Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2012, Article ID 175262, 13 pages
doi:10.1155/2012/175262

Research Article

Authentication and Integrity in the Smart Grid: An Empirical Study in Substation Automation Systems

Xiang Lu,[1,2] Wenye Wang,[2] and Jianfeng Ma[1]

[1] *Department of Computer Science, Xidian University, Xi'an 710071, China*
[2] *Department of Electrical and Computer Engineering, North Carolina State University, Raleigh, NC 27606, USA*

Correspondence should be addressed to Xiang Lu, xlu6@ncsu.edu

Received 8 March 2012; Accepted 3 April 2012

Academic Editor: Qun Li

The smart grid is an emerging technology that integrates power infrastructures with information technologies to enable intelligent energy managements. As one of the most important facilities of power infrastructures, electrical substations undertake responsibilities of energy transmissions and distributions by operating interconnected electrical devices in a coordinated manner. Accordingly, it imposes a great challenge on information security, since any falsifications may trigger mal-operations, and result in damages to power usage. In this paper, we aim at authentication and integrity protections in substation automation systems (SAS), by an experimental approach on a small scale SAS prototype, in which messages are transmitted with commonly-used data origin authentication schemes, such as RSA, Message Authentication Code, and One-Time Signature. Through experimental results, we find that, current security solutions cannot be applied directly into the SAS due to insufficient performance considerations in response to application constraints, including limited device computation capabilities, stringent timing requirements and high data sampling rates. Moreover, intrinsic limitations of security schemes, such as complicated computations, shorter key valid time and limited key supplies, can easily be hijacked by malicious attackers, to undermine message deliveries, thus becoming security vulnerabilities. Our experimental results demonstrate guidelines in design of novel security schemes for the smart grid.

1. Introduction

The smart grid envisions a revolutionary regime of energy managements by integrating information technologies with power systems to make energy generation and consumption efficient and intelligent [1]. Towards such a promising paradigm, the crux lies in timely and accurate information exchanges for synergistic coordinations among a variety of electric power devices [2], in order that intelligent power management applications, such as relay protection [3] and demand response [4], can be readily implemented for ubiquitous system supervisory and efficient device controls.

As the most critical facility in power systems, widely deployed substations are engaged in crucial functions of energy transmissions and distributions, including voltage transformation and regulation, power quality measurements, and interconnections of multiple electric systems [5]. Towards such important and diversified functions, a variety of power devices are installed in substations, such as transformers, breakers, and insulators. Furthermore, a large number of power devices in the substation result in extensive control and system information exchanges and deliveries, serving for collaborative system operations. For example, to ameliorate power qualities and avoid potential energy losses, the capacitor bank, which is made up of groups of individual capacitors, requires real-time power factor measures of phasor measurement units (PMUs) as references of power factor tuning in distribution substations [6]. Also, an electrical regulator resorts to electronic voltage transformers for information of real-time voltage measures to automatically maintain a constant voltage level on distribution feeders [7]. Hence, timely and accurate information exchanges are vital to device and system operations towards efficient power managements.

To enable substantial information exchanges, power devices in a substation are organized to form a substation automation system (SAS) via microprocessor-based equipment controllers, which are also known as intelligent

electronic devices (IEDs) [8, 9]. In this way, equipment information and system events are able to be transmitted and responded elegantly, thereby effectively preventing potential system failures.

Nevertheless, since the SAS encompasses all critical system information, it is prone to be the primary target of malicious attacks [10], even terrorist attacks. Through the SAS, attackers can readily invade the substation to launch attacks by unauthorized operating equipments or tampering system parameters. For example, an attacker can counterfeit device failures by modifying real-time device data, like current and voltage, to trigger inappropriate protection operations, for example, "tripping" relays to cut off feeders. Even worse, such an incorrect operation may spread quickly to neighbor substations due to interconnections between substations, thereby deriving cascading failures in a large area [11]. Thus, *how to protect the integrity and authenticity of SAS messages between interconnected power equipments* is a crucial challenge not only for the reliability of the smart grid, but for the national security and public safety [12].

Prior works have identified potential threats faced by the SAS [13] and recommended to leverage data origin authentication schemes [14–16] to protect the authenticity and integrity of SAS messages by corroborating that entity is the one that is claimed and validating that the message is unmodified [17, 18]. Intuitively, these solutions appear to be effective in countering against malicious message forgeries, because underlying cryptographic schemes are sensitive to falsifications. However, in this paper, we find that these schemes are not applicable when practically deployed in the SAS due to application and setup constraints in substations, including limited device computation capabilities, multicasted device messages, stringent timing requirements, and high-rate data sampling. For example, in a substation teleprotection scenario, the most critical "trip" message must be securely delivered in 3 milliseconds (ms) [9] between coordinated relays. Otherwise, the message will become stale and discarded by the destination, which may induce failures of protection operations and force entire systems to endure a fault current that is much higher than the rating value. Unfortunately, our results show that those proposed solutions cannot handle such a scenario with satisfactory performance. Moreover, limitations of security schemes can be hijacked by attackers and further result in significant performance degradation, thereby becoming security vulnerabilities.

To understand such potential vulnerabilities of current security schemes, we establish an SAS prototype with essential applications regarding relay protection and IED data sampling according to IEC61850 [9], the most dominant communication standard for substations. Then, we measure message delivery performance with three extensively recommended data origin authentication schemes, including RSA [14], message authentication code (MAC) [15], and one-time signature (OTS) [16, 19, 20]. Our results are threefold. Firstly, due to complicated computations, RSA is restricted only to applications that are not time critical, that is, without rigorous timing requirements. Secondly, MAC-based schemes can be potential solutions, yet need special configurations to reduce the waiting time of message validations and to resist collusion attacks. Finally, despite the fact that OTS-based schemes show better performance in our experiments in terms of efficient signing and verifications, the shorter key validation time is a fatal vulnerability that derives two new attacks, including delay compression attacks and key depletion attacks. Both may largely impede the applicability of OTS-based schemes. Based on the above analysis, we remark that the fundamental cause of these unsatisfactory results lies in that current security solutions are not designed to achieve both security and time-critical performance as required by the SAS. Therefore, there is an acute need for novel data origin authentication schemes that can address such issues jointly, that is, security requirements, as well as timing requirements, in the smart grid.

The remainder of this paper is organized as follows. In Section 2, we briefly introduce the electrical substation, including the one-line diagram and the communication architecture. In Section 3, we present a brief description of existing data origin authentication schemes, which is followed by system implementations of our testbed in Section 4. Measurements and analysis of security schemes are discussed in Section 5. Finally, we conclude in Section 6.

2. Preliminary of Substation Automation Systems in the Smart Grid

In this section, we firstly introduce the single-line diagram of a substation for the smart grid, by taking a 220 kV-132 kV transmission substation as an example. Then, we present the architecture of the corresponding substation automation system. Based on the system architecture, we summarize performance and security requirements in SAS applications and identify two critical messages for subsequent experimental studies, including protection messages and data sampling messages.

2.1. Single-Line Diagram of a Substation. First of all, we examine the single-line diagram of a substation to investigate *how power devices are wired in substations towards effective power managements*. Since diagrams of substations vary significantly with respect to types, functions, and sizes, we take a 220 kV-132 kV transmission substation [9] as a simple example to illustrate the topology of electronic devices in the substation, as shown in Figure 1. In this example, a 220 kV incoming feeder (a power line used to distribute electric power) is connected to a 132 kV bus (a conductor that serves as a common connection for electric circuits with very low impedance [10]) via a 220 kV-132 kV transformer. To protect the incoming feeder, two circuit breakers are placed on both ends of the transformer, which can be "tripped" to cut off the incoming feeder if currents or voltages exceed thresholds measured by the electronic current transformer/electronic voltage transformer (ECT/EVT). Besides the incoming feeder, there are also two outgoing feeders emanating from the 132 kV bus with the same configurations for feeder protections.

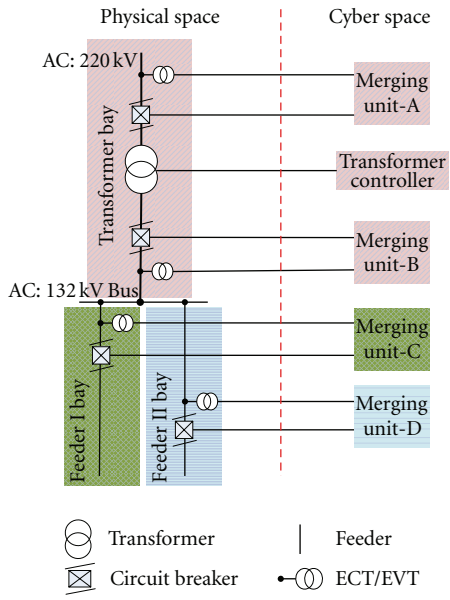

Figure 1: The single line diagram of a 220 kV-132 kV transmission substation.

Usually, an electric power substation is composed of *bays*, which are closely connected subparts in the substation with some common functionality [9]. For example, on the incoming feeder of Figure 1, the transformer, two ECT/EVTs and two circuit breakers work cooperatively to transform voltages and protect feeders, thereby forming a bay, named as the transformer bay. Similarly, we name the other two bays as feeder I/II bay, mapping with two outgoing feeders.

Towards an efficient equipment status monitoring, such substation equipments are expected to send out their running states. To this end, many IEDs are connected to corresponding power devices to digitize collected analog data and deliver state messages between devices. For example, a merging unit gathers information from connected devices, such as phase voltages and currents from the ECT/EVT and ON/OFF status from the circuit breaker [8]. In the same way, a transformer controller monitors and controls the 220 kV-132 kV transformer by taking measurements of running states. Then, substation devices, as well as attached IEDs, are ready to be interconnected for a substation automation system.

2.2. System Architecture of Substation Automation. Based on system functions, the SAS is logically divided into three levels, including the process level, the bay level, and the station level [9]. The process level is close to power equipment, which is designed for data acquisition and issuing commands. The key IED in this level is the merging unit [9], which is exploited to sample instantaneous current or voltage values and ON/OFF states via the attached ECT/EVT and circuit breakers, such as merging unit C in feeder I bay of Figure 2. The sampled measures are further fed into the bay level equipment, like relay C and feeder I bay controller, as references of system states.

The bay level involves multiple IEDs to execute control operations in response to bay events and operators' commands. For example, in the feeder I bay, there are two IEDs, including relay C and feeder I bay controller. Relay C is in charge of fault handling by "tripping" or "untripping" circuit breakers, which is determined by negotiations with other relays, like relays A and D in Figure 2, to ensure synergetic protection actions in the same substation [21]. The feeder I bay controller is for automation tasks regarding local device monitoring and control to facilitate local operation decisions, such as "reclosing" the circuit breaker for fault clearing before incoming commands.

Further, the station level consists of a station computer with databases for data storages, a gateway device for remote communications, a GPS server for synchronization inside the substation, human machine interface (HMI), and operators' workplaces. All of these are used for stationwide functions, such as the station level interlocking (interlocking is installed to prevent incorrect equipment operations by specifying the operational sequencing [22]) and control operations issued by operators [9].

Besides hierarchical levels, two buses are also deployed between levels to interconnect IEDs, including the process bus to connect process level IEDs and bay level IEDs and the station bus to connect bay level IEDs and station level facilities. To ensure reliable connections, both buses adopt a dual-bus architecture to avoid a single connection of failure. Also, a synchronization bus is originated from the GPS to provide time synchronization services within the substation. Thereby, all substation devices are interconnected via an SAS, such that information of device running states can be flexibly delivered among devices for synergetic system operations, such as failure diagnosis, malfunction isolations, and fault clearances.

2.3. Security and Performance Requirements. Through the fully functional SAS, a large amount of power management applications are enabled by operating power devices in a coordinated fashion. For example, the relay interlocking is achieved by relay negotiations to determine a "tripping" sequence of circuit breakers with the minimum system cost of fault isolations, whereas the load shedding (the load shedding is an intentionally engineered electrical power outage, which is in response to a situation where the demand for electricity exceeds the power supply capability [22]) is executed after communications of bay controllers, also targeting the minimum system cost. In spite of the diversity of power management applications, they all have two common features implied, that is, (1) most SAS applications are delay sensitive and have stringent timing requirements for coordination messages deliveries; (2) most coordination messages are usually *multicasted* to multiple related devices. For example, the stationwide interlocking messages must be delivered to relays in 10 ms, and the sampling data need to arrive at several bay-level IEDs in 3 ms from process-level merging units [9]. Thus, the message delivery delay is considered as one of the most important performance requirements in the substation automation, which is formally defined as follows.

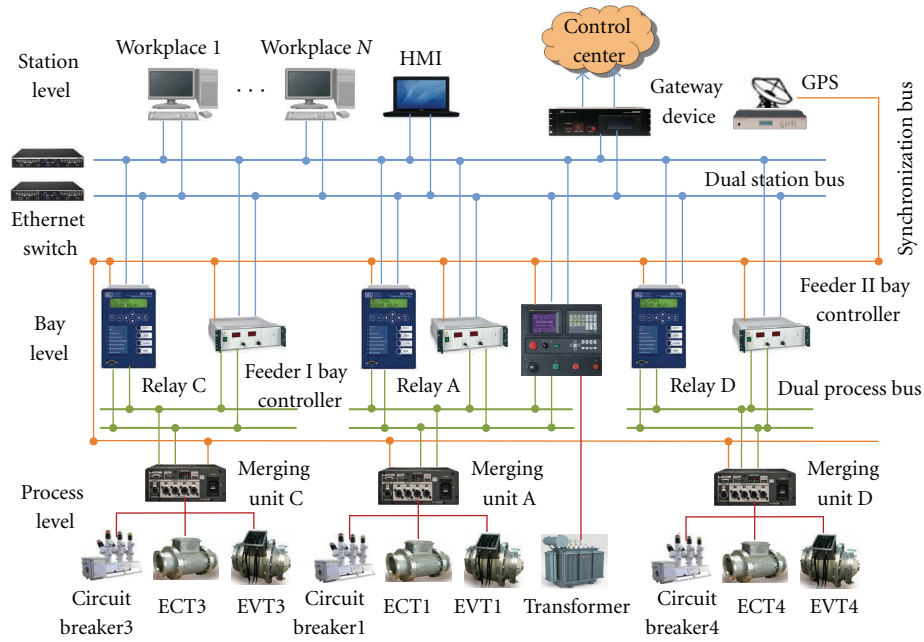

Figure 2: The system architecture of the substation automation system in the 220 kV-132 kV transmission substation.

Definition 1. The message delivery delay is the elapsing period from the time instant that a message is generated at the application layer of a power device to the time instant that the message is delivered to the application layer of its destination device.

Table 1 summarizes timing requirements of key messages in SAS applications [2, 9, 23], including protection messages, monitoring and control messages, system-maintenance-related messages, and data-sampling messages. We can see that timing requirements vary dramatically with respect to message types. The most critical ones are protection and continuous sampling messages with 3 ms delay thresholds inside the substation. As shown in Figure 2, protection messages are normally transmitted between relays via the station bus, whereas the continuous sampling messages are on the process bus emanating from the merging unit to several bay level IEDs.

In addition, since SAS messages are usually designed to operate equipments, dealing with system states, message security, especially the authenticity and integrity of SAS messages, is critical to prevent unauthorized equipment operations and detect forged system information. What is more interesting is that those delay-sensitive messages are also security-sensitive ones. For example, a protection message, which intends to isolate failures by changing ON/OFF statuses of circuit breakers, needs to be meticulously protected against malicious falsifications or forgeries in case of unexpected mal operations.

Therefore, the security challenge in SAS can be formulated as a joint mission, that is *to deliver a message with integrity protections within a predetermined time period to multiple receivers*. Considering a fact that security-related processing are normally time-consuming tasks, the more time critical a message is, the more challenging a corresponding security scheme is. A subsequent question is whether we have solutions to achieve the joint goals. To address this open question, we focus on two time-critical messages, that is, protection and data-sampling messages, to find out *whether current security schemes can be used to accomplish such a challenging task*.

Table 1: Timing requirements of message deliveries in substation automation systems.

Message types	Substation interior	Substation exterior
Protection	3 ms	8 ~ 12 ms
Monitoring and control	16 ms	1 s
Maintenance	1 s	10 s
Data sampling	3 ms	10 ms

3. Security Scheme Candidates

As aforementioned, since time-critical SAS messages are mostly related to critical equipment operations, message authenticity and integrity are of great importance for accurate and synergetic equipment controls. To prevent attackers from manipulating SAS messages in transit between substation devices, data origin authentication schemes [24] are extensively proposed to protect SAS messages for two purposes [18]: (1) to corroborate that incoming messages are originated from a legitimate sender as claimed; (2) to verify that the incoming message has not been tampered with. In this section, we briefly review several important data origin authentication mechanisms as solution candidates for protections of time-critical SAS messages, which are

either recommended solutions in standards and literatures, such as RSA [14] and one-time-signature-based schemes [16, 20], or promising approaches that have been verified in other networks, such as message-authentication-code-based schemes [15, 25, 26].

3.1. RSA. RSA is the most commonly used public key cryptography scheme, which is based on the presumed difficulty of factoring large integers [27]. In the smart grid, RSA is the primary choice of data authenticity and integrity protections via the generated RSA digital signature. Moreover, IEC62351, the most comprehensive standard on security issues of power systems, explicitly specifies RSA as the solution to protect time-critical messages [14] in substation automation systems.

According to specifications in IEC62351, a time-critical SAS message is firstly hashed by SHA256, and then the hashed message digest is encrypted by the RSA private key to generate a RSA signature, which is attached at the end of original message. At the receiver, the signature is decrypted by the transmitter's public key. Then, the receiver compares the decrypted hash value with the actual hash value of the received message. If the two agree, the message can be verified from the holder of the RSA private key and without any modification.

3.2. Message Authentication Code. MAC is a widely adopted symmetric-key cryptography scheme, which relies on a small fixed-size block of data to authenticate a message. To calculate an MAC, communication entities need to share a secret key since the MAC is a function of an arbitrary-length message and the shared key. We consider two typical MAC-based schemes to protect time-critical SAS messages.

(i) Incomplete-key-set scheme [25]: it is proposed to prevent malicious message forgeries in multicast scenarios. In this scheme, a complete key set is divided into multiple orthogonal subsets, which are further allocated to multicast receivers. Only the sender holds a complete key set with l keys, whereas each receiver only knows its own key subset. During the transmission, l MACs are calculated through l keys of the sender and appended with the original message. Receivers can only verify MACs based on their own key subsets but cannot fabricate other MACs from unknown key subsets.

(ii) Timed efficient stream loss-tolerant authentication (TESLA) [26]: it is characterized with an excellent computation efficiency and a low-communication overhead. The main idea of TESLA is that the sender uses different keys in different time slots to compute MACs attached with original messages and always discloses expired keys in current time slot to make receivers verify previously buffered messages. Accordingly, the sender is prone to corrupt falsifications since only expired keys will be published.

3.3. One-Time Signature. One-time signature [28] features a higher computation efficiency based on one-way functions without a trapdoor, which makes it suitable for fast message authentications. Since the idea was invented, a multitude of OTS algorithms [19, 29, 30] were proposed to overcome two intrinsic drawbacks, including the larger signature size, and the "one timedness" that means one key can only sign one message. Among these algorithms, hash to obtain random subsets (HORSs) [19] is recognized as the fastest one regarding signature generation and verification with shorter signatures. Also, HORS enables "multiple timedness" to sign multiple messages using one key if a security level decrease can be tolerated.

The nice features of HORS are further adopted in a time valid HORS (TV-HORS) scheme [16], which is specifically designed for integrity protections of time-critical messages in the power system. In the TV-HORS, one HORS key is reused to generate multiple signatures in a predetermined time period. Since the key reuse leads to a rapid decrease of the security level, which entails that an attacker gains more possibilities to forge a signature, it is necessary to ensure that the decreased security level is still strong enough to resist attacks. To this end, [16] illustrated a quantity relationship between achieved security levels and the allowable reuse number of one key. In the following sections, we focus on TV-HORS as an example of OTS-based scheme to demonstrate its performance in SAS message protections. We refer to the detailed HORS algorithm as follows.

(i) *Key Generation.* Generate t random l-bit strings $s_1, s_2, \ldots, s_t$ to be used as the private key K_{pri}. The corresponding public key is computed as $K_{\text{pub}} = \{v_1, \ldots, v_t\}$, where $v_i = f(s_i)$ and f is a one-way function.

(ii) *Signing.* To sign a message m, compute $h = \text{hash}(m)$, where Hash is a collision resistant hash function. Split h into k substrings $h_1, h_2, \ldots, h_k$ of length $\log_2 t$ bits each. Interpret each h_j as an integer i_j. The signature of m is $(s_{i_1}, s_{i_2}, \ldots, s_{i_k})$.

(iii) *Verification.* To verify a signature $(s'_{i_1}, s'_{i_2}, \ldots, s'_{i_k})$ for message m, compute $h = \text{hash}(m)$. Split h into k substrings $h_1, h_2, \ldots, h_k$ of length $\log_2 t$ bits each. Interpret each h_j as an integer i_j. Check if $f(s'_j) = v_{i_j}$ holds for each j.

Based on three types of data origin authentication schemes discussed above, we proceed to conduct an empirical study to measure delivery performance of secure SAS messages in a real setting testbed. Through performance analysis, we aim to answer the open research question, that is, *whether existing data origin authentication schemes can be readily used to protect SAS messages with stringent timing requirements.*

4. A Small-Scale SAS Prototype

To facilitate performance evaluations of time-critical SAS messages with different data origin authentication schemes,

we focus on two types of information, including teleprotection and data-sampling messages, for evaluations over a simple SAS prototype as described in IEC61850 [9], which is the dominant standard on substation automation systems. In this section, we firstly describe IEC61850 specified substation automation systems with emphasis on transmission protocols of time-critical messages. Then, we present implementations of our prototyped SAS testbed, including the hardware configuration and the application setup.

4.1. IEC61850-Based Substation Automation System. IEC-61850 is the most popular standard for the design of electrical substation automation, aiming to provide interoperability among diversified devices within substations. As shown in Figure 3, regular device operations are specified into a set of abstract services in IEC61850, such as abstract communication service interface (ACSI) for data queries and acquisitions, TimeSync for synchronization services, generic substation event (GSE, including generic object oriented substation events (GOOSE) and generic substation state event (GSSE)) for fast and reliable multicasting of substation event messages (e.g., protection messages regarding fault reporting), and sampled measured value (SMV) for sampled value multicasting. Then, such diversified abstract services are further instantiated into concrete application protocols and communication profiles through the specific communication service mapping (SCSM) according to different transmission requirements. For example, ACSI is mapped to leverage the manufacturing message specification (MMS) to query device data through TCP packets, whereas the synchronization messages are mapped onto UDP packets to synchronize substation devices.

Particularly, since GOOSE/SMV in IEC61850 undertakes transmission of time-critical protection and data-sampling messages, IEC61850 proposes a series of special designs to ensure efficient processing and transmissions of GOOSE/SMV messages [9, 13, 31]: (i) mapping GOOSE/SMV messages from the application layer directly to the link layer, to reduce processing time and avoid tedious protocol headers; (ii) conferring the highest transmission priority on GOOSE/SMV to avoid packet queuing and buffering; (iii) defining application layer retransmissions to replace the transport layer towards reliable transmissions.

In line with these design requirements, we develop a GOOSE/SMV module in the Linux kernel to ferry messages between applications and network adapters. Accordingly, we establish a prototyped SAS testbed with two simple time-critical applications, including relay protections and data sampling, based on the developed GOOSE/SMV module.

4.2. Implementations of the SAS Prototype. Figure 4 shows system implementations of our prototyped SAS testbed following the one-line diagram of the feeder I bay in Figure 2. We emulate IEDs used in the feeder I bay, including relay C, merging unit C, and the feeder I bay controller, all of which are running Ubuntu 10.03 with Linux 2.6.32. To simulate computation capacities of IEDs as embedded devices, the

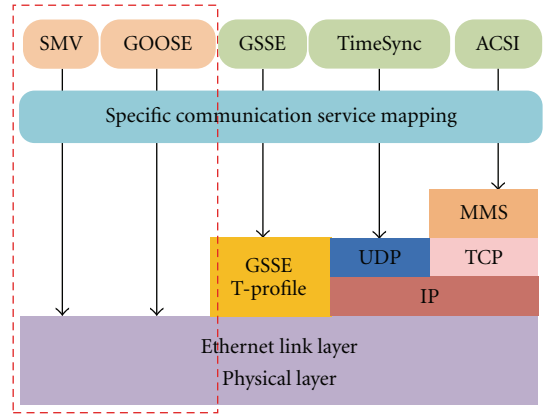

Figure 3: GOOSE/SMV protocol architecture in IEC61850.

CPU frequencies are tuned into a low processing speed. Moreover, the three emulated IEDs are connected in one-hop local networks established by a TRENDnet TE100-S8P 10/100 Mbps Ethernet Switch and a 54 Mbps 802.11 g Linksys Wireless Router as the dual process buses.

Besides hardware settings, a customized application software is also installed for each IED to send protection and data-sampling messages based on the implemented GOOSE/SMV module, as shown in Figure 5. To achieve security protections on GOOSE/SMV messages, we develop a security scheme lib using the OPENSSL [32] to involve aforementioned data origin authentication schemes, including RSA, MAC, and HORS. When transmitting messages, merging unit C firstly samples current or voltage values of the feeder via the ECT and EVT to generate corresponding messages. Then, the generated message is signed by security schemes, such as RSA, MAC, or HORS. According to IEC61850, the signed message bypasses the TCP/IP stack and is directly delivered to the network adapter driver through our GOOSE/SMV module. At the receiver, the GOOSE/SMV module submits received messages to the security lib for signature verifications. All verified messages will be finally accepted by Relay C for future processing.

Based on the established SAS testbed, we then carry out a series of experiments to measure delay performance of such secure SAS messages in two kinds of process buses, including the Ethernet and WiFi buses and analyze feasibilities of proposed security schemes.

5. Performance Results and Analysis

In this section, we aim to illustrate performance impacts of data origin authentication schemes on time-critical SAS messages and to address two questions specifically, (i) *whether existing data origin authentication schemes are satisfactory to protect time-critical SAS messages;* (ii) *what factors are bottlenecks that undermine the applicability of current security schemes in the SAS*. To proceed, we first introduce the performance metric and parameter settings of security schemes used in our experiments. Then, we present measurement

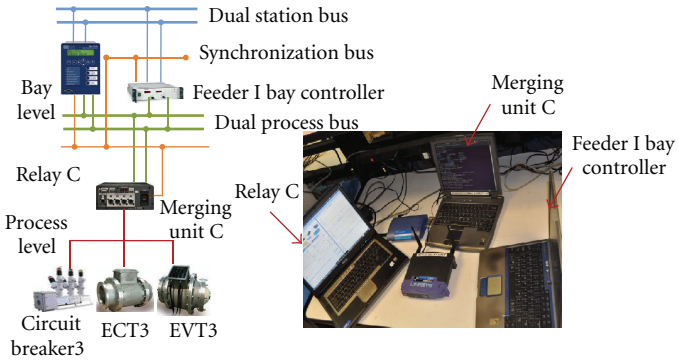

Figure 4: The hardware configurations of the prototyped SAS testbed.

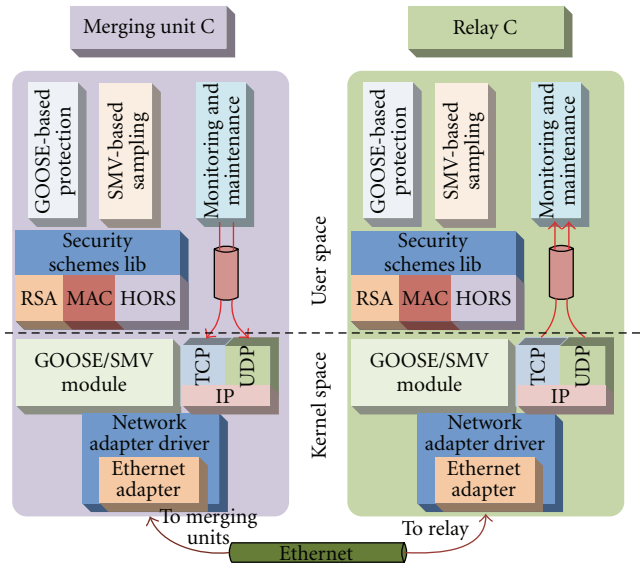

Figure 5: The software architecture of the prototyped SAS testbed.

results of implemented data origin authentication schemes in two deployed process buses, including the Ethernet and WiFi buses. Finally, we present the detailed performance analysis regarding scheme feasibilities and inherent scheme vulnerabilities.

5.1. Performance Metric. In evaluations of SAS messages along with security schemes, it is evident that traditional network metrics, such as delay, throughput, and packet losses, cannot be used, because they cannot reveal the fact that whether a security scheme is applicable to the SAS regarding stringent timing requirements. At the same time, we omit the security analysis on purpose, in that the detailed analysis of security functions can be easily found in [14–16, 19, 20]. More importantly, these solutions are selected for evaluations because of their satisfactory security features for messages protections. To this end, we take a *message validation ratio* as the performance metric, as defined in Definition 2.

Definition 2. The *message validation ratio* (MVR) is the proportion of the successfully delivered GOOSE/SMV messages to the total transmitted messages.

In other words, if 1000 GOOSE messages are transmitted, we take measures of delay of each message. Then, we compare the measured delay results with preset delay thresholds based on the message type in Table 1, for example, 3 ms for the bay-level interlocking and 10 ms for the stationwide interlocking. Only those whose delays are less than delay thresholds can be counted as successful deliveries for calculations of the validation ratio.

5.2. Parameter Settings. Since the message validation ratio varies dramatically with different parameters of security schemes, such as the key length and adopted hash functions, we specify parameters of security schemes on the following settings. As for RSA, we adopt a typical 1024-bit RSA key. For MAC, we use SHA-1 with a fixed 160-bit MAC length. Regarding HORS, we generate a 160-byte HORS signature, which is composed of 16 10-byte strings chosen from 1024 random strings. It entails three key parameters defined as per scheme descriptions in Section 3.3: $l = 80$ is the bit length of the element s_i in the private key; $k = 16$ is the number of exposed private key elements s_i in a signature; $t = 1024$ implies the total number of elements s_i in a private key.

5.3. Measurements of Security Schemes. We now investigate performance impacts of data origin authentication schemes on time-critical GOOSE/SMV message transmissions in two process buses, including the Ethernet bus and the WiFi bus, which are both the most widely used communication technologies in the smart grid paradigm [33–35].

5.3.1. Results in the Ethernet Process Bus

RSA-Signed Messages. Our first experiments are the implementation of RSA-signed GOOSE/SMV messages over the Ethernet bus. Figure 6 shows variations of message validation ratios along with the GOOSE/SMV message length and the CPU frequency of the signer, when taking 3 ms as the delay threshold. We can find that, compared with the message length, MVRs of *RSA-signed* messages are more susceptible to the CPU frequency, which is justified by a significant MVR rise when increasing the signer's CPU speed, from lower than 40% on 400 MHz to more than 85% on 1.2 GHz. This result reassure that the RSA performance is mainly dominated by

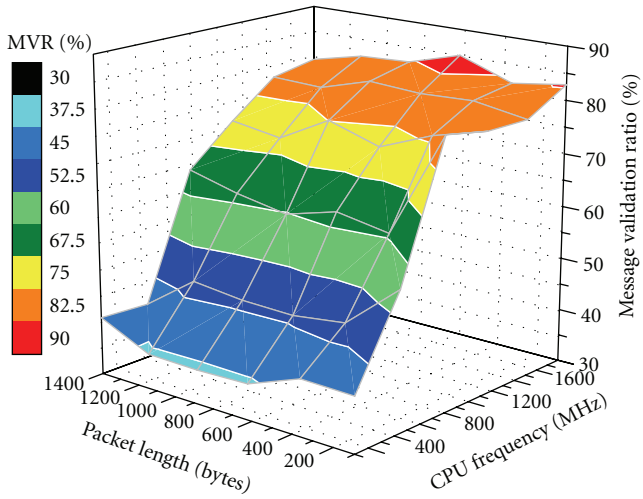

Figure 6: Message validation ratios of RSA-signed messages in the 3 ms delay threshold.

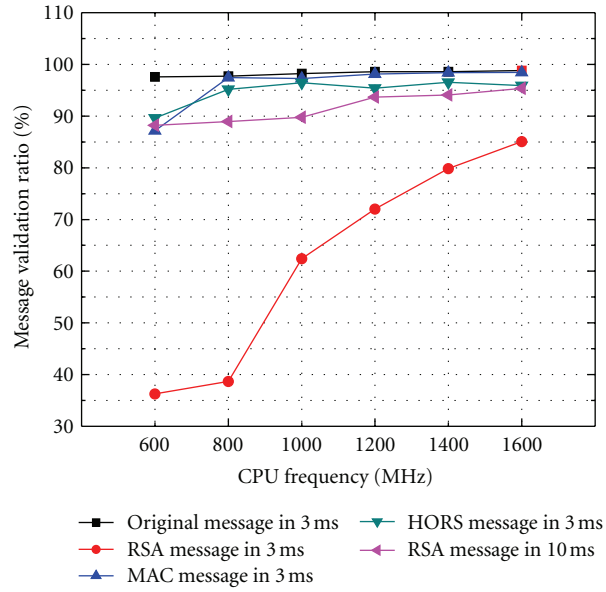

Figure 7: Performance comparisons among security schemes.

the signer's CPU frequency. In other words, when RSA is applied onto power electronic devices, the CPU capacity is a critical factor in IEDs.

As mentioned, most IEDs are microprocessor-based devices with constrained computation capacities. For example, SEL-3530 real-time automation controller [36], a popular IED production as the device controller, is furnished with a 533 MHz processor. According to Figure 6, such a CPU speed induces that more than 40% GOOSE/SMV messages cannot be signed and verified in 3 ms if using SEL-3530 as the device controller to transmit *RSA-signed* messages. Even with a faster CPU, like 1.6 GHz, message validation ratios of *RSA-signed* messages are still 15% lower than that of original GOOSE/SMV messages without security schemes, as shown in Figure 7. Therefore, we can infer that RSA is not suitable on the current off-the-shelf products for applications whose timing requirement is less than 3 ms.

Interestingly, if we relax delay constraints from 3 ms to 10 ms in Figure 7, performance of *RSA-signed* messages will dramatically catch up with that of original messages without digital signatures. In this case, RSA becomes an appropriate option for applications whose delay threshold is larger than 10 ms, such as operations across substations [9].

MAC-Attached and HORS-Signed Messages. In Figure 7, message validation ratios are almost the same in most situations among original messages, MAC-attached messages, and HORS-signed messages. It tells that both security schemes are potential solutions for application messages, whose timing requirements are less than 3 ms. The only exception occurs when the CPU frequency is set to 600 MHz, where message validation ratios of *MAC-attached* and *HORS-signed* messages are around 5% lower than that of original ones. Nonetheless, they are still close to 90%. Therefore, both MAC and HORS are arguably ideal cryptographic answers regarding delay performance in the Ethernet process bus.

Based on the above measurements, we can summarize that, RSA is not a suitable choice to secure time-critical messages with the 3 ms delay threshold, although it is a recommended solution in IEC62351 [14]. Nevertheless, if the delay threshold is extended to 10 ms [9], RSA is still viable. Therefore, we can deploy RSA to protect messages transmitted across substations, but cannot use it for teleprotection and data-sampling messages inside the substation. In addition, both *MAC-attached* and *HORS-signed* messages show satisfactory delay performance in the Ethernet process bus, which makes them as alternative choices to replace *RSA-signed* messages to protect time-critical data inside the substation.

Remark 3. Timing requirements of SAS messages are essential to evaluate the feasibility of data origin authentication schemes. With existing intelligent electronic devices in the power systems, RSA is not considered a good option for delay-sensitive teleprotection and data-sampling messages inside a substation. However, it remains to be a good candidate for messages to be delivered to the outside of substations, as well as nonteleprotection-related messages. For the Ethernet-bus-based SAS architecture, both *MAC-attached* and *HORS-signed* messages are suggested as good options for message authentications.

5.3.2. Results in the WiFi Process Bus. Different from Ethernet, transmissions in the WiFi bus are subject to more challenges due to the broadcast nature of wireless medium, which are more vulnerable to interferences and limited transmission rates. Especially for multicasted SAS messages, the transmission rate provided by the WiFi bus is much less than that in the 10/100 Mbps Ethernet. There are only three options in our settings, including 1 Mbps, 2 Mbps, and 6 Mbps. In the following experiments, we intend to

measure delay performance of *MAC-attached* and *HORS-signed* messages in the rate-limited WiFi process bus. Note that, since RSA does not show satisfactory performances in the Ethernet, we will only focus on the other two schemes in the WiFi test. To ensure results that are applicable to current off-the-shelf IEDs, we tune the CPU frequency to 600 MHz to emulate IEDs' computation capabilities.

Figure 8 shows delay performance of *MAC-attached* messages in different transmission rates of the WiFi bus. We observe an obvious decline of the message validation ratio when reducing the transmission rate from 6 Mbps to 1 Mbps. In 6 Mbps, the message validation ratio drops slightly along with the increase of the message length. However, in 1 Mbps and 2 Mbps, drops of message validation ratios become significant when increasing the packet length. The same situation also happens on *HORS-signed* messages, as shown in Figure 9. Comparing two figures, we can find that although declining trends are similar, dropping slops vary a lot. We further assume that given poor networking conditions, that is, limited multicasting rates in the WiFi bus, at most 20% transmission failures are acceptable if using the 3 ms delay threshold. In other words, the acceptable probability of the message validation ratio is at least 80% in the WiFi bus. From this assumption, we are motivated to define another metric, named as *message validation size* to evaluate performance differences implied in Figures 8 and 9, which is formally defined as follows.

Definition 4. Given a message validation ratio threshold, message validation size (MVS) denotes the maximum allowable packet length to meet the message validation ratio threshold on the probability.

The message validation size tells the capabilities of security schemes to protect message contents. If a scheme is efficient, it can carry more payloads, that is, more bytes can be contained in the original message without violating the statistical requirements of the message validation ratio during transmissions. Adversely, if a scheme is inefficient, it struggles to meet the probability requirement by reducing the packet length to save the processing time. We list message validation sizes of *MAC-attached* and *HORS-signed* messages in Table 2. According to the table, *MAC-attached* messages are able to transmit 75 bytes in the original payload in the 1 Mbps transmission rate, whereas *HORS-signed* messages can deliver 30 bytes contents when using the same rate. Moreover, based on the GOOSE/SMV message format specified in IEC62351 [14], 15 bytes are claimed by the GOOSE/SMV protocol for the protocol header, cyclic redundancy check (CRC), and other reserved fields. As a result, valid payloads are 60 bytes for *MAC-attached* messages, and 15 bytes for *HORS-signed* messages. Hence, we can infer that facing with limited bytes, message contents, that is, device data, should be organized efficiently to carry more valuable information, especially when using HORS-based scheme in the WiFi network, which only ensures a 15-byte payload for message contents.

The reason of such a phenomenon lies in the longer HORS signature. As illustrated in parameter settings, the size of an attached SHA-1 MAC is 160 bits, but the length of the HORS signature is up to 160 bytes. The longer HORS signature inevitably occupies more processing time, which should have been used for payloads.

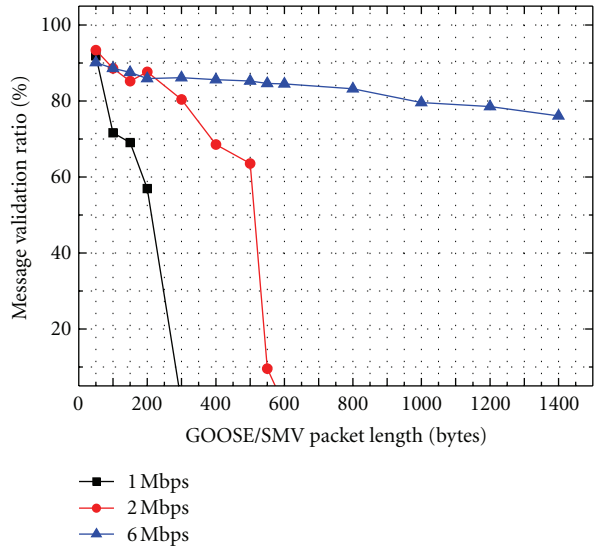

Figure 8: Message validation sizes of MAC-attached GOOSE/SMV messages in the WiFi process bus with 1 Mbps, 2 Mbps, and 6 Mbps multicasting rates.

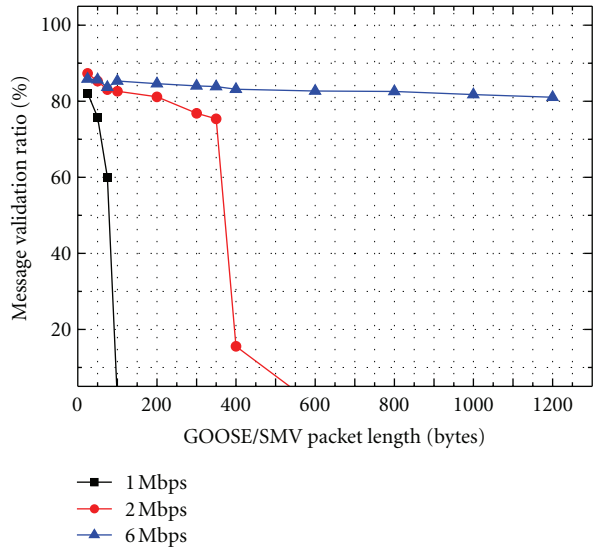

Figure 9: Message validation sizes of hORS-signed GOOSE/SMV messages in the WiFi process bus with 1 Mbps, 2 Mbps, and 6 Mbps multicasting rates.

Table 2: Message validation sizes of MAC- and HORS-signed messages in 80% MVR.

Message	1 Mbps multicasting	2 Mbps multicasting
MAC attached	75 bytes	300 bytes
HORS signed	30 bytes	200 bytes

Remark 5. When *MAC-attached* and *HORS-signed* messages are used in transmitting SAS messages over the WiFi bus, the transmission rate has a significant impact on the performance, that is, the message validation ratio. Our experiments reveal that at least 6 Mbps is required to achieve satisfactory performance for the multicasting SAS messages. However, in spite of significant declines of the message validation ratio, MAC and HORS still maintain a few bytes for valid payloads to deliver important, yet short messages with a higher message validation ratio. Therefore, both MAC- and HORS-based schemes can be recommended for time-critical SAS messages over the WiFi process bus.

5.4. Analysis of Data Origin Authentication Schemes. Since *MAC-attached* and *HORS-signed* messages exhibit satisfactory performance to secure time-critical GOOSE/SMV messages in the 3 ms delay requirement, we are encouraged to further consider data origin authentication schemes derived from MAC and HORS, such as TESLA [15], the incomplete-key-set scheme [25], and TV-HORS [16], for protecting the integrity and authenticity of time-critical SAS messages. Accordingly, an interesting question is *whether such excellent delay performances are enough to ensure MAC- and HORS-based schemes to be adopted as final solutions for message protections in the SAS*. To address this question, we elaborate details of security scheme feasibilities.

Constrains of TESLA. As one of the most efficient multicast authentication schemes, TESLA reduces authentication information to only one MAC and is widely used in sensor networks [15]. However, due to the concept of delayed authentications, which makes the use of buffer at the receiver side, that is, receiving packets first and waiting for the arrival of validation keys, additional waiting time may be induced in TESLA. Hence, the suitability of TESLA is totally determined by the interval between the arrival time of the current packet and the arrival time of the next packet, which is assumed to carry the released key for verifications of previous packets. As a result, there exist two contradictory suggestions. (i) TESLA is not applicable for GOOSE messages in deliveries of fault alarms. As transmissions of fault alarms are not continuous, the sender may not issue the next message for a long while. Thus, the receiver cannot verify previous alarms until the next fault triggers the next fault alarm. (ii) TESLA is applicable for continuous SMV messages only if the sampling rate is high enough to guarantee that the next message is able to arrive before the delay deadline. Therefore, careful performance investigations and meticulous system configurations are necessary before deploying TESLA for time-critical SAS message protections.

Constraints of the Incomplete-Key-Set Scheme. The incomplete-key-set scheme aims to leverage multiple MACs for multicasted data authentications. In experiments of *MAC-attached* messages, we observe that the GOOSE/SMV message attached with only one MAC shows excellent performance even in the worst network conditions. Nevertheless, the incomplete-key-set scheme requires multiple MACs attached within one message, which deduces two potential concerns. The first one is regarding multiple MACs, which leads to a larger packet size, as well as a longer transmission time. A promising solution is to truncate MACs in a shorter length, as referred to in [37]. The second one is the intrinsic scheme vulnerability for the collusion attack, in which bad members of a multicast group work together to retrieve a complete key set by manipulating their own key subsets, thereby fabricating valuable messages. Such a vulnerability is easy to be handled if keys are shared only in a small group, which is possible in some substations. For example, in a standard 69 kV distribution station, the total number of equipment controllers is 39, which is partitioned into 11 different bays. In that case, at most 5 devices are involved in a bay [38] to form a key shared group. The small size of the key shared group makes partitions of key sets more secure against the collusion attack. Therefore, the incomplete-key-set scheme is a promising solution for some substations, in which the number of IEDs is small.

Remark 6. Due to the high computation efficiency, MAC-based schemes are promising security solutions for time-critical SAS messages, even on off-the-shelf products with limited computation capabilities. The main challenge of MAC-based scheme lies in *how to remain the message security in a multicast scenario*, that is to ensure that receivers can verify the authenticity and integrity of multicast messages, but cannot generate valid MACs on behalf of the sender. Therefore, a reasonable way is to introduce *asymmetry* between the sender and multiple receivers to prevent fabricated MACs [24]. Since MAC is a symmetric-key cryptography, that is, the sender and the receiver share the same key material, MAC-based schemes have to seek other ways to achieve the envisioned *asymmetry* for the multicast scenario. For example, TESLA makes use of time as the source of *asymmetry* to create unfair knowledge of key materials in the time domain, while the incomplete-key-set scheme resorts to incomplete knowledge of key materials between communication entities to generate the *asymmetry*. Towards ideal MAC-based schemes in the SAS, the novel *asymmetry* should be taken with comprehensive considerations on impacts of specified application environments inside the substation, including features of traffic flows (discrete GOOSE messages and continuous SMV flows), available bandwidths, and the size of the multicast group.

Constraints of TV-HORS. The most salient feature of TV-HORS is "multiple timedness," which makes one private key to sign multiple messages. However, the more signatures one private key signs, the more exposed elements in the private key, which leads to a security level decrease and provides attackers more opportunities to counterfeit a message from released private key elements. To analyze the relationship between the security level and the maximum reuse time of the key, we resort to the following formulation defined in [16], that is, $L = k \log_2(t/vk)$. The notations are as follows:

(i) L denotes the security level that implies that an attacker has to compute 2^L hashes on average to obtain a valid signature for a new message;

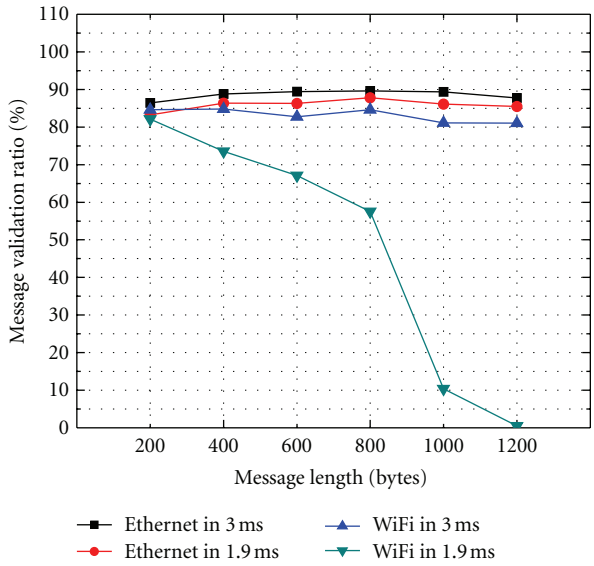

Figure 10: Message validation ratios of HORS-signed messages with different delay thresholds.

(ii) k indicates the number of exposed private key elements in one signature;

(iii) t is the total number of elements in a private key;

(iv) v tells allowable key reuse times, namely, the maximum number of messages signed by one key.

For the sake of an intuitive understanding, we take a concrete parameter set as the example $L = 44$, $k = 11$, $t = 1584$, and $v = 9$, which is computed from the previous equation. In this setting, one private key can be reused at most 9 times to ensure that the resulting security level is not less than 44, which is a medium security level [16]. In terms of GOOSE messages, which is usually used to report alarms, 9 times are high enough since fault occurrences are discrete in a low frequency. Accordingly, the key reuses can be allocated separately into multiple fault alarms.

However, the story is totally different in SMV messages, which features continuous transmissions in a high sampling rate. For example, for protection operations, the sampling rate of three phase currents and voltages can achieve 4800 samples per second, each of which should be contained in one message [9, 39]. It means that the merging units are expected to multicast 4800 messages every second to the relay and the bay controller in Figure 4 to report real-time current and voltage measures. At this rate, 9 times key reuse can last at most 1.9 ms, that is, a key update occurs every 1.9 ms. The corresponding key update frequency is 526 times per second. From this point, we reveal two potential threats that may be hijacked by attackers to compromise the integrity protection provided by HORS.

Delay Compression Attacks. The limited times of the key reuse induce that one key may expire very soon, around 1.9 ms in our parameter setting. Once the key is expired, the signed messages will not be valid any more. In other words, signed messages must be verified in 1.9 ms. It actually proposes another timing requirement for message validations, which is different from the 3 ms delay threshold required by message deliveries. Thus, the timing requirement is further squeezed to 1.9 ms from 3 ms. Figure 10 shows performance of *HORS-signed* messages in different delay thresholds. The tighter delay threshold results in at least 5% MVR decreases in the Ethernet bus, and even more in the WiFi bus when the message length is increasing. Therefore, the "multiple timedness" TV-HORS brings in tighter timing requirements to deteriorate message validation ratios, when the scheme is utilized to protect the high-rate sampling messages. As a result, we name the decreasing effect of message validation ratios as a *delay compression attack* launched by compressing the delay threshold.

Table 3: Key generation time of TV-HORS on different devices.

Device	CPU	Algorithm	Time(s)
Laptop	1.33 GHz	SHA-1	1.598
		SHA-256	2.787
TS-7800	500 MHz	SHA-1	17.496
		SHA-256	29.029
TS-7250	200 MHz	SHA-1	20.4
		SHA-256	32.14

Key Depletion Attacks. According to the parameter setting, the signing key needs to be updated 526 times in one second, which implies a huge key consumption. Since SMV messages are usually used in the long-term device monitoring, even throughout the entire life of devices, the HORS-based scheme should be self-contained on devices, which entails that TV-HORS needs to replenish keys by itself. Table 3 illustrates capabilities of key generations on different devices. It shows required computation time to generate 526 keys for one second key consumptions over different embedded devices, whose computation capabilities are comparable with the off-the-shelf IED products. It is obvious that the key generation speed is slower than the consumption speed. With the mismatched speed, attackers can easily achieve a key depletion attack to exhaust stored keys and compromise the entire integrity protection system by a large amount of bogus messages.

Therefore, OTS-based schemes, like HORS, are far from practical deployments, since the allowable reuse times of a key are still relatively low, although it has been extended a lot in the past decades of years. With such limited key reuse times, the scheme tends to show more disadvantages to derive delay compression attacks, as well as key depletion attacks, in which OTS-based schemes seem to be message attackers, rather than message protectors.

Remark 7. Different from MAC-based schemes, OTS-based schemes rely on the *asymmetry* derived from asymmetric key materials. To maintain the security of the scheme, the sender and receivers have to maintain the only *asymmetry* on the key materials. That is why multicast communication

entities keep updating their keys during SMV transmissions. Therefore, we can infer that the fundamental reason of two illustrated new attacks, including delay compression attacks and key depletion attacks, lies in the strong dependence of TV-HORS on the key asymmetry. To avoid such a strong dependence on asymmetric key materials, a possible way is to introduce new *asymmetries* to create hybrid *asymmetries*. Accordingly, it may deduce novel OTS-based schemes, dealing with high-rate transmitted messages in the substation.

6. Conclusion and Future Works

In this paper, we studied security solutions for time-critical messages in the smart grid by taking an experimental approach on a small-scale substation automation system prototype, with the focus on extensively proposed data origin authentication schemes. The main challenge for security schemes in the substation is to accomplish a joint mission to ensure security requirements on message authenticity and integrity, along with strict timing requirements on message deliveries. In particular, we have several interesting observations regarding performance of security schemes in time-critical transmissions. For instance, we find that RSA, which is recommended for the smart grid, is a good solution for nonteleprotection messages, while it is not appropriate for delay-sensitive messages inside the substation. Our results reveal that, diversified application environments of the substation automation system, such as device computation capabilities, message traffic features, fluctuant network bandwidths, and stringent timing requirements, have immediate and significant impacts on performance of data origin authentication schemes and may result in completely different suggestions in terms of scheme feasibilities. More importantly, design limits of security schemes, including clumsy computations, additional waiting delays, and short key valid time, may turn the strength of these algorithms into vulnerabilities when they are applied into substation automation systems. Therefore, there is an acute need for security solutions towards an efficient, yet secure substation automation system in the smart grid.

Acknowledgments

This work was supported by ERC Program of the National Science Foundation under Award no. EEC-0812121. A part of this work was published in the 2011 IEEE Military Communications Conference (Milcom'11).

References

[1] Office of the National Coordinator for Smart Grid Interoperability, "NIST framework and roadmap for smart grid interoperability standards, release 1.0," NIST Special Publication 1108, 2010.

[2] W. Wang, Y. Xu, and M. Khanna, "A survey on the communication architectures in smart grid," *Computer Networks*, vol. 55, no. 15, pp. 3604–3629, 2011.

[3] Y. Zhang, M. Prica, M. D. Ilic, and O. K. Tonguz, "Toward smarter current relays for power grids," in *Proceedings of the IEEE Power Engineering Society General Meeting (PES '06)*, June 2006.

[4] M. H. Albadi and E. F. El-Saadany, "Demand response in electricity markets: an overview," in *Proceedings of the IEEE Power Engineering Society General Meeting (PES '07)*, June 2007.

[5] Power Systems Engineering Research Center, *The 21st Century Substation Design*, PSERC Publication, 2010.

[6] R. Ellenbogen, "At load power factor correction," in *New York State Energy Research and Development Authority*, 2009.

[7] Department of Agriculture, "Design guide for rural substations," 2001.

[8] T. S. Sidhu, M. G. Kaanabar, and P. Parikh, "Implementation issues with iec61850 based substation automation systems," in *Proceedings of the 15th National Power Systems Conference (NPSC '08)*, 2008.

[9] IEC, *IEC 61850 Communication Networks and Systems in Substations*, 2003.

[10] EWICS, "Electric power systems cyber security: power substation case study," in *Proceedings of the European Workshop on Industrial Computer Systems*, 2006.

[11] P. Hines, B. O'Hara, E. Cotilla-Sanchez, and C. Danforth, "Cascading failures: extreme properties of large blackouts in the electric grid," *SIAM Mathematics Awareness Month*. In press.

[12] E. M. Brunner and M. Suter, *International Critical Information Infrastructure Protection Policies Handbook 2008/2009*, ETH, Zurich, Switzerland , 2008.

[13] Z. Lu, X. Lu, W. Wang, and C. Wang, "Review and evaluation of security threats on the communication networks in the smart grid," in *Proceedings of the IEEE Military Communications Conference (MILCOM '10)*, pp. 1830–1835, November 2010.

[14] IEC62351, "Power systems management and associated information exchange—data and communications security," International Electrotechnical Commission, Geneva, Switzerland, 2007.

[15] A. Perrig, R. Canetti, D. Song, and J. D. Tygar, "Efficient and secure source authentication for multicast," in *Proceedings of the Network and Distributed System Security Symposium (NDSS '01)*, pp. 35–46, 2001.

[16] Q. Wang, H. Khurana, Y. Huang, and K. Nahrstedt, "Time valid one-time signature for time-critical multicast data authentication," in *Proceedings of the 28th Conference on Computer Communications (INFOCOM '09)*, pp. 1233–1241, April 2009.

[17] Europe Task Force Smart Grids, *Expert Group 2: Regulatory Recommendations for Data Safety, Data Handling and Data Protection*, 2011.

[18] H. Khurana, R. Bobba, T. Yardley, P. Agarwal, and E. Heine, "Design principles for power grid cyber-infrastructure authentication protocols," in *Proceedings of the 43rd Annual Hawaii International Conference on System Sciences (HICSS '10)*, January 2010.

[19] L. Reyzin and N. Reyzin, "Better than BiBa: short one-time signatures with fast signing and verifying," in *Proceedings of the 17th Australasian Conference on Information Security and Privacy (ACISP '02)*, 2002.

[20] Q. Li and G. Cao, "Multicast authentication in the smart grid with one-time signature," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 686–696, 2011.

[21] V. H. Todd, *Protective Relays: Their Theory, Design, and Practical Operation*, 1922.

[22] K. Harker, *Power System Commissioning and Maintenance Practice*, Power Series 24, IEE, 1998.

[23] IEEE, "IEEE standard communication delivery time performance requirements for electric power substation automation," IEEE Std 1646-2004, 2005.

[24] Y. Challal, H. Bettahar, and A. Bouabdallah, "A taxonomy of multicast data origin authentication: issues and solutions," *IEEE Communications Surveys and Tutorials*, vol. 6, no. 3, pp. 34–57, 2004.

[25] R. Canetti, J. Garay, G. Itkis, D. Micciancio, M. Naor, and B. Pinkas, "Multicast security: a taxonomy and some efficient constructions," in *Proceedings of the 18th Annual Joint Conference of the IEEE Computer and Communications Societie (INFOCOM '99)*, pp. 708–716, March 1999.

[26] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "Efficient authentication and signing of multicast streams over lossy channels," in *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 56–73, May 2000.

[27] R. L. Rivest, A. Shamir, and L. Adleman, "method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[28] R. C. Merkle, "A certified digital signature," in *Proceedings of the Advances in Cryptology (CRYPTO '89)*, 1989.

[29] A. Perrig, "The BiBa one-time signature and broadcast authentication protocol," in *Proceedings of the 8th ACM Conference on Computer and Communications Security (CCS '01)*, pp. 28–37, November 2001.

[30] D. Naor, A. Shenhav, and A. Wool, "One-time signatures revisited: have they become practical," Tech. Rep., 2005.

[31] Z. Lu, W. Wang, and C. Wang, "From jammer to gambler: modeling and detection of jamming attacks against time-critical traffic," in *Proceedings of the 30th IEEE International Conference on Computer Communications, Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '11)*, pp. 1871–1879, Shanghai, China, April 2011.

[32] OPENSSL, http://www.openssl.org/.

[33] V. C. Gungor and F. C. Lambert, "A survey on communication networks for electric system automation," *Computer Networks*, vol. 50, no. 7, pp. 877–897, 2006.

[34] B. Akyol, H. Kirkham, S. Clements, and M. Hardley, *A Survey of Wireless Communications for the Electric Power System*, 2010.

[35] NIST Smart Grid, "Smart grid panel agrees on standards and guidelines for wireless communication, meter upgrades," *News Release*, 2011.

[36] Schweitzer Engineering Laboratories, "SEL-3530-4," http://www.selinc.com/sel-3530/.

[37] C. Szilagyi and P. Koopman, "Flexible multicast authentication for time-triggered embedded control network applications," in *Proceedings of the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN '09)*, pp. 165–174, July 2009.

[38] T. S. Sidhu and Y. Yin, "IED modelling for IEC61850 based substation automation system performance simulation," in *Proceedings of the IEEE Power Engineering Society General Meeting (PES '06)*, June 2006.

[39] A. Apostolov, "Testing of complex IEC 61850 based substation automation systems," *International Journal of Reliability and Safety*, vol. 2, no. 1-2, pp. 51–63, 2008.