Sensors & Transducers, Vol. 160, Issue 12, December 2013, pp. 148-154

www.sensorsportal.com

Sensors & Transducers

© 2013 by IFSA

http://www.sensorsportal.com

A Study on Security Mechanism of Civil Air Defense and Disaster Warning Control System based on CDMA Wireless Access

Dan CHEN, Yijun LIU
School of Computer Engineering, Jiangsu University of Technology,
Changzhou, Jiangsu, China, 213001
Tel.: 086-13776878588,
E-mail: adair_cd@163.com

Received: 11 October 2013 /Accepted: 22 November 2013 /Published: 30 December 2013

Abstract: Due to the use of wireless transmission and open networks, mobile communications are faced with enormous security threats. This study focuses on security mechanisms of the civil air defense and disaster warning control system based on CDMA wireless access. The working principle and process of authentication and data encryption are presented in detail. Further we propose and develop a novel hybrid cryptosystem combining AES and ECC for this control system in order to achieve the convenience of a public-key cryptosystem and the efficiency of a symmetric-key cryptosystem. Providing high security and encryption efficiency as well as simple management of keys, the proposed cryptographic approach can meet the requirements for security and real-time-ness of data transmission in the wireless access control system. *Copyright © 2013 IFSA.*

Keywords: CDMA wireless access, Security mechanism, Data encryption, Hybrid cryptosystem.

1. Introduction

Mobile communication system is a vital part of modern communication networks for information exchange and transmission. With rapid developments of mobile communication technologies, the security has become one of the most critical problems in communication and received a great deal of attention, while all operators are trying to improve service quality of their own network.

The mobile communication network comprises two general components of the access network and the core network [1]. Security threats which the access network is faced with are mainly from the air interface. When information is transmitted through the air interface of the wireless channel, it's easy for intruders to capture the wireless signals of mobile phones or base stations by using the receiving equipment tuned to the appropriate frequency, and then illegally intercept information about users and network.

The security mechanisms widely used in CDMA wireless access involve the authentication mechanism for active attacks and the encryption mechanism for passive attacks [2]. In this work, we focus on the study of data encryption mechanism, and further propose and develop a novel data encryption approach of hybrid cryptosystem for the civil air defense and disaster warning control system based on CDMA wireless access.

Article number P_1593

2. Existing Security Mechanisms of CDMA Network

With existing security mechanisms, the CDMA mobile communication system has achieved basic security in part. Due to the use of spread spectrum communication, interception of communication contents is almost impossible. Moreover, a set of comprehensive access security mechanisms are adopted, as shown in Fig. 1. Four security algorithms are applied to CDMA wireless access. (1) Cellular Authentication and Voice Encryption, abbreviated as CAVE, is used to query and response according to the authentication protocols and generate keys; (2) Private Long Code Mask, abbreviated as PLCM, is used to control the spread spectrum, and the XOR operator is performed on spread spectrum sequence and data voice to achieve encryption; (3) The algorithm ORYX based on stream cipher of LSFR is applied to the data encryption service for wireless users; (4) Enhanced Cellular Message Encryption Algorithm, abbreviated as E_CMEA, generates symmetric keys to encrypt signaling messages, such as short messages.

The authentication mechanism involves entity authentication and message authentication [3]. Entity authentication is the act of confirming the truth of identities, and message authentication is verifying integrity and authenticity of communication contents for the receiver. During the authentication process, information is exchanged between mobile stations and base stations. Typically, the authentication process involves all entities in the network, including Mobile Switching Center, abbreviated as MSC, Visit Location Register, abbreviated as VLR, Home Location Register, abbreviated as HLR, Authentication Center, abbreviated as AC, Base Station Subsystem, abbreviated as BSS, and the Mobile Station, abbreviated as MS. By using the root key A_Key, entity authentication in CDMA system verifies identities of mobile terminals and network accessing.

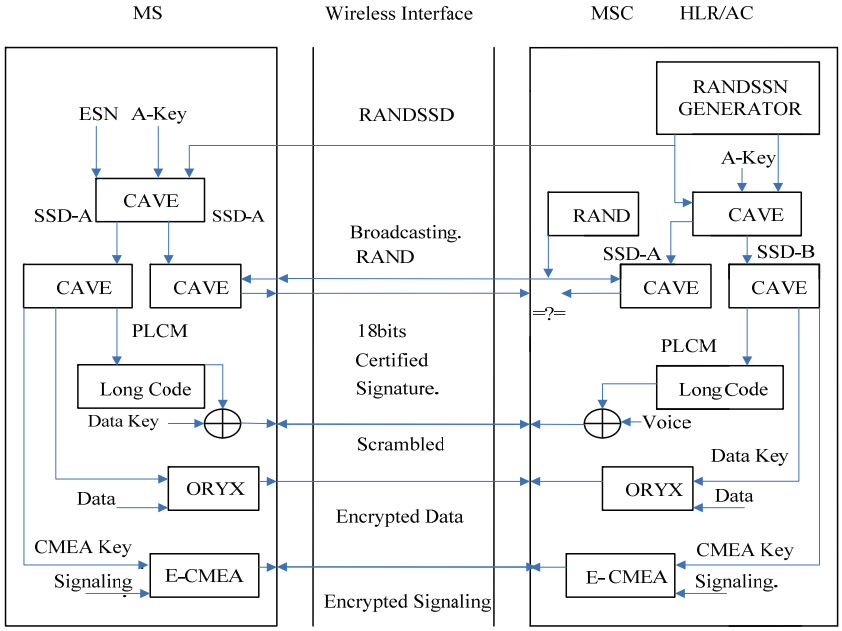


Fig. 1. Security mechanisms of the wireless access CDMA network.

3. Data Encryption of AES and ECC

In the CDMA mobile communication system, a set of comprehensive authentication mechanisms have been used in user identification and access control in order to improve the system security and confidentiality. However, it's not sufficient for the security of mobile networks, and thus a certain encryption technology is necessary. The essential encryption objects of wireless access are voice, signaling and data.

The data encryption technology is significantly important in practical applications of the CDMA system [4]. In cryptography, symmetric-key cryptography and public-key cryptography are widely used [5]. In symmetric-key cryptography, the same cryptographic keys are used for both encryption of plaintext and decryption of ciphertext. As a symmetric-key cipher, the algorithm Rijndael has been chosen by the NIST as Advanced Encryption Standard, abbreviated as AES, due to the fact that it not only has a good anti-attack performance, but also has high execution efficiency and a low computational cost in comparison with other various symmetric-key block cipher algorithms. In public-key cryptography where the sender and receiver are not required to share a common key in order to communicate securely, the algorithm ECC, i.e. Elliptic Curve Cryptography, is usually used.

3.1. Advanced Encryption Standard AES

As the basis of AES, the algorithm Rijndael designed by Joan Daemen and Vincent Rijmen has excellent anti-attack capability and performance [6].

The algorithm Rijndael is a flexible block encryption algorithm, supporting variable block and key sizes of 128, 192 and 256 bits, and iteration numbers of 10, 12 and 14. The iteration number relates with block and key sizes. Note that the block size is always 128 bits in AES. The possible iteration number of 10, 12 or 14 corresponds to the key size of 128, 192 or 256 bits respectively. Multiple rounds of operations such as substitutions, column mix, etc. are performed in execution of the algorithm.

The algorithm Rijndael not only has excellent anti-attack capability of resisting differential and linear cryptanalysis attack, square attack, algebraic computation attack, XSL attack and so on, but also has high efficiency of encryption and decryption. Due to variable sizes of the key and the plaintext block, the algorithm provides a high degree of design flexibility, overcoming the disadvantage of DES, i.e. Data Encryption Standard. Moreover, it has a low memory requirement [7]. Therefore this algorithm is applicable to encryption and decryption in wireless data communication service.

3.2. Elliptic Curve Cryptography ECC

In 1985, N. Koblitz and V. Miller independently proposed Elliptic Curve Cryptography, ECC for brevity, whose security is based on the intractability of the elliptic curve discrete logarithm problem, ECDLP for brevity [8, 9].

An elliptic curve denoted by E is a plane curve which consists of the points satisfying the Weierstrass equation:

$$y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6 \quad (1)$$

along with a distinguished point at infinity, where $a_i \in F$, i=1,2,3,4,6, F is a field. The ordered pair (x, y) satisfying the equation (1) represents the point on the elliptic curve over field F. The F can be the rational number field or the finite field $GF(Pr)$. The ECC uses a particular elliptic curve over a finite field satisfying the equation (2):

$$y^2=x^3+ax+by \pmod p, \quad (2)$$

where p is referred to as the rank of the elliptic curve, is a prime or a power of 2, and a and b satisfy $4a^3+27b^2 \neq 0$.

The problem ECDLP is: given a prime p, an elliptic curve E, points P and Q on E, find a number k less than p, such that $Q=kP$. It has been proved that it is tractable to compute Q given k and P but intractable to compute k given Q and P. Due to this intractability which is the principle of ECC, a small key size in ECC can produce equal security provided by other public-key cipher algorithms.

The ECC cryptosystem provides the highest bit-strength among all public key cryptosystems at present. It has advantages of high security strength per bit, low computational cost, excellent efficiency, small storage space, low bandwidth requirement, and simple key management [10]. Providing a high security with low cost and low time delay, the ECC is especially suitable for the wireless communication situations demanding high efficiency with limitations of computing capability, space of integrated circuit, and bandwidth [11].

4. The Civil Air Defense and Disaster Warning Control System Based on CDMA Wireless Access

With a wide application range, the CDMA wireless data transmission system can be applied to almost all data transmission businesses of low or medium rate [12, 13], such as industrial remote signaling, telemetry and remote control, automation of city electricity distribution network, Internet access, stock information, public security, etc.. Besides traditional Internet applications, the CDMA wireless terminals also support electronic commerce of B2B and B2C and related electronic payment, stock trading, and the bank transfer, etc. The TCP/IP protocol stack is embedded in the CDMA 1X wireless data terminal [14], to simplify the interface design and realize the transparent data transmission between the user terminal and the server. Thus remote wireless data transmission can be achieved conveniently by using CDMA technology.

In this work, the civil air defense and disaster warning control system is designed and implemented by using the CDMA wireless access technology. This system is a typical application of CDMA technology in industrial remote signaling, sensing and telemetry [15, 16]. In particular, the encryption technology is used to enhance security of this civil air defense control system. The system has two primary components of the central control center and the remote alarm terminal, and the other parts are provided by China Unicom Corporation. The system architecture is shown in Fig. 2.

The alarm instructions are issued by the computer in the central control center. Then they are transferred to the remote alarm terminal through the Internet and CDMA networks. After receiving the instructions, the remote alarm terminal starts the alarm, e.g. electric alarm or acoustic alarm. The alarm ringing is automatically transmitted to the central control center and then displayed on the computer's electronic map.

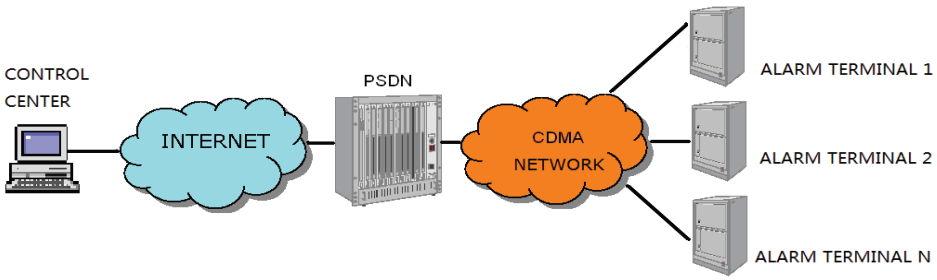


Fig. 2. Architecture of civil air defense and disaster warning control system.

As the alarm executor, the remote alarm terminal is a control terminal for electric alarm or acoustic alarm. Its working principle is as follows. After receiving legal instructions from remote control or effective keyboard operations, the alarm controller completes the alarm task through driver circuit for the electric or acoustic alarm. Fig. 3 illustrates the structure of the remote alarm terminal. The remote alarm terminal comprises the microcontroller AT89C52 of Atmel company, the CDMA 1X wireless data transmission terminal, i.e. the CDMA communication module, the voice circuit, the sound intensity detection module, man-machine interface, and alarm driver, etc., realizing the functions of communication, broadcast, state detection and manual operation, etc.

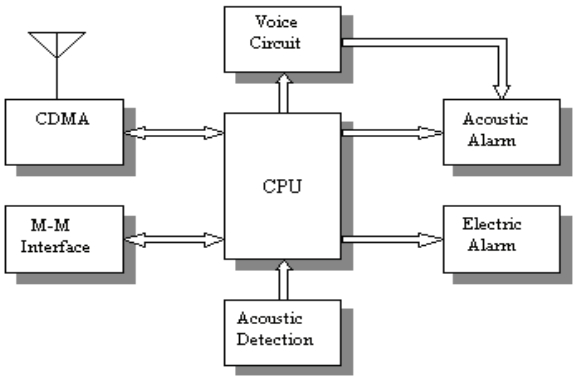


Fig. 3. Structure of the remote alarm terminal.

5. The proposed Hybrid Cryptosystem Combining AES and ECC

In comparison to public-key encryption, the requirement that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption. Public-key cryptosystems are convenient in that they do not require both parties to share a common secret. However, they often rely on complicated mathematical computations and are thus generally much more inefficient than symmetric-key cryptosystems [17]. In many applications, the high cost of encrypting long messages in a public-key cryptosystem can be prohibitive.

Apart from a high security, the real-time communication and quick response are significantly critical for the civil air defense and disaster warning control system. Considering the requirements of this wireless access control system, we propose a hybrid cryptosystem combining AES encryption with ECC, in order to achieve the convenience of a public-key cryptosystem and the efficiency of a symmetric-key cryptosystem. It is worth pointing out that the digital signature [18] and authentication are also included in the proposed hybrid cryptosystem.

5.1. Components of the Hybrid Cryptosystem

The hybrid cryptosystem has three major components: ECC-based generation of public and secret keys, AES-based data encryption and decryption, and digital signature.

1. ECC-based generation of public and secret keys.

Appropriate parameters are selected to construct the encryption elliptic curve [19]. Assume that $E=(p, a, b, G, n, h)$ represents the elliptic curve defined on the binary field, where p, a and b determine an elliptic curve, G is the base point, n is the order of point G, h is the integer part of the quotient when dividing m, the number of all points on the elliptic curve, by n. The parameters of p, a, b, G is public. A point P with order of n on the elliptic curve E is selected, where n is a large prime number and P is public. A random integer of K_s is generated in [1, n-1], and K_p is computed by $K_p = K_sP$. Thus the key pair (K_s, K_p) is determined, where K_s is the secret key and K_p is the public key.

2. AES-based data encryption and decryption.

1) Encryption and decryption of the secret key.

In the encryption of the AES secret key, the plaintext, i.e. AES key, is coded into the point $M=(mx, my)$ on $Ep(a, b)$, and a random integer r is generated, $r<n$. Then compute $C_1=M+rK$ and $C_2=rG$. C_1 and C_2 are transmitted to the receiver.

After receiving the message, the receiver decrypts the AES secret key. The point M is obtained by computing $C_1-kC_2=M+rK-K(rG)=$ $=M+rK-r(kG)=M$. Then M is decrypted to the AES secret key.

2) Encryption and decryption of the text.

For the AES encryption of plaintext, a 128-bit secret key is generated and then the plaintext is converted into byte blocks. The AES encryption has a fixed block size of 128 bits, and the spaces are used to supplement the insufficient block. A block is organized to four rows with 4 bytes per row, which is considered as a state. Data writing and reading adopt column priority and unit of byte. To transform the original plaintext into the ciphertext, a set of rounds are applied, which involve nine rounds of ByteSubs, ShiftRows, MixColumns and AddRoundKey, and one round of ByteSubs, ShiftRows and AddRoundKey.

In the process of decryption, the secrete key is obtained by decrypting the received message, and then a set of reverse rounds are applied to transform ciphertext back into the original plaintext using the key. The ciphertext is grouped into 128-bit blocks for a series of transformations.

3. Digital signature.

The digital signature on the elliptic curve involves three components of the key generation algorithm, signature algorithm and authentication algorithm.

1) Key generation algorithm.

For key generation, a secure Hash function is predetermined firstly. The elliptic curve $E=(p, a, b, G, n, h)$ and the key pair (K_s, K_p) defined as before are used, where K_s is the secret key and K_p is the public key. The Hash function, elliptic curve parameters and the public key K_p are public.

2) Signature algorithm.

The signature algorithm for the message M is outlined as follows.

Step 1. Randomly select a large integer K such that $2 \leq K \leq n-2$;

Step 2. Compute $K \times P=(x_1, y_1)$, $r=x_1 \bmod n$. If $x_1 \in GF(2^K)$, continue. If $r=0$, go to step 1 to re-select the K;

Step 3. Compute $s=K^{-1}(H(M)+K_s \bullet r) \bmod n$, where $H(\ )$ is a one way Hash function $SHA(\ )$, and M is the plaintext. IF $s = 0$, go to step 1 to re-select the K;

Step 4. Return (r, s), the signature of the message M.

3) Authentication algorithm.

The receiver performs authentication as follows.

Step 1. Calculate $c = s\text{-}1 \bmod n$ and $H(M)$;

Step 2. Calculate $u_1=H(M) \bullet c \bmod n$, and $u_2 = r \bullet c \bmod n$;

Step 3. Calculate $u_1P = u_2K_p = (x_0, y_0)$, and $v = x_0 \bmod n$;

Step 4. Return the authentication result. The signature is correct if $v=r$, and incorrect otherwise.

5.2. Procedure of Encryption and Decryption

The task of the cryptosystem is to encrypt and decrypt terminal data, enhancing the security of data transmission. The communication flow is shown in Fig. 4.

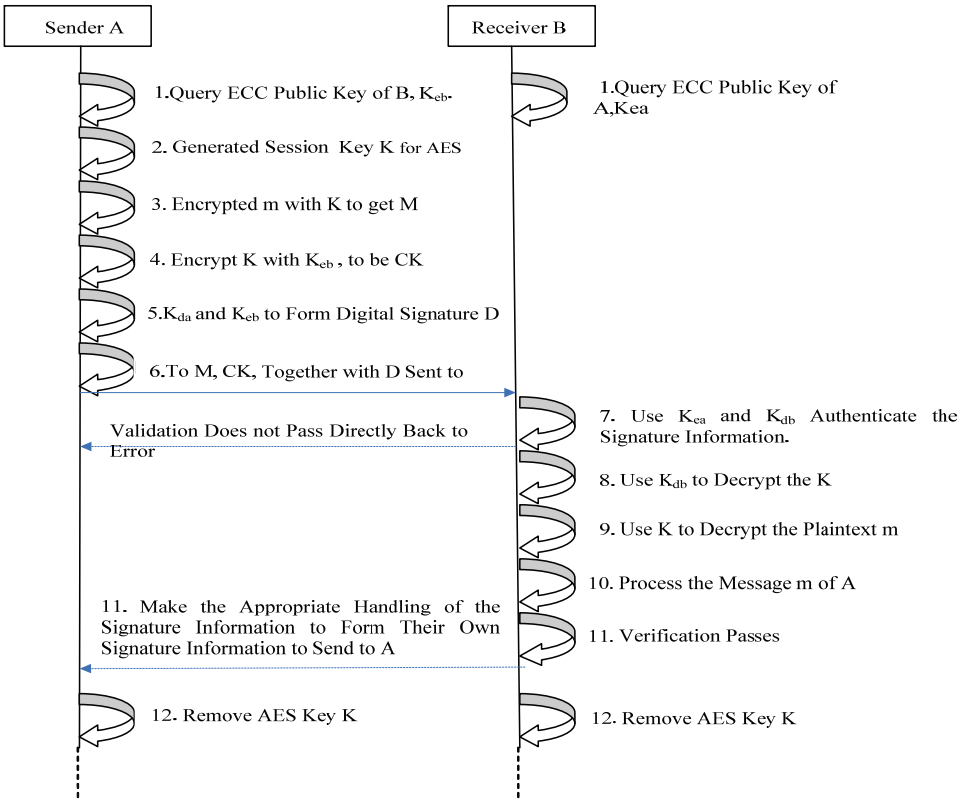


Fig. 4. Flowchart of encryption and decryption in the hybrid cryptosystem.

In ECC, the pair of encryption keys is generated with the public key and the elliptic curve parameters. Assume that *A* is the sender which has encryption key K_{ea} and decryption key K_{da}, and *B* is the receiver which has encryption key K_{eb} and decryption key K_{db}. At first *A* randomly generates the AES key *K*, i.e. the session key, and obtains ciphertext *M* by encrypting the message of plaintext *m*. Then *A* encrypts the key *K* by using the ECC algorithm to achieve digital signature, and finally sends the ciphertext *M* and the encrypted key, together with the signature to *B*. After receiving them, *B* decrypts the session key by using the ECC algorithm and verifies the signature. If the signature is verified, this session key is used to decrypt the ciphertext *M* to obtain plaintext *m*.

5.3. Implementation of the Hybrid Cryptosystem

Here we describe the implementation of the proposed hybrid cryptosystem combining AES and ECC for wireless network communication system. The defined base class Crypto for encryption and decryption has three member functions of SetKey( ) for key generation, EnCrypto( ) for encryption and DeCrypto( ) for decryption. In two classes of AESCrypto and ECCCrypto derived from the base class, the concrete algorithms of the AES and ECC encryption are implemented respectively by overriding the member functions of the base class. The code fragment of hybrid data encryption combining AES and ECC for wireless transmission is as follows.

```
BOOL CreatSocket (BSTR sendData, BSTR*
precvData, int ServerIP, int Port, BSTR szError)
{     int Status, iReturn;
///Initialize Winsock. And assign the socket IP
address and Port.
      ……
// Establish a connection to the server socket.
      connect(ServerSock, (PSOCKADDR)
&destination_sin, sizeof(destination_sin));
/// Send a string to the server.
      SetKey(key, 256); /// Key generation.
      EnCrypto(ciphertext, sendData); /// Data
encryption, sendData is the plaintext to be sent.
      BYTE* pSendData;
      int len =
Encoding::UnocodeToBytes(ciphertext,
&pSendData);
      send(ServerSock, (char*) pSendData, len, 0);
      free(pSendData);
/// Receive data from the server socket.
      BYTE* pRecvData;
      iReturn = recv(ServerSock, (char*)
pRecvData, len, 0); /// pRecvData is the
received ciphertext to be decrypted into
plaintext.
      DeCrypto(plaintext, pRecvData); /// Data
decryption
      Encoding::BytesUnocode(plaintext, len, &str);
      *precvData = str.AllocSysString( );
///Disable ServerSock.
      ……
}
```

6. Conclusions

In this paper, we study security mechanisms of the CDMA air interface and analyze data encryption technologies. A hybrid cryptosystem combining AES and ECC is proposed for the civil air defense and disaster warning control system based on CDMA wireless access. The proposed cryptographic approach which involves the data encryption and decryption, digital signature and authentication, not only provides a high security with simple management of keys for data transmission on the CDMA public network channel in mode of Internet access, but also guarantees real-time-ness of communication due to high efficiency of data encryption and decryption.

Acknowledgements

This work is supported by University Natural Science Research Project of Jiangsu Province (No.12KJD520003) and Applied Basic Research Program of Jiangsu University of Technology (No. KYY10059). Furthermore, we are indebted to the support and encouragements received from the staff and colleagues of the school of computer engineering.

Reference

[1]. V. Garg, Wireless Communications & Networking, *Morgan Kaufmann*, 2007.

[2]. M. Shin, J. Ma, A. Mishra, W. A. Arbaugh, Wireless Network Security and Interworking, in *Proceedings of the IEEE*, Vol. 94, Issue 2, 2006, pp. 455-466.

[3]. M. Bohge, W. Trappe, An authentication framework for hierarchical ad hoc sensor networks, in *Proceeding of the 2nd ACM Workshop on Wireless Security*, New York, USA, September 2003, pp. 79-87.

[4]. J. H. Roh, M. Y. Kim, H. K. Moon, An approach to designing lightweight security protocol on binary CDMA sensor networks, in *Proceedings of the International Conference on Ultra Modern Telecommunications & Workshops (ICUMT'09)*, St. Petersburg, Russia, 12-14 October 2009, pp. 1-6.

[5]. N. Ferguson, B. Schneier, T. Kohno, Cryptography Engineering: Design Principles and Practical Applications, *John Wiley & Sons*, 2010.

[6]. T. Jamil, The Rijndael algorithm, *Potentials, IEEE*, Vol. 23, Issue 2, 2004, pp. 36-38.

[7]. G. Di Natale, M. Doulcier, M. L. Flottes, B. Rouzeyre, A reliable architecture for parallel implementations of the advanced encryption standard, *Journal of Electronic Testing*, Vol. 25, Issue 4-5, 2009, pp. 269-278.

[8]. Alghazzawi, M. Daniyal, A Novel Password based Multi Party Key Agreement Protocol on Elliptic Curve, *International Journal of Computer Science & Information Technology*, Vol. 4, Issue 1, 2012, pp. 75-81.

[9]. Kar, Jayaprakash, B. Majh, An Efficient Password Security of Three Party Key Exchange Protocol based on ECDLP, *International Journal of Security & Its Applications*, Vol. 3, Issue 4, 2009, pp. 25-32.

[10]. M. Morales-Sandoval, C. Feregrino-Uribe, A hardware architecture for elliptic curve cryptography and lossless data compression, in *Proceedings of the 15th International Conference on Electronics, Communications and Computers (CONIELECOMP' 05)*, Puebla, Mexico, 28-02 February 2005, pp. 113-118.

[11]. X. Lin, The Application of Elliptic Curve Cryptography in Electronic Commerce, in *Proceedings of the IEEE Symposium on Electrical & Electronics Engineering (EEESYM' 2012)*, Kuala Lumpur, Malaysia, 24-27 June 2012, pp. 547-549.

[12]. C. Jun, L. Jingli, A Wireless Data Acquisition and Transmission System Design, in *Proceedings of the First International Workshop on Education Technology and Computer Science (ETCS '09)*, Wuhan, China, 7-8 March 2009, pp. 768- 772.

[13]. R. X. Gao, P. Hunerberg, Design of a CDMA-based wireless data transmitter for embedded sensing, *IEEE Transactions on Instrumentation and Measurement,* Vol. 51, Issue 6, 2002, pp. 1259-1265.

[14]. K. H. Walse, D. R. Dhotre, Wireless network: Performance analysis of TCP, *Information Technology Journal,* Vol. 6, Issue 3, pp. 363-369.

[15]. W. Xiaoli, G. Xiaohong, L. Jianwei, Research on remote intelligent monitoring system, in *Proceedings of the 2011 International Conference on Uncertainty Reasoning and Knowledge Engineering (URKE'2011)*, Bali, Indonesia, 4-7 August 2011, pp. 52-55.

[16]. W. Xiaoli, L. Jianwei, CDMA-based application of wireless intelligent monitoring system, in *Proceedings of International Conference on Computer, Mechatronics, Control and Electronic Engineering (CMCE'10)*, Changchun, China, 24-26 August 2010, pp. 278-281.

[17]. W. Haodong, S. Bo, C. C. Tan, L. Qun, Comparing Symmetric-key and Public-key Based Security Schemes in Sensor Networks: A Case Study of User Access Control, in *Proceedings of the 28th International Conference on Distributed Computing Systems (ICDCS' 08)*, Beijing, China, 17-20 June 2008, pp. 11-18.

[18]. J. Stapleton, P. Doyle, S. T. Esquire, The digital signature paradox, *in Proceedings of the Sixth Annual IEEE SMC, Information Assurance Workshop (IAW'05)*, West Point, NY, USA, 15-17 June 2005, pp. 456-457.

[19]. IEEE Std 1363-2000, 2000. IEEE Standard Specifications for Public-Key Cryptography, Approved 30 January 2000.

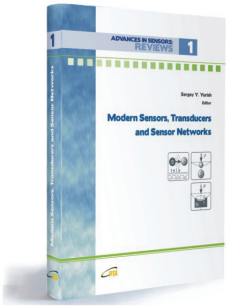
2013 Copyright ©, International Frequency Sensor Association (IFSA). All rights reserved.
(http://www.sensorsportal.com)

International Frequency Sensor Association (IFSA) Publishing

ADVANCES IN SENSORS: REVIEWS 1

Modern Sensors, Transducers and Sensor Networks

Sergey Y. Yurish, Editor



Formats: printable pdf (Acrobat) and print (hardcover), 422 pages

ISBN: 978-84-615-9613-3,
e-ISBN: 978-84-615-9012-4

Modern Sensors, Transducers and Sensor Networks is the first book from the Advances in Sensors: Reviews book Series contains dozen collected sensor related state-of-the-art reviews written by 31 internationally recognized experts from academia and industry.

Built upon the series Advances in Sensors: Reviews - a premier sensor review source, the *Modern Sensors, Transducers and Sensor Networks* presents an overview of highlights in the field. Coverage includes current developments in sensing nanomaterials, technologies, MEMS sensor design, synthesis, modeling and applications of sensors, transducers and wireless sensor networks, signal detection and advanced signal processing, as well as new sensing principles and methods of measurements.

Modern Sensors, Transducers and Sensor Networks is intended for anyone who wants to cover a comprehensive range of topics in the field of sensors paradigms and developments. It provides guidance for technology solution developers from academia, research institutions, and industry, providing them with a broader perspective of sensor science and industry.

http://sensorsportal.com/HTML/BOOKSTORE/Advance_in_Sensors.htm