ISSN 2277-3601

A Secure key Distribution and Management Scheme for Home Area Network in Smart Grid

[1]Halim Halimi, [2]Aristotel Tentov
[1] Department of IT, State University of Tetovo, Tetovo, Macedonia
hhalimi2000@yahoo.com
[2] Department of CST, Faculty of Elec. Engin. and Inform.Techn., Skopje, Macedonia
toto@feit.ukim.edu.mk

ABSTRACT

Securing the network communication for the smart grid requires a secure key distribution and management scheme. Advanced metering Infrastructure (AMI) is considered as an integral part of the smart grid that collects and analyzes the information of energy consumption using the communication network. In order to achieve data confidentiality, privacy, and authentication in AMI, various crypto algorithms are used, such as demand key distribution and management schemes. Investigation on properly designed key distribution and management scheme for securely gathering both individual and aggregated meter's readings is one of the critical requirements. In this paper, we propose a secure key distribution for Home Area Network (HAN) in smart grid as well as a new key distribution and management scheme, which uses identification scheme of Wu – Hsu and tailored to smart grid. We also give the scheme for key update/freshness and key revocation. Specifically, a group ID based mechanism is proposed to establish the keys for a large amount of users with small overload.

Indexing terms/Keywords

Gateway; Home Area Network (HAN); Smart meter.

Academic Discipline And Sub-Disciplines

Computer Science and Engineering;

SUBJECT CLASSIFICATION

Cryptography; Smart grid security

TYPE (METHOD/APPROACH)

Theoretically research method

Council for Innovative Research

Peer Review Research Publishing System

Journal: INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY

Vol 12, No. 8

editor@cirworld.com

www.cirworld.com, www.ijctonline.com

INTRODUCTION

The current power grid is ageing and cannot respond to the electricity quality requirements for the next century. Computation and communication capabilities are being incorporated in the power grid to promote it to smart grid.

The smart grid, designed to replace traditional electric power infrastructure, is able to provide efficiency, security and reliability through a two-way flow of electricity and communication.

Smart grid is the key technology that includes the current power grid with the necessary tools using advanced telecommunications and information technologies [1]. It includes a two-way digital communication infrastructure for real time information exchange [2] within the grid.

In order to deploy the two-way communication, one possible solution is to use advanced metering infrastructure (AMI).

Advanced metering infrastructure (AMI) is one of the major advancements for collecting and analyzing the measurements of energy consumption using the communication network. An AMI includes software, hardware, communication networks, smart meters and customer-associated systems. As part of the AMI, the smart meters (SMs) have a processing chip and a nonvolatile storage so they can perform smart functions like periodic reporting of energy usage updates to end users as well as the generation facilities at power companies and communicate with smart appliances at home to control them. With the recent development of AMI, the cyber security issues in AMI are becoming very important, as AMI is part of the critical infrastructure of the smart grid. In order to achieve data confidentiality, privacy and authentication in AMI, new key distribution and management scheme is needed, which uses various security crypto algorithms. In several works for authentication in AMI [2] [3] [4] the key distribution and management are not studied. In work [3], a device authentication mechanism and key establishment scheme for smart grid Home Area Network with few security properties is proposed. In work [5] a framework for key distribution and management in smart grid is given. The author in work [6] proposes a lightweight key and management scheme for home area network (HAN), which is one of the key components in the communication infrastructure of the AMI. The challenge demand of new key distribution and management schemes is securing AMI from cyber attacks. In this work, we propose a key distribution and management scheme in HAN, which uses identification scheme of Wu – Hsu [7] and tailored to smart grid. Specifically, a secure pair – wise key agreement scheme is designed to provide the authenticity of the smart appliances in a wireless star network of appliances in a HAN. The scheme for key update, key revocation and security analysis are also discussed.

The rest of this paper is organized as follows: the system model and problem formulations are given in section II. Section III provides an efficient key distribution scheme to secure high rate real time data aggregation to the utility. Security analysis is given in section IV. Finally, we conclude this article in section V.

SYSTEM MODEL

Smart grid as a complex system uses multiple communication technologies and standards in different points along the generation, transmission, distribution infrastructure to the consumers where the electricity is consumed. This communication infrastructure is ranging from Home Area Network (HAN), Building Area Network (BAN), Neighborhood Area Network (NAN) and the Internet. A HAN is in the lowest end of the hierarchical level, i.e. at the consumer-end.

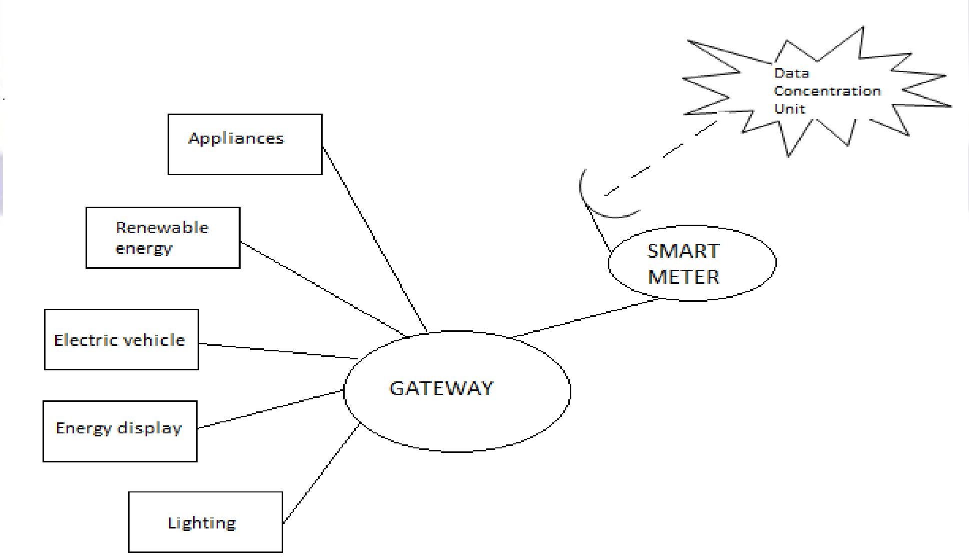

Figure 1. Illustration of HAN modeling

The HAN enables consumers to efficiently manage their on-demand power requirement and presents the basis of a communication infrastructure for energy management in smart grid. HAN connects the smart meter, several smart electrical appliances and alternative private energy sources or electric vehicles. Figure 1 illustrates an overview of a HAN.

A smart meter should collect real-time power consumption of each device in HAN using short-range wireless communication standards like Zigbee (802.15.4) and Wi-Fi (802.11).

Although wireless systems provide relatively cheaper and flexible solution for smart grid communication, they are also more vulnerable to cyber attacks compared with wired systems.

The main focus of this study is the key distribution and management in a HAN. We consider HAN as a two-way communication infrastructure between end-users and utility provider with multiple appliance accesses to a centralized gateway (G) through the smart meter. The sensitive information exchange within the HAN is needed to introduce a strong security, privacy and integrity mechanism, which can guarantee the trustworthiness of the data.

In the model, the smart appliances are considered as end nodes. A HAN presents a group of end nodes linked in a star topology to a gateway node, which is connected to the smart meter. Each equipment (appliances) and the smart meter are considered to be one hop to the gateway. An attacker located in the wireless range of the G can eavesdrop the wireless communication within the HAN. The attacker may launch various attacks on the HAN, including intercepting the message between devices, compromising, impersonation attacks, conspiracy, maliciously modifying the information, and forgery attack. In order to achieve data security, privacy, integrity and authentication in HAN various crypto algorithms are used, such as demand key distribution and management schemes. This work provides secure key distribution and management scheme in HAN using identification scheme of Wu-Hsu [7], which guarantees the communication security between the group of devices in the HAN as well as the HAN interface of the smart meter and the gateway.

PROPOSED KEY DISTRIBUTION AND MANAGEMENT SCHEME FOR HOME AREA NETWORK IN SMART GRID

In this section, we first present the essential security principles needed in the networking communications system.

The new scheme is inspired by an efficient user identification scheme with new distribution preserving anonymity for distributed computer networks of Tzong-Su Wu and Chien-Lung Hsu [7].

In addition to making the scheme fit and efficient for the smart grid, we assume that it is secure against many active attacks.

System Components

According to the conceptual model introduced by NIST [8], we consider three types of defined components: smart meters (data collectors), Gateway controller (data aggregators) and smart appliances.

Smart Meter

A smart meter works as a collector collecting data and communicating with its gateway. It is responsible for collecting the data from all appliances in the household.

The communication in home area network (HAN) is done using IEEE 802.15.4 Zigbee radio communications, Wi-Fi based communications while within wide area network (WAN) it would use GPRS communication [8], [9].

The smart meter plays an important role and to make communication secure it contains a processor having the ability of operating cryptographic computations.

Gateway Controller

It is the data aggregator within the HAN and it is responsible to monitor the electric flows and send the real–time electric information to the smart appliances. Upon receiving the authentication request message from an end-device (appliances) and after verifying the certificate, it needs to authenticate the end-devices.

Smart Appliances

Smart appliances are defined as appliances, which monitor, control and protect their electrical energy usage in response to customer needs. In order to provide feedback and advice on their energy use, smart appliances can sense their energy consumption and enable substations to view the complete home energy usage.

Smart appliances are a small but important piece of the smart grid architecture. The group of smart appliances includes smart meters, distributed generation capabilities, renewable energy sources and hybrid electric vehicles.

Smart appliances have an important role in the smart grid by making residential appliances more efficient and shifting their usage from peak to off-peak periods, so the average electricity usage will be cut. Reducing the loads in peak periods, will improve the health and stability of the power grid.

The most required functions of smart appliances are:

- Open specification for exchange of energy consumption data, user messages, operational status, and demand response user control.
- Open communications platform or providing an adaptation for other kind to this level.

- Ability to report demand response status and at least two types of warning messages regarding reduced energy efficiency of the appliance.
- Ability to reduce load for a "delay period"
- Ability to delay the defrost function to "off-peak" hours

The Proposed Scheme for Device Identification

The proposed scheme can be divided into two phases: the key generation phase and anonymous identification of devices.

The devices can be identified by the G, a consideration that might be useful for some security purposes. After the key generation phase, each device will be authenticated to the G using the secret key. The G can identify the legal devices with an efficient protocol in the identification phase of the anonymous devices. After the identification phase, the G exchanges the session key with the devices.

Key Generation

For two large primes p and q we calculate N=p*q. For any element $g\epsilon\, Z_N^*$ and a hash function H, e and f are selected so that $e * f = 1\, mod\ \phi\ (N)$ where $\phi\ (N)$ is the Euler's totient function. The parameters N, e, g, and H function are public and f, p, q are kept secret, then with a secure channel each devices D_i and G receives a secret key

$$D_i = ID_i^f \bmod N \qquad (1)$$

Where ID_i^f is the identity of D_i or G.

Identification of Anonymous Devices

The device D_i transmits the request for service to the G. After receiving the request, G generates a random number R_G and calculates.

$$z = g^{R_G} SK_G\ mod\ N \qquad (2)$$

which is then sent to D_i . D_i generates a random number R_D and calculates

$$a = z^e / ID_G\ mod\ \ N \qquad (3)$$

$$x = SK_D H(a^{R_D} |\,| T) \bmod N \qquad (4)$$

$$y = g^{e*R_D \bmod N} \qquad (5)$$

where T is the timestamp, H is a hash function, SK_G is a secret key of a Gateway and SK_D is a secret key of a devices. D_i sends (x, y, T) to G.

After receiving, G checks T and verifies the equation

$$ID_{D,i}\ ?= (x / H(y^{R_G} |\,| T))^e (\bmod N) \qquad (6)$$

If equation (6) is satisfied for some $ID_{D,i}$ existing in the identity list, D_i is accepted as an authorized user (devices). The identification phase of the devices is presented in the figure 2. After the identification protocol, the devices and the gateway share one common session key:

$$K_{jG} = a^{x*R_D} = y^{x*R_G} = g^{e*x*R_D*R_G(mod\ N)},\quad j \in \{1,2,.....n\} \qquad (7)$$

where n is the number of smart appliances in the HAN.

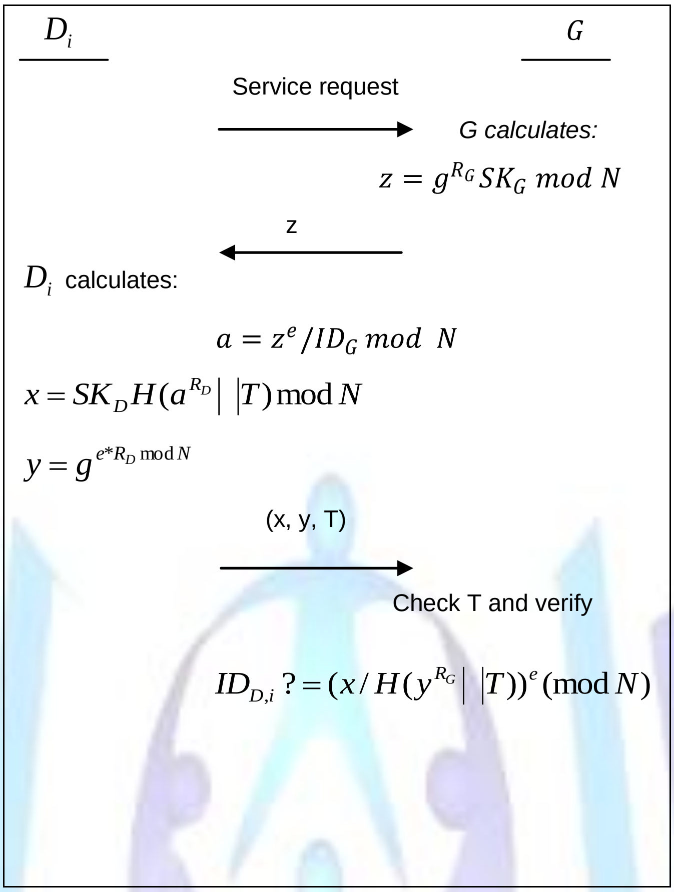
D_i
G
Service request
G calculates:
$z = g^{R_G} SK_G \; mod \; N$
z
D_i calculates:
$a = z^e / ID_G \; mod \; N$
$x = SK_D H(a^{R_D} \| T) \bmod N$
$y = g^{e * R_D} \bmod N$
(x, y, T)
Check T and verify
$ID_{D,i} \; ? = (x / H(y^{R_G} \| T))^e (\bmod N)$

Figure 2. Illustration of the identification phase of the devices

High Rate Secure Data Aggregation

For a device in direct communication with the G, we consider the HAN structure in Figure 1, where privacy is preserved when data is directly forwarded to the neighborhood area network (NAN) gateway through the secure network of G. The privacy security requirement for AMI, including energy usage pattern and power demand of a customer, should be kept secret to prevent access of unauthorized users. Homomorphic encryption techniques are to carry out different operations on cipher text and return results without knowing the plaintext messages. Several encryption techniques exist, which support different homomorphic techniques, such as multiplicative homomorphism RSA-[10], additive homomorphism-Paillier [11], Boneh – Goh- Wissim [12]. An additive homomorphic encryption scheme has been developed by M. Onen and R. Molva, which provides secure end-to-end confidentiality data aggregation and can very well adapt to the electricity usage privacy requirements. In order to implement a new scheme with key distribution and management for smart grid we use Wu – Hsu identification scheme.

Group Key Generation for Devices

We derive the shared group key from the pair-ways keys generated in the above scheme. Group key is generated from each and every legitimate smart device of the group. The unauthenticated group key agreement is based on the Diffie Hellman (DH) key agreement.

Suppose *n* denotes the total number of smart appliances (devices) in the HAN. Let G_K be the group key for all devices in the HAN. The G first generates a symmetric key with each and every device in the HAN as described in the previous section. Then the G will aggregate all the symmetric keys in one common group key as follows:

$$G_K = \prod_{j=1}^{n} K_{jG} = K_{1G} * K_{2G} \, . \, . \, . \, . \, . \, . K_{nG} =$$

$= g^{e*R_G}(R_{D,1} + R_{D,2} + \, . \, . \, . \, . \, . \; R_{D,n})$, where $R_{D,i}$ is the randomly generated number of the *i*th devices.

After this step, the G will use the individually shared secret key to encrypt the group key and create the messages $msg_i = E_{K_D^i}(G_K)$ to each corresponding D_i in the HAN.

Key Update/Freshness

One of the important key management requirements is that an attacker should not be able to decrypt the intercepted messages in the past if a node is attacked and its secret material compromised. Thus, it is not desirable to encrypt messages using the same distributed key in every session, i.e. the distributed keys need to be updated / refreshed periodically. Therefore, the G and all the devices respectively generate the messages encryption key, R_G and R_D in each session in the proposed mechanism. The G and the smart appliances exchange an encrypted message using the i th version of the key K_{jG}^{i}, $(j \in 1,2,....n)$. They replace the common session key K_{jG}^{i} by the $K_{jG}^{i+1} = H(K_{jG}^{i})$ and clear K_{jG}^{i} where H is a secure hash function. This dependence can be shown from the following equations: (2), (3), (4), (5), (7). As can be seen from the equation (7) for different randomly chosen numbers R_G and R_D the session key K_{jG}^{i} has different values. If either or both parties are compromised, the attacker can capture only the most recent version of the key and cannot calculate any previous versions of the key, due to the one-way property of H. Thus the pair-wise key can be updated very often with little computational overload due to the efficiency of the hash function.

When any pair-wise key is updated, the group key needs to be updated, which is computationally expensive. The G needs to update its group key when all pair-wise keys are updated .

SECURITY ANALYSIS

After the identification phase, every user (devices) D_i securely accesses a certification authority (CA) to be loaded with the following parameters: the ID of devices, the multiplicative group parameters (Z_N^*, p, q) and H (cryptographic hash function).

The security is discussed under the properties of the one-way hash function and the factorization rule.

One-way hash function has two properties: a) it is impossible to find a message m giving its hashed value $h(m)$ (one – way property) and,

b) it is impossible to find two different messages with the same hash value i.e. $h(m) = h(m^{'})$ [13], [14].

Factorization. Let $N = p * q$ and $\gcd\left(e, \emptyset(N)\right) = 1,$ where p and q are unknown large primes. For any $y \in Z_N^*$, it is computationally impossible to find x such that $y = x^e\,(mod\ N)$ with the knowledge of N and *e* [15].

Authentication

In the symmetric key scheme, the G and a D_i select two random numbers R_G and R_D in the multiplicative group and calculate z, x, y per Wu – Hsu scheme. A D_i that has not been loaded with the group parameters will not be able to generate an acceptable released session key causing factorization and discrete logarithm problem in the multiplicative group.

One-way authentication enables the G to verify the identity of D_i. Although two–way authentication provides a higher security where both parties can identify each other. One-way authentication owns the advantage of efficiency. If an attacker obtains the session key $K_{jG} = y^{kx}\,(mod\ N),$ he cannot derive the parameters z, a, x without knowing the secret key of G. If the D_i sends some encrypted sensitive information to the attacker then the attacker cannot recover the information without knowing the secret key $SK_G.$ From Figure 1, if the attacker intercepts D_i service request, then he cannot find *z* without knowing the secret key SK_G to reply to the D_i. Therefore, they cannot exchange the session key K_{jG} and the attack will not be successful.

Privacy

The G proceeds the same way with all the devices in the HAN and generates the group key as described earlier. Each D_i only knows its own pair wise symmetric key although they share the same group key. The group key will be used by every device to encrypt the messages within the HAN, ensuring the privacy of each D_i in the HAN.

Below, we show that Wu-Hsu scheme is secure for securing the appliances, against some considered possible attacks, such as compromising attacks, The equation (1) can be rewritten as $SK_G^e = ID_D\ (mod\ N).$ Based on the factorization rule it is impossible to calculate SK_G from eq. (1) with the known ID_{Di}. Also, from the same rule, without knowing the random numbers R_G and R_D it is impossible to find SK_G and SK_D from the expression of z and x by eq. (2) and eq. (3), respectively.

1) If the attacker obtains the released session key, he cannot identify the D_i by using the eq. (6). From the released session key, $K_{jG} = y^{kx}(mod\ N)$ the attacker should first derive the value of $y^k(mod\ N)$. The attacker cannot resolve y^k based on the factorization rule.

2) The calculated parameters (x, y, T) of the appliances are impossible to be falsified be the attacker. To falsify the parameters(x, y, T), the attacker has to first determine y and T, and then try to compute x by the expression:

   $x = SK_{Di}H(y^{R_G} || T) mod\ N$. This is impossible to calculate, since the secret SK_{Di} is unknown.

3) If the attacker can find some numbers $R_D^{'}$ and timestamp $T^{'}$ so that $H(a^{R_D} || T) = H\left(a^{'R_D{'}} || T^{'}\right)$, then he can construct other identification parameters $(x, y^{'}, T^{'})$ needed for verification of the eq. (6) and $y^{'} = g^{e*R_D^{'}} mod\ N$. But it is impossible to find two different values $(x, y^{'}, T^{'})$ with the same hash function.

4) The attacker cannot capture the session key, because the generation of the parameter z requires the secret key SK_G, which is protected under the FAC rule. Without the knowledge of SK_G, the attacker might attempt to find the numbers R_G and satisfy the equation $\frac{z^e}{ID_G} = g^{e*R_G}\ (mod\ N)$ and send z to the D_i. If the attacker can choose such R_G and z to satisfy the equation, then he can exchange a common session key $K_{jG} = a^{x*R_D} = y^{x*R_G}\ mod\ N$ with D_i. According the eq. (7), the attacker can use two ways to find R_G and z.

i. Randomly choose the number R_G and then try to find: $z = g^{R_G}(ID_G)^d\ mod\ N = (g^{e*R_G}\ ID_G)^d$ mod N, which is protected by FAC rule, and the attacker cannot resolve it.

ii. Randomly choose the number z and then try to find R_G. From the above equation, the attacker can find R_G if he can solve the discrete logarithm over modulo N [16], [17]. From the above discussion, the attacker cannot capture and exchange the session key K_{jG} with the D_i.

CONCLUSION

A new key distribution and management scheme is proposed for the Home Area Network (HAN), which is one of the key components in the communication infrastructure of the smart grid. This scheme includes various topologies of the communication among G and smart appliances. The scheme provides the integrity, privacy and authenticity of the real time meter's data of the individual users power demand and aggregates them as real time response. A distributed pair-wise key is proposed to securely collect individual power demand between G and D_i.

REFERENCES

[1]. Smart Grid Website. US Department of Energy. [Online]. Available: http:www.oe.energy.gov/smartgrid.htm

[2]. Y. Yan, Y. Qian, and H. Sharif, "A secure and reliable in-network collaborative communication scheme for advanced metering infrastructure in smart grid "in IEEE Wireless Communication and Networking Conference (WCNC), march 2011, pp. 909-914.

[3]. B. Vaidya, D. Makrakis, and T. Hussein, "Device authentication for smart energy home area network", in IEEE International Conference on Consumer Electronics, 2011.

[4]. T. Matsumoto, T. Kobayashi, S. Katayama, K. Fukushima, and K. Sekiguchi, "Information-theoretic approach to authentication codes for power system communications," in IEEE Transmission and Distribution Conference and Exposition, 2010.

[5]. J. Xia, Y. Wang, "Secure Key Distribution for the Smart Grid", IEEE Transaction, Volume 3, no.3, 2012, pp.1437-1443.

[6]. J. Kamto, L. Qian, J. Fuller, J. Antia, "Light Weight Key Distribution and Management for Advanced metering Infrastructure", in IEEE International Conference on GLOBECOM Workshops, Dec. 2011, pp. 1216-1220.

[7]. T. Wu, and C. Hsu, "Efficient user identification scheme with key distribution preserving anonymity for distributed computer networks", in Computer&Security, Volume 23, no. 2, 2004, pp. 120-125.

[8]. "National Institute of Standards and Technology Draft, Rev. 1.0", *NIST Framework and Roadmap for Smart Grid Interoperability Standards*, 2009.

[9]. M. Anastasopoulos , A. Voulkidis , A. V. Vasilakos and P. Cottis "A secure network management protocol for smartgrid bpl networks: Design, implementation and experimental results", *Science Direct: Comput. Commun.* vol. 31, no. 18, 2008, pp. 4333 -43 427.

[10]. R. L. Rivest, A. Shamir, and L. M. Adleman, “A method for obtaining digital signatures and public key cryptosystems (reprint),” Commun. ACM, vol. 26, no. 1, 1983, pp. 96–99.

[11]. P. Paillier, “Public-key cryptosystems based on composite degree residuosity classes,” in EUROCRYPT, 1999, pp. 223–238.

[12]. D. Boneh, E.-J. Goh, and K. Nissim, “Evaluating 2-DNF formulas on ciphertexts”, in TCC, ser. Lecture Notes in Computer Science, J. Kilian, Ed., vol. 3378. Springer, 2005, pp. 325–341.

[13]. Diffie W, Hellman M. “New directions in cryptography”. IEEE Trans Inf Theory 1976;IT-22(6):644-654.

[14]. Schneier B. “Applied cryptography”. 2nd ed. John Wiley & Sons, Inc.; 1996.

[15]. Rivest R, Shamir A, Adleman L. ”A method for obtaining digital signature and public-key cryptosystem”. Commun ACM 1978;21(2):120-6.

[16]. Girault M. “An identity-based identification scheme based on discrete logarithms modulo a composite number”. Advances in cryptology EUROCRYPT ’90, Berlin: Springer-Verlag;1991, pp. 481-6.

[17]. Murakami Y, Kasahara M. “A discrete logarithm problem over composite modulus”. Electron Commun Jpn Pt III Fundam Electron Sci 1993;76(12):37- 46.

Halim Halimi received his M.Sc. at the Computer Science and Engineering Department, University Ss Cyril and Methodius-Skopje, Macedonia and is currently working toward gaining his Ph.D. degree in the same institution. He is a research assistant in the Department of Information Technologies at the State University of Tetovo, Macedonia.
His research interests include smart grid security and applied cryptography.