There are some constraints from the implementation perspective. So we use $F^I$ to denote the implementation constraint function.

$$F^I(d) \rightarrow \{0, 1\}$$

A decision $d \in D$ is valid if and only if $F^I(d) = 1$.

2) Delay Constraints: As we introduced in Section 2, we can determine the delay requirement for the security implementation. The time consumption of an encryption or authentication method is a very significant concern when choosing a security scheme from the decision space as some of the algorithms may cost too much time and thwart the communication applications’ real time data requirements.

$$F^I(d) \rightarrow r$$

where $r$ is a positive real time indicating time consumption of $d$.

3) Security Coverage: As we previously stated, we focus on two aspects of security: Confidentiality and Integrity. We can estimate the coverage of a decision $d \in D$ by measuring each of these aspects. So a function can be symbolized as follows:

$$F^C_s(d) = m_s$$

where $d \in D$, $\Phi$ is the set of security aspects $\Phi = \{\text{Confidentiality, Integrity}\}$, $s \in \Phi$.

The value of security coverage is denoted:

$$S = \sum_{s \in \Phi} w_s F^C_s(d)$$

where $w \in W$ and $W$ is a set of weights that reflect the priority of different aspects in a given situation.

The problem is formally defined. But when we move to next step to establish the constraint and goal
functions, the inherent uncertainty of the system becomes a difficulty. Quantifying the uncertainty with an appropriate method is necessary to solve the problem. To do this, we use probability distributions to model aleatory uncertainty and subjective logic to characterize the epistemic uncertainty. Opinions are elicited from stakeholders as a measurement of the security coverage of different security schemes, which is a kind of epistemic uncertainty.

5.1. Quantifying Aleatory Uncertainty

It is straightforward to use probability distributions to quantify aleatory uncertainty, such as the uncertainties brought by the random behavior of the system (noise).

Probability distributions are a natural choice for describing aleatory uncertainty. There are generally two ways to do distribution fitting: parametric methods and regression methods. We mostly use parametric methods to model aleatory uncertainty in our work.

For parametric methods [19], the parameters of the distribution are calculated from the data series. Usually, there are three common methods: method of moments, method of L-moments [20] and Maximum likelihood method. For example, given a data stream \( X \), the idea of the parametric method is to construct a probability distribution with estimated parameters to minimize the predefined difference between this distribution with estimated parameters and the original data stream \( X \).

5.2. Quantifying Epistemic Uncertainty

An opinion of subjective logic is usually denoted as \( \omega_A^x \) where \( A \) is the subject, also called the belief owner, and \( x \) is the proposition to which the opinion applies. The proposition \( x \) is drawn from a state space denoted as \( X \). The propositions are disjoint set in the state space.

If \( x \) is a proposition, an opinion can be denoted as a tuple (ordered) as \( \omega_x = (b, d, u, a) \), where \( b \) is the positive belief that \( x \) is true, \( d \) is the negative belief that \( x \) is not true, \( u \) indicates the uncertainty with the beliefs and \( a \) is a base rate which is essentially the prior probability if there is no evidence.

The invariant of \( b, d, u \) is \( b+d+u=1 \) and \( b, d, u, a \in [0,1] \). We can use some corner cases to understand the subjective logic better. \( b=1 \) is essentially a binary logic true; vice versa \( d=1 \) equals to binary logic false. \( b+d=1 \) is actually a traditional probability without uncertainty considered. \( b+d < 1 \) indicates that a degree of uncertainty exists or is considered. \( b+d = 0 \) means the belief owner is totally uncertain. The expectation can be defined as \( E = b + au \).

Binomial opinions can be represented on an equilateral triangle as shown in Figure 4 [17]. Any point within the triangle can be interpreted as the belief tuple of \( (b,d,u) \). The \( b, d, u \)-axes indicated by the Belief, Disbelief or Uncertainty label dash from one vertex to the opposing edge orthogonally.

Beta distributions are normally denoted as Beta(\( \alpha, \beta \)) where \( \alpha \) and \( \beta \) are its two parameters.

The Beta distribution of a binomial opinion \( \omega = (b, d, u, a) \) is the function

\[
\text{Beta}(p | \alpha, \beta) = \frac{\Gamma(\alpha + \beta)}{\Gamma(\alpha)\Gamma(\beta)} p^{\alpha-1}(1-p)^{\beta-1}
\]

where \( \alpha = 2b/a + 2a \) and \( \beta = 2d/a + 2(1-a) \).

By this, we can easily convert a subjective logic opinion to a probability distribution.

5.3. Eliciting Opinions on Security with Uncertainty from Stakeholders

Security coverage is hard to directly measure using mathematical models as it is always associated with epistemic uncertainty. So eliciting opinions on security coverage from stakeholders is a practical choice. It is commonly agreed that eliciting users’ preferences in terms of complex utility functions is challenging [21].

People are usually not good at expressing opinions with numerical values. However, verbal categories are more intuitive. In the fuzzy verbal category approach [17] opinions are measured with 2-dimensional fuzzy categories: the likelihood opinion and the certainty

---

2571
opinion. Stakeholders can choose their opinions from the fuzzy verbal categories as Figure 5 indicates.

![Figure 5 Fuzzy Verbal Categories.](image)

Figure 5 Fuzzy Verbal Categories.

However, not all of the opinions in the verbal categories make empirical sense. In order to rule out improper opinions, we overlay the verbal categories with shading in Figure 5. Only those opinions that lie within the shaded triangle are valid. For example, 1E is not a valid opinion in real life as people cannot say that something is absolute while also being completely uncertain about it. So 1E stands outside of the shaded area. When the stakeholders choose a value from the fuzzy categories, this value can be converted into a subjective opinion if it is valid. Then, the opinions marked in the fuzzy verbal categories can be mapped to the opinion triangle of Figure 4 by treating the shadowed area in the fuzzy verbal category as an opinion triangle as in Figure 6. Thus, the triple \( (b,d,u) \) can be determined and corresponding beta distribution can be constructed.

6. A Case Study

A case study has been performed to apply the proposed uncertainties quantification methods to a benchmark power system oscillation model.

6.1. Power System Description

The model is a two-area four-machine system as shown in Figure 7. The parameters of the system can be found in [22]. In this system, buses 7, 8, and 9 are modeled as substations and called \( SS_{Bus7} \), \( SS_{Bus8} \), and \( SS_{Bus9} \). We have studied quantification of uncertainties for two types of power system applications in this study system. One is a protection function and the other is a control function. Another type of function in power system, monitoring function, is out of the scope of this study since monitoring functions have lowest requirement on QoS.

![Figure 7 Power System used for the case study showing the communication links.](image)

For the protection function, transmission line protection is applied on the lines between \( SS_{Bus7} \) and \( SS_{Bus9} \). Current differential line protection is the chosen protection scheme. For this protection scheme, according to standard IEC 61850-90-1, current measurements on \( SS_{Bus7} \) and \( SS_{Bus9} \) have to be delivered to one another via the communication system. At each substation, the remote and local current measurements are compared to identify whether there is a fault on the line or not. The result of comparison is used to control the breakers to isolate the line if a fault is detected. The QoS requirements for this line protection function are listed in Table 2.

<table>
<thead>
<tr>
<th>Item</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report Rate</td>
<td>at least 12 samples per power cycle</td>
</tr>
<tr>
<td>Latency</td>
<td>Less than 8ms</td>
</tr>
<tr>
<td>BER</td>
<td>Less than ( 10^{-6} )</td>
</tr>
<tr>
<td>Time Synchronization</td>
<td>Less than 0.1ms</td>
</tr>
</tbody>
</table>

Table 2 Line Differential Protection QoS Requirements
Therefore, the sampled value method defined in IEC61850-9-2 is chosen as the protocol for exchanging current measurements between SS_{Bus 7} and SS_{Bus 9}. To ensure that the breaker controller is working properly, an interlocking function is also applied by using GOOSE messages to exchange breaker status between these two substations.

For the control function, this power system is unstable when the system is without the power system stabilizer (PSS). In order to keep the system stable, a Static Var Compensator (SVC) is deployed on SS_{Bus 7}. Normally, an SVC is used for maintaining voltage level. It also can be used to control the system oscillation as a Power Oscillation Damping (POD) controller. More details can be found in [23]. The POD controller requires a power measurement signal input from SS_{Bus 8}. In this case study the source of the control input signal of the POD is a Phasor Measurement Unit (PMU) in substation SS_{Bus 8}. The signal follows synchrophasor data format. From the previous study in [23], the QoS requirement are as stated in Table 3.

In this simplified case study, we only consider DES, Triple DES, AES, and RSA encryption algorithms. Details about these algorithms can be found in [24].

We use a Raspberry Pi Model B to emulate an IED and run Java implementations of these four encryption algorithms on it. A set of running-time data is obtained by running these algorithms repeatedly. Using the parametric method described in Section 5.1, we derive the distributions of running time of the encryption algorithms on the Raspberry Pi.

Opinions about the security coverage of the encryption algorithms are also drawn from the stakeholders. Stakeholders can mark their opinion on the security of each algorithm from the Fuzzy Verbal Category in Figure 5. Then, with the method demonstrated in Figure 6, these opinions can be translated into a belief tuple. Parameters of the Beta distribution can be inferred from the belief tuple by the formula introduced in Section 5.2.

**Table 3 POD Controller QoS Requirements**

<table>
<thead>
<tr>
<th>Item</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report Rate</td>
<td>60 packets per second</td>
</tr>
<tr>
<td>Latency</td>
<td>Less than 20ms</td>
</tr>
</tbody>
</table>

Figure 8 Uncertainties with DES.

Figure 9 Uncertainties with Triple DES.

Figure 10 Uncertainties with AES.

Figure 11 Uncertainties with RSA.
Table 4 Latency Distribution and Opinions on Security Coverage of Four Encryption Algorithms

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Latency</th>
<th>Opinion on Security</th>
<th>Distribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>DES</td>
<td>N(2.66, 0.19)</td>
<td>5D</td>
<td>Beta(1, 1.5)</td>
</tr>
<tr>
<td>Triple DES</td>
<td>N(6.68, 0.66)</td>
<td>4C</td>
<td>Beta(4, 4)</td>
</tr>
<tr>
<td>AES</td>
<td>N(8.38, 0.65)</td>
<td>3B</td>
<td>Beta(5, 3)</td>
</tr>
<tr>
<td>RSA</td>
<td>N(5324.45, 305.47)</td>
<td>2B</td>
<td>Beta(16, 2)</td>
</tr>
</tbody>
</table>

Table 4 lists the distributions of latency and the Beta distributions denoting the subjective opinions about the security coverage of the encryption algorithms.

We use the Monte Carlo method [25] to compute the probabilities of each combination of latency and security coverage. Figure 8, Figure 9, Figure 10 and Figure 11 depict the distributions corresponding to the latencies and security coverages. Time axis in these graphs indicates latencies in milliseconds and security coverage is the probability that the stakeholders expect these algorithms to be secure. Different colors are used to show the probability (calculated through Monte Carlo method) at each combination of latency and security coverage. Each probability specifies how likely that this security algorithm can assure the security coverage while satisfying the latency requirements.

For our first application scenario, the latency requirement is < 9ms. RSA is ruled out as it can never meet the latency requirement. For the remaining three algorithms, if the administrator wants the security coverage to be higher than 0.4, then the probability for DES to satisfy both latency requirement and security requirement is 0.1, Triple DES is 0.6 and AES is 0.5. So the administrator may choose Triple DES as the solution. But if the communication delay is a little bit higher, which allows less time for the security implementation to operate, the administrator may prefer to choose DES.

For the second application scenario (the POD controller case), the latency requirement is less than 20ms. All three symmetric key algorithms can meet the latency requirement. The administrator would favor AES as its security coverage is always better than the other algorithms when latency is not a concern.

7. Conclusions and Future Work

In this paper, we provide a framework to investigate QoS and security of power grid communication system in an integral way by quantifying different types of uncertainties associated with them. We use probability distributions to capture the characteristics of delay for security overhead and apply subjective logic to describe the stakeholders’ opinions on security coverage of security schemes. The Monte Carlo method is employed to produce a unified view of the overall uncertainty with these two aspects. A simple study case shows how to utilize our method to make decisions related to QoS and security in practice. In our study case, the administrator of the system can have a clear view on the trade-off between QoS assurance and security coverage and can choose the most fitting security scheme to achieve best security coverage while satisfying QoS requirements.

This initial work suggests several directions for further investigation: 1) More precise modelling can be applied to deal with uncertainty in both the security delay and communication delay which are both probabilistic in nature; 2) Make use of more advanced techniques to model security coverage, capturing the related uncertainty; 3) Apply the work to more real life cases: it can be employed to both choose a fitting security scheme incorporating QoS requirements and to evaluate real life systems.

8. References


