Securing Indirect Communication for Advanced Metering Infrastructure in Smart Grid

Mustafa Saed
Electrical and Computer Engineering
University of Detroit Mercy
Detroit, USA
email: saedma@udmercy.edu

Kevin Daimi and Nizar Al Holou
College of Engineering and Science
University of Detroit Mercy
Detroit, USA
email: {daimikj, alholoun}@udmercy.edu

***Abstract*— Smart grid will soon be a reality. As a result of connecting the traditional power grid to networks, all the vulnerabilities related to information technology will be inherited by the smart grid. Hence, the smart grid must be protected against various cyber-attacks. An essential component of the smart grid is the Advanced Metering Infrastructure (AMI). In an attempt to protect smart meters' communication with the collector, two security schemes based on PKI are introduced in this paper. The security requirements of confidentiality, integrity, and nonrepudiation are analyzed with respect to these schemes.**

***Keywords*— AM; Direct Connection; Smart grid; Security**

I. INTRODUCTION

Smart grids utilize bidirectional communication with consumers to facilitate an information-driven style to indirect energy control and management. To this extent, they deploy large scale smart meters at consumer's sites for bidirectional real time communication using existing network protocols [17]. The smart grid characterizes the new trends of the current power grid nationally and internationally. It emerged in response to environmental changes, improved energy efficiency, and reduced pollution emissions [15]. The smart grid, which is supported by information technology and intelligent control, relies on six components, namely; power generation, transmission, transformation, distribution, consumption and dispatching [11]. Smart grid refers to the next generation power grid, which upgrades the electricity distribution and management by encompassing a scalable and ubiquitous two-way communication infrastructure to enhance control, efficiency, reliability and safety [19] [24]. It is, therefore, no surprise that many countries are considering it as the future direction of the classical power grid [10] [16] [18].

Incorporating the Internet in the smart grid will widely open the door for various security attacks traditionally associated with the Internet. Undoubtedly, Smart Grid systems will significantly improve efficiency and reliability but at the expense of possibly introducing new vulnerabilities. Hence, smart grid utilization should meet rigorous security requirements [14]. Cyber-security, as a vital challenge of the smart grid transformation, must be enforced right at the beginning and not glued when attacks take place [1]. To reach full customer trust and to ensure excellent permanence of the current power supply, all components of smart grid communication network need to be extremely secure to satisfy confidentiality requirements [22]. Vulnerabilities are expected in power transmission networks, power grid, SCADA system access points and zone management [4] [6] [8]. To eliminate vulnerabilities or at least minimize their impact, strong security measures must be put in place.

Within the smart grid, the AMI plays a major role. It uses bi-directional communications between consumers and the utility, and requires robust communication network to take into account a large number of devices, small data burst transmission, high-level of reliability, and changing propagation conditions [13] [20]. Formerly, Automatic Meter Reading (AMR) was used for automatically collecting energy consumption and status data from metering devices and then transferring that data to a central database system for billing and further analysis. To allow for additional data to be read, stored, and transmitted to servers, and to control the metering devices remotely, The AMI proved to be the solution [12]. Advanced Metering Infrastructure includes the components responsible for measuring, collecting and analyzing energy usage. It consists of the Meter Data Management (MDM) system, communication network, access points, and the end points. The end points connect to smart meters, and other display and control end devices [3] [9] [23]. AMI is the only part of the smart grid in which all line segments and substations are visible [5].

Based on the importance of AMI and the vital role that it plays within the smart grid, it is very demanding that the AMI must be protected from various possible cyber-security attacks. The following security requirements must be enforced: confidentiality, integrity, availability, and nonrepudiation [7]. Consumers do not want others to know how much energy they are consuming or how it is being used (confidentiality). Meter readings and control commands should not be modified while they are being transferred (integrity). The availability of meter reading is critical for utilities and consumers. It is also critical that sending and receiving components and devices cannot deny sending information including readings and commands (nonrepudiation). There are a number of possible attacks on AMI components including denial of service, device

ISBN: 978-1-61208-422-0

tampering, snooping, impersonation, wormhole, black hole and routing attacks. Therefore, AMI demands a reliable and secure communication approach between the smart meters and consumer equipment [2].

Vaidya et al [21] stressed that many of the available schemes for both single-path and multipath routing are not suitable for meshed AMI network. Consequently, they introduced a security mechanism for multipath routing based on Elliptic Curve Cryptology (ECC), digital signature, and Message Authentication Code (MAC) for such an AMI network. Their approach allows the Certificate Authority to do a lot more work than they should normally do (issuing certificates) including controlling the nodes' creation of public and private key. Nodes (smart meters) are doing a number of computations despite their known limited computing power. This also tends to slow the system. Furthermore, a smart meter sends it information to all the neighboring smart meters. This provides attacker the opportunity for attacking more than one goal (smart meter) as they all have the information of the source meter. The neighboring nodes, acting as as intermediate nodes, will do even more calculations and broadcast the results. This means all other nodes (smart meters) have now the information. Again, there are many nodes that the attacker can try and many nodes will be affected. An interesting security protocol for AMI communications in smart grid where the smart meters are interconnected through wireless network was introduced by Yan et al [25]. The paper indicated that the Public Key Infrastructure (PKI) is not desirable and relied on symmetric key cryptology. However, the number of symmetric keys used is large (2n, where n is the number of nodes) and comparable to the number of keys should the PKI has been followed. Symmetric keys are normally used for large messages. Furthermore, smart meters have limited capabilities, and therefore, verifying the MAC by the successor node is time consuming and should have been left to the collector. The paper did not specify what will happen when the two MAC's are not equal. This implies that the integrity of a meter's reading is not handled correctly.

This paper proposes two schemes for securing the indirect meter-to-collector communications. Both schemes are based on PKI. Unlike the work of Vaidya et al [21], this paper allows each node to send the encrypted, authenticated, and signed reading of a smart meter to its successor only (just one node). The successor cannot tell the reading of the predecessor node. If a node is attacked, readings of other nodes will not be affected. The paper also avoids the need for a certificate authority by allowing the collector node to take care of issuing certificates to all smart meters under its authority. Furthermore, nodes do not waste time performing lengthy calculations. In contrast to the approach of Yan et al [25], PKI provides stronger encryption using public and private keys. It is clear how the keys are created/recreated and exchanged. The messages (readings) are small indicating PKI is the convenient way here. The verification of the hash functions is carried out by the collector, which has more powerful computing capabilities. If the computed hash function is not equal to the received hash function for a smart meter's reading, the collector will reject that reading and inform the substation of a possible attack on that smart meter. Therefore, the integrity of a message (reading) is handled correctly. Furthermore, this paper adds anonymity to the meters by using anonymous IDs, and adds confusion to the order of readings of smart meters using a PRNG.

The AMI architecture used for this scheme will be introduced, and the security of the schemes will be analyzed. The reminder of the paper is organized as follows: Section II introduces the AMI architecture. Section III deals with the process of secure reading collection. The analysis of AMI communication security is presented in Section IV. Finally, the paper is concluded in Section V.

II. AMI ARCHITECTURE

AMI networks are responsible for connecting a substantial number of devices needed to collect readings from smart meters. As this paper is concerned with securing smart meters to collector communication, only this part of the AMI architecture will be introduced.

There are two ways of connecting smart meters to connecters; direct and indirect connections. In direct connection, smart meters directly communicate with collectors to transfer readings and exchange information and commands. For indirect (or indirect) connection, one or more smart meters are directly connected to the collector. The rest are either connected to the nearest smart meters that have direct connection with the collector or through a series of smart meters until the one directly connected to the collector is reached. The collector is responsible for collecting readings from all smart meters within its coverage area (network). Coverage area could include both direct and indirect connection.

An example of an indirect connection is presented in Figure 1 to clarify the connection." In this figure, smart meters SM_0 and SM_6 are directly connected to the collector C. Other smart meters are either directly connected to SM_0 and SM_6 (SM_1 and SM_7), or through other smart meters (for example SM_3, SM_4, SM_5, SM_8, SM_9). Collectors are connected a substation. The substation is extremely important to the efficient functioning of an electric utility since it contains a large quantity of significant information needed for the successful operation and management of the smart grid. Securing the direct smart meter-to-collector connection is easier than the indirect connection because it only needs one level of security connection with collector only. For indirect smart meter-to-collector connection, two levels of security are needed. First, the inter-meter connections must be secured, and then the direct connection with the collector. The collector will collect all the readings. If there is a problem with a reading or a missing reading due to an attack or any physical reason, the collector will report that to the substation, which will inform the management of the utility company.

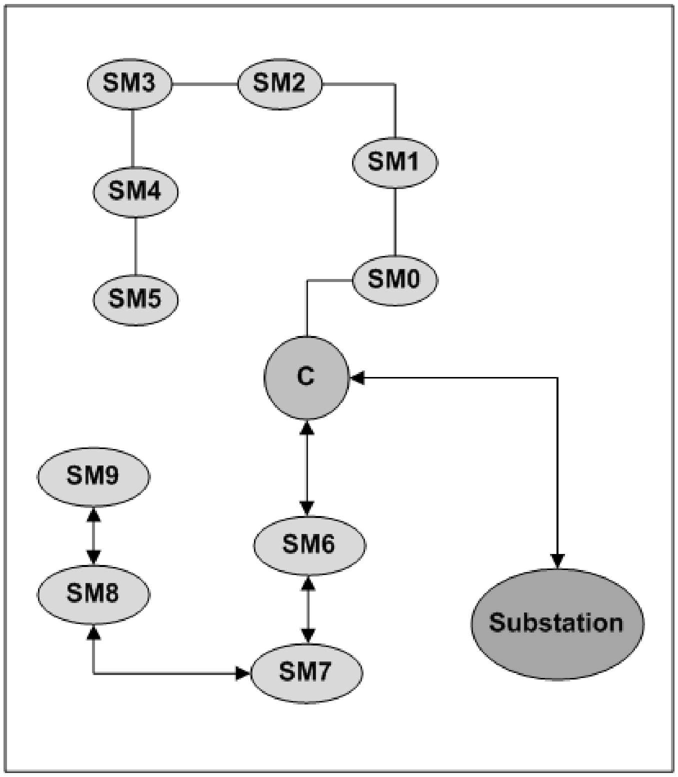

Figure 1. Smart meter-collector indirect connection

III. SECURE READING COLLECTION PROCESS

Two approaches for the indirect communication between smart meters and collector will be introduced below. In both approaches, anonymous ID's (A-ID's) for the smart meters are used. To create anonymous ID's, each smart meter XORs the current ID (real one initially and then anonymous) with the output of a true random number (TRN) generated by a ring oscillator, T_i [26]. Any other true random value can be used instead of or in addition to the one generated by the ring oscillator. In other words, $A\text{-}ID_i = ID_i$ XOR T_i for the first $A\text{-}ID_i$, and $A\text{-}ID_i$ = Previous $A\text{-}ID_i$ XOR T_i for subsequent $A\text{-}ID_i$'s. Table I presents the notations used in these approaches.

In the first approach, the collector C should have initially received all the public keys and IDs of the smart meters. On the other hand, the smart meters, SM's, should have the public key of the collector using any secure process. Furthermore, the predecessor and successor nodes for each smart meter are identified during installation and configuration of each smart meter. The node directly connected to the collector has no successor. The nodes at the end of the connection have no predecessors. Note that the scheme will be applied to the upper part of Figure 1 to observe how smart meters SM_0-SM_5 securely send their readings to the collector C. The readings for smart meters SM_6-SM_9 at the lower part of the figure will be collected using the same approach.

Each smart meter, SM_i, replaces its real ID_i with an anonymous one, $A\text{-}ID_i$, appends ID_i to it and encrypts both with the public key of collector, PU_c, before sending the resulting message, $E(PUc,\ A\text{-}ID_i \parallel ID_i)$, to C through the indirect connection (Figure 2). The collector, C, creates certificates for each smart meter, SM_i. It appends $A\text{-}ID_i$ to the public key of each smart meter, PU_i, and the period of validity PRV, and then encrypts $PU_i \| A\text{-}ID_i \| PRV$ with its private key, PR_c to get the certificate for each smart meter ($CR_i = E(PR_c, PU_i \| A\text{-}ID_i \| PRV)$ since all smart meters have the public key PU_c of the collector. The CR_i is further encrypted with PU_i. Having done that, C then attaches $A\text{-}ID_i$ to the resulting message and forwards $E(PU_i, CR_i) \parallel A\text{-}ID_i$ to smart meters via SM_0. Certificate creation is depicted in Figure 3 for both the collector and smart meter.

Every SM_i checks the $A\text{-}ID_i$. If it is its ID, it decrypts $E(PU_i, CR_i)$ with its private key PR_i to get its certificate. Otherwise, it will forward the message to adjacent smart meters to do the same until all smart meters receive their certificates.

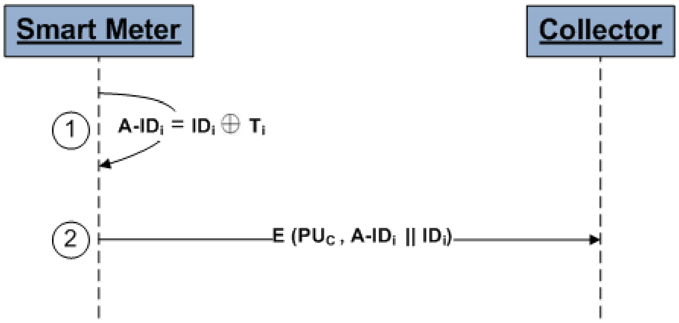
Smart Meter
Collector
1
$A\text{-}ID_i = ID_i \oplus T_i$
2
$E\ (PU_C\ ,\ A\text{-}ID_i\ \|\ ID_i)$

Figure 2. Creating and sending anonymous ID

Each SM_i XORs its reading, R_i, with the TRN produced by the ring oscillator, T_i, concatenates the resulting message with T_i and the hash function of the reading $H(R_i)$. The resulting message will be encrypted with PR_i to get $X_i = E\ [PR_i,\ M_i \parallel H(R_i) \parallel T_i]$, where $M_i = R_i$ XOR T_i. To enable the collector to recognize the source meter's reading, $A\text{-}ID_i$ is attached to X_i and both encrypted with PU_c to get $Y_i = E(PU_c,\ X_i \parallel A\text{-}ID_i)$. The XOR operation is used to obscure the reading of the meter. T_i is needed to allow the receiver to XOR it with M_i to get R_i. Having done that, R_i will be hashed and compared to $H(R_i)$.

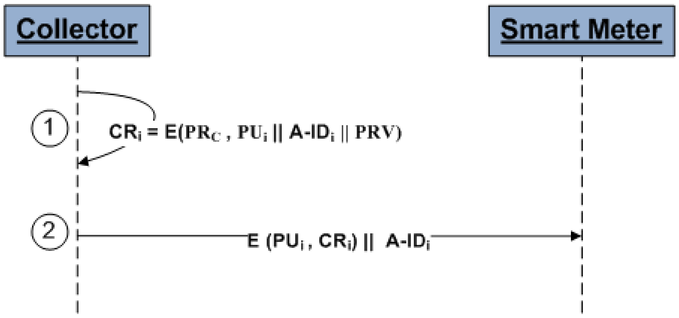
Collector
Smart Meter
1
$CR_i = E(PR_C\ ,\ PU_i \parallel A\text{-}ID_i \parallel PRV)$
2
$E\ (PU_i\ ,\ CR_i) \parallel\ A\text{-}ID_i$

Figure 3. Creating and sending certificates

The predecessor and successor nodes exchange certificates to authenticate each other. On successful authentication, the predecessor smart meter encrypts its Y_i with the public key PU_{i-1} of the successor, and forward $E[PU_{i-1},\ Yi]$ to the successor. The receiving successor decrypts the received message with its private key PR_{i-1}, prepends or appends its own Y_{i-1} and encrypts the two ($Y_i \parallel Y_{i-1}$, or $Y_{i-1} \parallel Y_i$, for example) with its successor's public key. This process will continue until all Y_is have been concatenated at SM_0. Using Figure 1 above, we should have Y = $Y_5 \| Y_4 \| Y_3 \| Y_2 \| Y_1 \| Y_0$ or any other ordering. SM_0 sends Y to C. Any missing Yi indicates a problem, possibly an attack, within that meter. If this occurs, the collector will reject the received message and report to the substation to investigate the issue.

The decision on whether to append or prepend Y_i is based on pseudorandom number generator (PRNG), which generates pseudorandom bit stream. Y_{i-1} is prepended if the pseudorandom bit is '0' and appended if the bit is '1'. This will obscure the order of Yi's and make it hard to relate the Yi's to their smart meters. To illustrate this, Figure 4 is provided.

The collector, C, uses its PR_c to decrypt Y. Then, based on the A-ID_i, it uses the appropriate PU_i to decrypt each Y_i to obtain $M_i \| H(R_i) \| T_i$ for each smart meter. It XORs M_i with T_i to get the reading R_i. It later finds the hash function of R_i and ensures it is equal to the received hash function $H(R_i)$ to guarantee the integrity of the reading, R_i. Figure 5 illustrates the meter readings collection process. To simplify Figure 5, Z = $Y_5 \| Y_4 \| Y_3 \| Y_2 \| Y_1$ (order is based on PRNG') is used.

Note that smart meter 5, SM_5, has no predecessor, and therefore, no PRNG' unit exists. Only smart meters SM_4-SM_1 have it because they have predecessors (smart meters connected to them, as depicted in Figure 1). Once the order of Y_i's is decided, the result is encrypted with the public key of the next meter, PU_{i-2}, and forwarded to the next smart meter, SM_{i-2}. The PRNG for SM_0 is not followed by encryption as in Figure 4 because it is forwarding directly to the collector.

TABLE I. NOTATIONS USED

Symbol	Meaning
C	Collector
SM_i	Smart meter i
SM_0, SM_6	Smart meters directly connected to C
PU_C , PR_C	Public & private keys of collector
PU_i , PR_i	Public & private keys of smart meter i
||	Concatenation
E	Encrypt
→	Send to
R_i	Reading of smart meter i
$H(R_i)$	Hash function of reading R_i
T_i	TRN from Ring Oscillator for smart meter i
PRV	Period of validity
ID	Identification
ID_C	ID of collector
ID_i	ID of smart meter i
A-ID_i	Anonymous ID for smart meter i
CR_i	Certificate of smart meter i

After a predefined number of readings or when the validity period PRV of the certificate expires, new keys for both collector and SM's will be generated and exchanged. The collector will use its old PR_c to encrypt the new PU_c and then encrypt the result with the old PU_i and attaches A-ID_i prior to sending it to SM_i. The A-ID_i will allow each smart meter to tell if the message is intended for it. The smart meter in question, SM_i, will decrypt this message to get the new public key of the collector. At the other side, each smart meter generates new A-ID_i, PU_i and PR_i, appends the new A-IDi to the new PU_i, encrypts the resulting message with the old PRi and then with the new public key of the collector, PU_c. Finally, the old A-IDi is attached before sending it to the collector. The collector will apply the required series of decryptions to get the new A-ID_i and PU_i of each smart meter. Note that the old A-ID_i is added to allow the collector to recognize each smart meter. Furthermore, new certificates will be generated and forwarded to the smart meters as mentioned above. This is detailed in Figure 6 below. New keys, certificates, and anonymous IDs are also created and exchanged when an attack is anticipated or has already occurred.

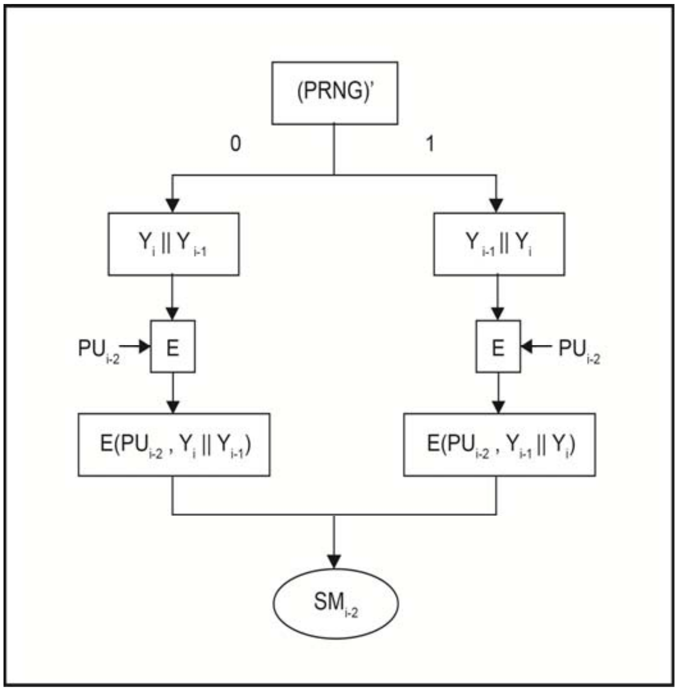

Figure 4. PRNG operation

An alternative approach is used if the creation and storage of certificates are not desirable due to computing power and memory limitations. For each adjacent smart meter pair, the collector sends the predecessor the public key of the successor encrypted with the public key of the predecessor, and sends the successor the public key of the predecessor encrypted with the public key of the successor. In both cases, the A-ID_i is attached to allow smart meters to capture messages belonging to them. Apart from replacing the certificate with the collector providing the public keys for the predecessors and successors, the rest is exactly as in the first approach.

IV. AMI COMMUNICATION SECURITY ANALYSIS

The security of the above schemes is analyzed with respect to confidentiality, integrity, and non-repudiation. Although hash functions can help with intrusion and virus detection, availability cannot be satisfied by cryptology alone (schemes above), and therefore, it will not be part of the analysis.

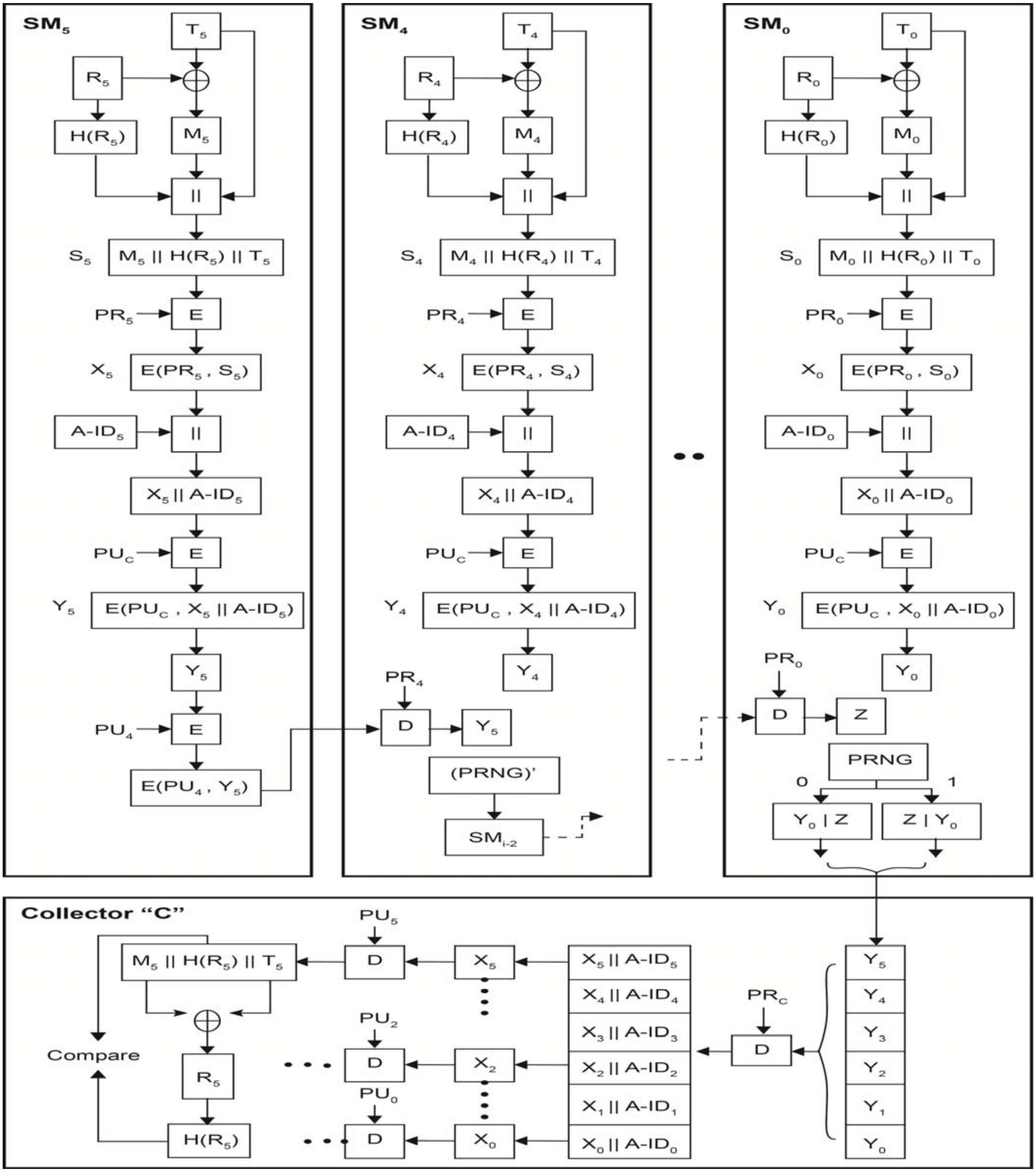

Figure 5. Meter readings collection process

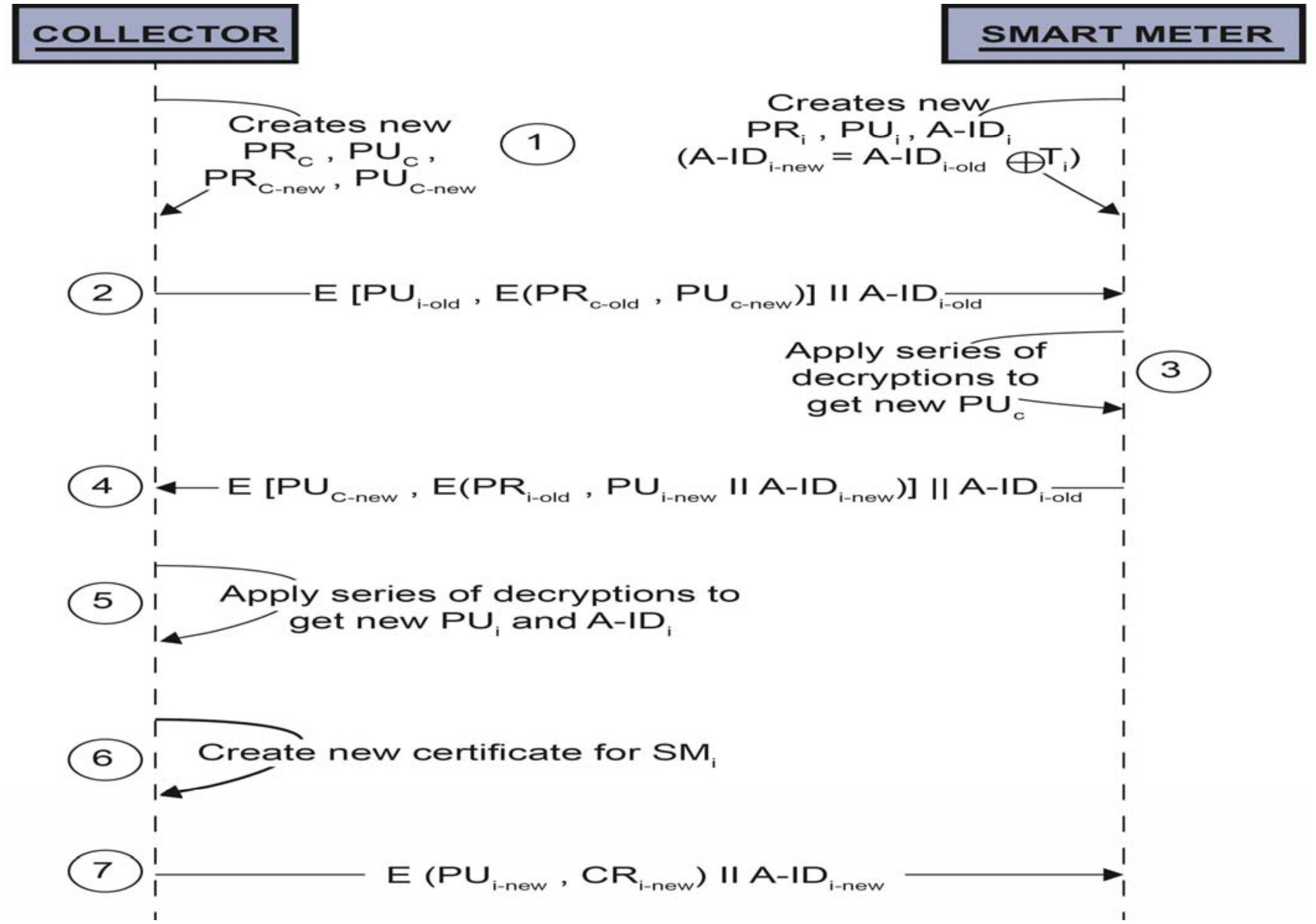
COLLECTOR
SMART METER
Creates new PR_C , PU_C , $PR_{C\text{-new}}$, $PU_{C\text{-new}}$
1
Creates new PR_i , PU_i , A-ID_i
(A-$ID_{i\text{-new}}$ = A-$ID_{i\text{-old}}$ $\oplus T_i$)
2
E [$PU_{i\text{-old}}$, E($PR_{c\text{-old}}$, $PU_{c\text{-new}}$)] II A-$ID_{i\text{-old}}$
Apply series of decryptions to get new PU_c
3
4
E [$PU_{C\text{-new}}$, E($PR_{i\text{-old}}$, $PU_{i\text{-new}}$ II A-$ID_{i\text{-new}}$)] || A-$ID_{i\text{-old}}$
5
Apply series of decryptions to get new PU_i and A-ID_i
6
Create new certificate for SM_i
7
E ($PU_{i\text{-new}}$, $CR_{i\text{-new}}$) II A-$ID_{i\text{-new}}$

Figure 6. Exchanging new keys, IDs, and certificates

A. Confidentiality

Confidentiality ensures that the message sent can only be disclosed to the authorized parties. This implies that authorization restrictions are in place to ensure personal and information confidentiality.

Consumers definitely do not like others to intrude on their confidentiality in terms of energy quantity used or how it was used. They need assurance that no unauthorized disclosure of the transferred information will take place.

The proposed protocols ensure that confidentiality is met through four levels. First and most important, the message that is forwarded to the next smart meter or directly to the collector in the case of SM_0 is encrypted with the public key of the collector ($Y_i = E(PU_c, X_i \| A\text{-}ID_i)$). Only the party that has the private key (collector), PR_C, can decrypt this message. In fact, because the contents of X_i are encrypted with PR_i, and then X_i is encrypted with PU_c, authentication and digital signature are also taken care of.

In addition, the replacement of real IDs with anonymous ones will make it hard to relate a reading to a particular smart meter. Furthermore, the use of pseudorandom number generator (PRNG) introduced further hardship in judging the link between the reading and smart meter. Finally, readings are XORed with a random value that modifies the actual reading. This will make it very hard for attackers to extract the actual reading.

B. Integrity

Customers and utilities need an assurance that the data received is exactly as sent. This assurance guarantees that the data received has not been subject to any modification, insertion, deletions, or replay on its way to its destination. This is referred to as data integrity.

Message authentication is a technique used to ensure the integrity of the message. With regards to smart meter-to-collector communication, meter readings messages and commands should arrive exactly as they left the source that issued them.

The reading, R_i, in the proposed schemes has its integrity fulfilled through the use of cryptographic hash function, $H(R_i)$. Upon receiving the message, the collector extracts R_i and find its $H(R_i)$. It then compares the computed $H(R_i)$ with the received one. Any mismatch indicates the message has been modified. Further guard to ensure the integrity of the message was carried out by using digital signature. The hash value, $H(R_i)$, is encrypted with the private key of each smart meter ($X_i = E\ [PR_i, M_i \| H(R_i) \| T_i]$). Only the receiver with the public key of the smart meter, which is the collector, can decrypt the hash value.

C. Nonrepudiation

Non-repudiation guarantees that the sender cannot deny it sends the information, and the receiver cannot deny it receives it. No smart meter can deny its reading because the reading and its hash value are encrypted with the private key of smart meter (X_i = E [PR_i, M_i || $H(R_i)$ || T_i]). Provided the key was not compromised, no party but the smart meter knows its own private key.

In a similar analysis, the collector cannot deny it sent each smart meter its certificate [(CR_i = E(PR_c, PU_i||A-ID_i||PRV)] because it is encrypted with its private key and no other party knows its private key. Furthermore, the use of hash functions, $H(R_i)$, is used for nonrepudiation of the origin (dispute resolution).

V. CONCLUSION

Smart meter-to-collector communication plays a critical role within the Advanced Metering Infrastructure. Protecting them against possible cyber-attacks is a vital requirement. To contribute to this effort, two cryptographic protocols based on PKI were introduced. One of these protocols involved using certificates issued by the collector. Only the indirect communication of smart meters with the collector was investigated. Securing such a connection is harder than the direct one because readings have to travel through other smart meters before reaching the collector. The introduced schemes satisfied the security requirements; confidentiality, integrity, and nonrepudiation.

REFERENCES

[1] S. M. Amin, "Smart Grid Security, Confidentiality, and Resilient Architectures: Opportunities and Challenges," IEEE Power and Energy Society General Meeting, San Diego, CA, 2012, pp. 1-2.

[2] V. Aravinthan, V. Namboodiri, S. Sunku, and W. Jewell, "Wireless AMI Application and Security for Controlled Home Area Networks," IEEE Power and Energy General Meeting, San Diego, CA, 2011, pp. 1-8.

[3] M. Chebbo, "EU Smart Grids Framework: Electricity Networks of Future 2020 and Beyond", IEEE Power Engineering Society General Meeting, Tampa, FL, 2007, pp. 1-8.

[4] G. Chen, Z. Y. Dong, J. H. David, G. H. Zhang, and K. Q. Hua, "Attack Structural Vulnerability of Power Grids: A Hybrid Approach Based on Complex Networks," Physica A: Statistical Mechanics and its Applications, vol. 389, 2010, pp. 595-603.

[5] S. Choi, S. Kang, N. Jung, and I. Yang, "The Design of Outage Management System Utilizing Meter Information Based on AMI (Advanced Metering Infrastructure) System," in Proc. the 8th International Conference on Power Electronics, Shilla Jeju, Korea, 2011, pp. 2955-2961.

[6] S. Clements and H. Kirkham, "Cyber-security Considerations for the Smart Grid," IEEE Power and Energy Society General Meeting, Minneapolis, MN, 2010, pp. 1-5.

[7] F. M. Cleveland, "Cyber Security Issues for Advanced Metering Infrastructure (AMI)," IEEE Power and Energy General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century, Pittsburgh, PA, 2008, pp. 1-5.

[8] G. N. Ericsson, "Cyber-security and Power System Communication: Essential Parts of a Smart Grid Infrastructure," IEEE Transactions on Power Delivery, vol. 25, no. 3, 2010, pp. 1501-1507.

[9] D. G. Hart, "Using AMI to Realize the Smart Grid," IEEE Power Engineering Society General Meeting, Pittsburgh, PA, 2008, pp. 1-2.

[10] A. Ipakchi and F. Albuyeh, "Grid of the Future," IEEE Power and Energy Magazine, vol. 7, no. 2, 2009, pp. 52-62.

[11] X. Jin, Y. Zhang, and X. Wang, "Strategy and Coordinated Development of Strong and Smart Grid, in Proc. the 2012 IEEE Conference on Innovative Smart Grid Technologies – Asia (ISGT Asia), Tianjin, China, 2012, pp. 1-4.

[12] I. Joe, J. Y. Jeong, and F. Zhang, "Design and Implementation of AMI System using Binary CDMA for Smart Grid," in Proc. the Third International Conference on Intelligent System Design and Engineering Applications, Hong Kong, 2013, pp. 544-549.

[13] J. H. Khan and J. Y. Khan, "A Heterogeneous WiMAX-WLAN Network for AMI Communications in the Smart grid," in Proc. the IEEE third International Conference on Smart Grid Communication (SmartGridComm), Tainan, Taiwan, 2012, pp. 710-715.

[14] A. R. Metke and R. L. Ekl, "Smart Grid Security Technology," in Proc. IEEE Conference on Innovative Smart Grid Technologies (ISGT), Gaithersburg, MD, 2010, pp. 1-7.

[15] X. Miao, X. Chen, X. Ma, G. Liu, H. Feng, and X. Song, "Comparing Smart Grid Technology Standards Roadmap of the IEC, NIST, and SGCC," in Proc. 2012 China International Conference on Electricity Distribution (CICED 2012), Shanghai, China, 2012, pp. 5-6.

[16] R. O'neill, "Smart grid sound transmission investments," IEEE Power and Energy Magazine, vol. 5, no. 5, 2007, pp. 104-102.

[17] Y. Simmhan, A. G. Kumbhare, B. Cao, and V. Prasanna, "An Analysis of Security and Confidentiality Issues in Smart Grid Software Architectures on Clouds," in Proc. IEEE 4th International Conference on Cloud Computing (CLOUD 2011), Washington, DC, USA, 2011, pp. 582-589.

[18] H. Tai and E. Hogain, "Behind the Buzz: Eight Smart-Grid Trends Shaping the Industry," IEEE Power and Energy, vol. 7, no. 2, 2009, pp. 96-97.

[19] U.S. Department of Energy (DOE), Available: www.smartgrid.gov/the_smart_grid, [retrieved: April, 2015].

[20] U.S. Department of Energy (DOE), "The Smart Grid: an Introduction," Available: http://energy.gov/oe, [retrieved: April, 2015].

[21] B. Vaidya, D. Makrakis, and H. Mouftah, "Secure Multipath Routing for AMI Network in Smart Grid," in Proc. IEEE 31st International Conference on Performance Computing and Communications (IPCCC), Austin, TX, 2012, pp. 408-415.

[22] M. Wagner, M. Kuba, and A. Oeder, "Smart Grid Cyber Security: A German Perspective," in Proc. International Conference on Smart Grid Technology, Economics and Policies (SG-TEP), Nuremberg, 2012, pp. 1-4.

[23] J. Wang and V. C. M. Leung, "A Survey of Technical Requirements and Consumer Application Standards for IP-based Smart Grid AMI Network," in Proc. the International Conference on Information Networking (ICOIN), Barcelona, 2011, pp. 114-119.

[24] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements, and Challenges," IEEE Communications Surveys and Tutorials, vol. 15, no. 1, 2013, pp. 5-20.

[25] Y. Yan, Y. Qian, and H. Sharif, "A Secure and Reliable In-network Collaborative Communication Scheme for Advanced Metering Infrastructure in Smart Grid," in Proc. IEEE Wireless Communications and Networking Conference (WCNC), Cancun, Quintana Roo, 2011, pp. 909-914.

[26] P. Schaumont, "True Random Number Generation," Circuit Cellar, no. 268, 2012, pp. 52-58.