USEFUL AUTHENTICATION MECHANISM FOR IEC 61850-BASED SUBSTATIONS

Nastaran Akbari
Mashhad Electric Energy Distribution Company (MEEDC), Iran
akbari.nastaran@gmail.com

M.H.Yaghmaee
Mashhad Electric Energy Distribution Company (MEEDC), Iran
yaghmaee@ieee.org

Davod Noori
Mashhad Electric Energy Distribution Company (MEEDC), Iran

S.Hedaiat Akhbari
Mashhad Electric Energy Distribution Company (MEEDC), Iran
Hed_lan@yahoo.com

ABSTRACT

By increasing the use of Ethernet and Internet in electricity industry and particularly in IEC 61850-based substation automation systems, the possibility of cyber-attacks and authenticity of exchanged messages has increased. Such invasions would make catastrophic consequences in power grids; so, serious consideration in security of automation systems can result in more stable operational conditions. Despite the fact that security issues in IEC 61850 based substations located in high priorities, but most of the methods have not responded to complicated problems like complex computations, long keys and signature, and no consideration to multicast communications and so on.

The purpose of this paper is to present a method based on the IEC 61850 substation security issues and limitations. In the proposed schema which is based on OTS schemas, the signature length is reduced and the system is resistant against replay attack.

INTRODUCTION

Due to the use of communication technologies in smart grids, efficient network management is provided. Communication networks play a key role in the stability and performance of smart grids[1-3]; So, IEC 61850 standard is provided for substations and affected substations internal communications, external communications between substations and SCADA systems[4]. The main objective of using IEC 61850 is to solve interoperability issues between substation systems from different vendors; therefore, this standard has not paid much attention to security concerns. It should be noted that power networks are different from the secure environment of the Internet, for example DOS attacks will have a destructive effect on the network[5].

Substations have an important role in distribution network. The main core of substation automation is smart communication systems which connect all system components efficiently. Multicast communications have an important role in these systems because they enable efficient communication between one sender and multi receivers. Therefore, attacking this communication structure jeopardizes national and economic security. One of the best security solutions to deal with these threats is using authentication mechanisms. By using these mechanisms, each receiver can determine whether the message has been sent from a specific sender or not, and whether or not the message has changed in the way and also it can detect errors in the system. If the messages are not authenticated, the attacker can easily alter or forge messages or he can replay an old message[6].

Although multicast authentication is very important in substation, it has not been enough attention to this issue due to the unique requirements and limitations of substations. Authentication in this situation must be done quickly and efficiently, because many multicast messages such as GOOSE are delay sensitive and some substation devices have limited resources. Thus methods such as digital signatures based on public key[7], proposed methods in [8,9] and [10] are not appropriate for substations for a variety of reasons. In recent years, some methods have been presented based on OTS schemas [11,12] which can authenticate real-time multiple messages. The methods presented in [11-14,6] beside authenticate real-time multiple messages, have a suitable computational cost; However, the memory overhead and the signature size of these methods are enormous for use in smart grids and electrical substations, which have limited resources.

In this paper, suitable authentication mechanism has been provided to be used in power substations based on IEC 61850. The signature size of our method is declined as compared with other methods; therefore, bandwidth usage and messages size will drastically reduce. It is also resistant against replay attack which is one of the major attacks.

In the following, authentication mechanisms, their advantages and disadvantages will be reviewed, then our schema which is designed for use in substations will be described and it will be evaluated in terms of efficiency and security. Finally, the proposed method is being compared with other existing methods.

REVIEW

Digital signature based on public key [15] is one of the popular methods for multicast authentication, which is not appropriate for use in IEC 61850-based substations due to high computational cost because of limited IED resources and delay sensitive messages.

Although authentication based on symmetric methods [16,17] is fast, is not recommended to use in power substations because the secret key in these methods must be shared between sender and receiver. Considering that lots of equipment communicating with each other in substations and multicast messages are so important, a large number of keys must be exchanged between the transmitters and receivers with this method, which applies a high cost to the system. Therefore, using these methods in multicast communications is not only affordable but also in some cases drastically reduces security. One of the symmetric-based methods is TESLA[14]. The above problems have been resolved in this method and related methods [18,19]; however, these methods are not suitable for substations due to large messages buffering delay.

Hybrid message authentication methods are presented in [9,20]. These methods use both public key and hash functions idea, thus the computational cost are reduced. The advantage of these methods is distributing public key authentication and validation cost into multiple messages, but their problem is that all messages with part of a signature must be kept until the last message which contains last part of signature, received. As a result, the delay caused by buffering messages does not respond to messages timing requirements, thus using these methods in electrical substations containing real-time messages is not right.

One time signature methods such as [21,22] is one of authentication mechanism which has high speed. In these methods, public and private key is used for signing and authentication. Despite the existence of public key and private key, signing and validation is done quickly due to the use of hash functions and they are also efficient in terms of time. However, These methods have disadvantages too such as high signature size and key length. Several methods such as [6, 11-13, 23] have been presented to resolve the above problems, but some of them are not suitable for IEC-61850 based substations with specific requirements and restrictions. Our proposed method will be discussed in the next section.

THE PROPOSED METHOD

In the proposed method the following symbols will be used. *k*, *z*, *l* and *t* are security parameters, function f:$\{0,1\}^l \rightarrow \{0,1\}^l$ is a one-way permutation functional on *l*-bit strings. $f^k(x)$ is used to show the number of applied *f* to the value of x and *H*(.) is a one way hash function that converts input to $klog_2t$ length output. *G*(.) is a one way hash function in random oracle model which is shown as $G:\{0,1\}^* \rightarrow \left[0,\binom{z-1}{k-1}\right]$ [13].

Another function is $C_{k,z}$, input of this function is the output of G. This function is used to form the various combinations which is equal to z. As mentioned in [13], the following equation is used to implement this function.

$$\sum_{i=1}^{k} a_i = z \qquad (1)$$

In our schema, sender and receiver maintain internal states of the system in multicast authentication; This means that the sender save the number of used chains as internal state of the system and receiver keeps current public key; Thus multicast messages can be easily signed. The proposed scheme consists of three steps: key generation, signature generation and validation. In the following, each step is described with more details.

Key generation: first of all, *t* random *l* bit strings are generated. Then *d*-length chains as $s_i \rightarrow f^1(s_i) \rightarrow \cdots \rightarrow f^{d-1}(s_i)$ generated for each string. T chains form private key and public key for all *i*, where $1 \le i \le t$, is equal to $v_i = f^d(s_i)$.

Signature generation: sender stores the number of used chains for each *t* generated chain in key generation phase, as (b_1,...,b_t) parameters and he also generate g by applying G on message m. It should be noted that, our schema uses a bijective function $C_{k,z}$. The inputs of this function are: m, k, z and g, where 0<g<$\binom{z-1}{k-1}$, and the output is the g-th solution of the following equation: $\sum_{i=1}^{k} a_i$, where a_i is an integer such that $a_i \geq 1$ [13]. After using $C_{k,z}$, the hash value (*h*) must be generated by applying a cryptographic hash function *H* on the concatenation of *m* and *sq*, and the result of this step must be mapped into *k* substrings $h_1,\ldots,h_k$. Then, all h_i , where $1 \le i \le k$, must be interpreted as i_j, where $1 \le i_j \le t$ and $1 \le j \le k$. Now random function should be used to generate random value *p*, between 1 and *k*, which is the index of i_j. At the end of this phase, internal state b_{i_p} is equal to: $b_{i_p} = b_{i_p} + a_p$, and the signature is:

$$\mathrm{sig_p} = \mathrm{f}^{\mathrm{d}-\mathrm{b}_{\mathrm{i_p}}}(\mathrm{s}_{\mathrm{i_p}}) \qquad (2)$$

At the end of this phase, signature, *p*, *sq* and message will be sent to receivers such as IEDs.

Validation: in this step, internal state of receiver is current public key and it is shown as (u_1,…,u_t). To validate received signature ($\mathrm{sig_p}$), the same procedure as signature generation in transmitter must be performed. It means that first of all function G and $C_{k,z}$ shall apply to the message, then hash value is prepared by applying *H* on concatenation of *m* and *sq*. After that, the calculated value divided into *k* parts and each part interprets as a number between 1 and *t*. Finally, value with index *p* is selected and equation 3 is checked.

$$f^{a_p}(sig_p) = u_{i_p} \qquad (3)$$

After examining the equation three, one of the following scenarios occurs:

- If the equation is not available, the authentication fails because the message or *sq* has been changed. In this case, an error message is sent to a system engineer.
- If the equation 3 is right, the following steps will be done:

- $u_{i_p} = sig_p$
- Received *sq* compared with current *csq* and one of the following states will be happened.
  - If(*sq*>*csq*) then sender's *csq* value in receiver is equal to received *sq* and validation will be done successfully.
  - If(*sq*<*csq*) then replay attack has happened. In this case, an attacker intercepts the message and sends it to receiver with long delay, so that other messages have been sent to the receiver before sending a message by an attacker. Finally, validation fails and alert is sent to electrical engineer.
  - If (*sq*=*csq*) then replay attack has happened. In this case, an attacker intercepts the message and sends the same message to the recipient. If the message is not received, the recipient accepts it and otherwise due to get the same message at receiver replay attack is detected; so, message and signature will not be accepted and alert will be sent to system due to repeating attack and receiving identical message on behalf of the receiver.

ANALYZING THE PROPOSED METHOD

In this section, proposed method will be evaluated from different aspects, and it will be compared with other existing methods.

Performance Evaluation

In this section, the cost of key generation, signature generation and validation of proposed method are evaluated based on the number of permutations and one-way hash functions. In the key generation phase, we need to use permutation function *f* for *t* times, because *t* initial value exists in which keys generated by applying function *f*, *d* times. Private key length is *dtl*-bit and public key length is *tl*-bit because the length of each *t* is *l*-bit long. Signature length of proposed schema is *l*+*log*|*c*| bit and signature cost is 2 because it only requires to apply one function *G* and one *H*. According to the proposed schema, the receiver validation function needs to apply a function *G*, *H* and function *f* for a_p times; so, validation cost is equal to a_p+2.

Security évaluation

In this section, we will discuss the security evaluation of our proposed method against non-chosen message attack. We assume that an attacker have signature for an arbitrary message, independent of *G* and *H*. With this information, the attacker tries to forge a signature for any arbitrary messages.

We assume that an attacker has a valid signature *sig*, we want to calculate the probability in which an attacker can forge signature by applying one *H* and *G* on any arbitrary message *m*'. Suppose that *H* generate random strings and both functions *f* and *H* are irreversible. Since the signature is a random number which is the result of different combinations of z, it is impossible to use $f^i(sig_p)$, $i \geq 1$ to forge signature. To forge the signature, the inverse of the function *f* should be calculated which is not possible according to the definition of *f*; thus, an attacker must only use the signature i.e. *sig* to forge the signature.

In the proposed method, the attacker must exactly map an arbitrary message m′ to *sig*. In order to do this, *m* must be mapped to *k* parameter ($s_1,\ldots,s_k$) and then one of these parameters selected using a specific procedure. Considering that the attacker does not have access to the private keys, he cannot easily forge the signature since he must compute 2*l* values to achieve private key. In this case, the probability to obtain the signature is $\frac{1}{2^l}$ which is too small. Considering the fact that in most of HORS-based OTS schema, the length of *l* is 80 bit or more, thus the value of $\frac{1}{2^l}$ is too small if *l* is equal to minimum possible value (80). Furthermore, the probability to choose g in *G(m)=g* is $\frac{1}{\binom{z-1}{k-1}} = \frac{1}{\frac{(z-1)!}{(k-1)!(z-k)!}} = \frac{(k-1)!(z-k)!}{(z-1)!}$. As a result, the probability of forgery is obtained from the equation mentioned above.

$$\text{F-Prob} = \frac{(k-1)!(z-k)!}{(z-1)!2^l} \qquad (4)$$

Considering the small value of equation (4) and specific substation condition such as real-time communication and etc. , it can be observed that our proposed method is robust.

Compare with other methods

In table I, the performance of the proposed method is compared with that of Biba, HORS, TSV and HORSIC in terms of computational cost and security. As it can be seen in this table, our schema signature length has been reduced in comparison with other schemas. Furthermore, validation cost has been reduced due to use *a*, $a << z$. In this table, notations $\xi = \mu \prod_{r=1}^{g} (n_r!)$,

$\mu = \frac{t^k}{t(t-1)\cdots(t-k+1)}$ and $z = \sum_{i=1}^{k} a_i$ for $a_i \geq 1$

are used.

Table I:The comparison of our schema with the others

Method	Key generation cost	Signature generation cost	Validation cost	Sig size	Public key size	Resistance against replay attack
Biba[12]	t	2t	2k+1	kl	tl	
HORS[11]	t	1	k+1	kl	tl	
TSV[6]	(max{w_1+$\ldots + w_g$ }+1)t	ξ	$\sum_{r=1}^{g} n_r w_r$	kl+log ξ	tl	
HORSIC[13]	dt	$\mu+1$	z+2	kl+log μ	tl	
Our schema	dt	2	$a_p + 2$	l	tl	+

CONCLUSION

In this paper, an authentication mechanism was presented which is suitable for IEC 61850-based substations which is one of the important parts of distribution systems. This schema can support multicast authentication which is the most important type of communications in electrical substations. To achieve this objective, three main steps have been considered. In the first step, key generation, in the second step signature generation and sending it to receiver, and in the third step message authentication is done. If the authentication is done successfully, the rest of the procedure will be done normally; otherwise, the procedure will be stopped and message error will be sent to the person in charge.

Total size of signature has been significantly reduced, because of sending one signature instead of k signature to the receiver, so memory and bandwidth usage has been decreased. In addition, this schema is resistant against replay attack which is one of the important attacks in electrical substations.

REFRENCES

[1] S. M. Amin and B. F. Wollenberg. (2005, September) Toward a Smart Grid: Power Delivery for 21st Century. *IEEE Power and Energy Magazine*. 34–41.

[2] A. L. G. N. S. Prasanna, S. Sumanth, V. Simha,J. Bapat, and G. Koomullil, "Data Communication over the Smart Grid," presented at the in Proc. of IEEE Int. Sump.Power Line Communications and Its Applications, 2009.

[3] G. R. E. Santacana, T. Tang, and F. Xiaoming. (2010, March) Getting Smart. *IEEE Power and Energy Magazine*. 41–48.

[4] S.-W. Z. S.-J. Rim, and S.-J. Lee, "Development of an Intelligent Station HMI in IEC 61850 Based Substation," *Journal of Electrical Engineering & Technology*, vol. 4, pp. 13-18, 2009.

[5] S.-S. K. Hyo-Sik Yang, Hyuk-Soo Jang, "Optimized Security Algorithm for IEC 61850 based Power Utility System," *Journal of Electrical Engineering & Technology*, vol. 7, pp. 443-450, 2012.

[6] Q. L. a. G. Cao, "Multicast Authentication in the Smart Grid With One-Time Signature," *IEEE TRANSACTIONS ON SMART GRID*, vol. 2, 2011.

[7] W. Ertel, *Angewandte Kryptographie*: Hanser Verlag, 2007.

[8] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "Efficient authentication and signing of multicast streams over lossy channels," in *Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on*, 2000, pp. 56-73.

[9] D. Song, D. Zuckerman, and J. Tygar, "Expander graphs for digital stream authentication and robust overlay networks," in *Security and Privacy, 2002. Proceedings. 2002 IEEE Symposium on*, 2002, pp. 258-270.

[10] A. Perrig, D. Song, R. Canetti, J. Tygar, and B. Briscoe, "Timed efficient stream loss-tolerant authentication (TESLA): multicast source authentication transform introduction," RFC 4082, June2005.

[11] L. Reyzin and N. Reyzin, "Better than BiBa: Short one-time signatures with fast signing and verifying," in *Information Security and Privacy*, 2002, pp. 144-153.

[12] A. Perrig, "The BiBa one-time signature and broadcast authentication protocol," in *Proceedings of the 8th ACM conference on Computer and Communications Security*, 2001, pp. 28-37.

[13] J. Lee, S. Kim, Y. Cho, Y. Chung, and Y. Park, "HORSIC: An efficient one-time signature scheme for wireless sensor networks," *Inf. Process. Lett.*, vol. 112, pp. 783-787, 2012.

[14] Q. Wang, H. Khurana, Y. Huang, and K. Nahrstedt, "Time valid one-time signature for time-critical multicast data authentication," in *INFOCOM 2009, IEEE*, 2009, pp. 1233-1241.

[15] M. Branchaud, "A survey of public-key infrastructures," McGill University, 1997.

[16] N. FIPS, "180-2: Secure hash standard (SHS)," Technical report, National Institute of Standards and Technology (NIST), 2 001. **http://csrc**. nist. gov/publications/fips/fips180-2/fips180-2withchangenotice. pdf2001.

[17] F. Pub, "198, the keyed-hash message authentication code (hmac)," *Federal Information Processing Standards Publication*, vol. 198, 2002.

[18] D. Liu and P. Ning, "Multilevel μTESLA:

Broadcast authentication for distributed sensor networks," *ACM Transactions on Embedded Computing Systems (TECS)*, vol. 3, pp. 800-836, 2004.

[19] D. Liu, N. Peng, Z. Sencun, and S. Jajodia, "Practical broadcast authentication in sensor networks," in *Mobile and Ubiquitous Systems: Networking and Services, 2005. MobiQuitous 2005. The Second Annual International Conference on*, 2005, pp. 118-129.

[20] C. Karlof, N. Sastry, Y. Li, A. Perrig, and J. Tygar, "Distillation codes and applications to DoS resistant multicast authentication," in *Proceedings of the ISOC Symposium on Network and Distributed System Security (SNDSS)*, 2004, pp. 37-56.

[21] L. Lamport, "Constructing digital signatures from a one-way function," Technical Report CSL-98, SRI International1979.

[22] S. Goldwasser, S. Micali, and R. L. Rivest, "A digital signature scheme secure against adaptive chosen-message attacks," *SIAM Journal on Computing*, vol. 17, pp. 281-308, 1988.

[23] W. D. Neumann, "HORSE: an extension of an r-time signature scheme with fast signing and verification," in *Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004. International Conference on*, 2004, pp. 129-134 Vol.1.