Volume 3, No. 10, October 2012

Journal of Global Research in Computer Science

ISSN-2229-371X

RESEARCH PAPER

Available Online at www.jgrcs.info

A NOVEL ANALYTICAL APPROACH FOR THE PROTECTION OF THE WIRELESS NETWORK

Ravinder Gaur*[1]and D.B.Ojha[2]
*[1]Scientist –C , Department of Science & Technology, New Delhi ,INDIA
and M.Tech. Scholar Mewar University, Rajasthan)
rgaur@nic.in[1]
[2]Department of Mathematics, Mewar University, Rajasthan, INDIA
ojhabrat@gmail.com[2]

Abstract: A novel analytical approach for the protection of the wireless network which may be used for the collection of data on the health of the transmission line is demonstrated in this paper . In present paper, we presented an error free secure wireless communication network security using distributed key management scheme based on several IP technologies, cryptographic method such as asymmetric public key cryptosystem. We used, Ordeal Random Data Encryption System (ORDES), fault detection method, cheater identification and verifiable secret sharing which will further increase the usability of communication channel and facilitate error less delivery of the data on wireless network.

Keywords: Wireless; network, communication; security

INTRODUCTION

With the current economic growth, the need for power is continuously increasing. Currently, there are several efforts to provide high-quality power in various fields are going on world wide [1]. With this trends research works into the diagnosis of high voltage equipment are actively being performed to discover fault symptoms and to analyze the faults in order to not allow the same fault in the future [2]. Most of the monitoring and analysis are done for the insulators and power lines [3]. Insulator are used to isolate the naked power lines and to support the lines mechanically [4].There are several tools and methods used to detect the faults in the transmission line which can be categorized as: thermal imaging cameras [5] , human eyes , electric fields, corona cameras, neon lamp methods [6] and knowledge based approaches such as deployment of Sensors on the transmission tower [9]. Since there are variety of malfunction and fault may occur at the transmission line, the inspection needs to be done without stopping the power transmission. Currently most of the inspections are done periodically for each electric tower relying on human visual detection by an expert in the task [7],[8].

This is real situation with low efficiency, reliability and high risk inspection [4] . To prevent the accident and to improve the inspection reliability, it is the time to replace the human operators with inspection robots which can collect the data on the heath of transmission line [4]. This may lead to reduce the Electric power transmission and distribution losses (% of output) in India was 24.45 as of 2009. Its highest value over the past 38 years was 28.65 in 2001, while its lowest value was 16.36 in 1971. Electric power transmission and distribution losses include losses in transmission between sources of supply and points of distribution and in the distribution to consumers, including pilferage [10]. Technology development in sensors, robotics, unmanned vehicle, satellite and wireless communication could be leveraged to enable the development of an effective automatic inspection system for transmission line/ tower monitoring applications. The system concept was defined based on the sensing needs such as system tempering due to terrorism, manmade encroachment, vegetation encroachment, gun shot at insulators , lightening etc. by deploying the various sensor as per the need on the instrumentation facility provision on power utility towers [9]. The data communication on various parameter of health of the transmission line will rely on wireless / fiber optic technology. This data may be collected by the “Central data base” directly from the sensor/Hub wirelessly using : RF mode ; via Satellite or cell phone network , unmanned airborne vehicle (UAV) , manned aerial vehicle , “line crawler” Robot traveling the length of the line[9].

In a wireless network, data are transmitted through an open space and any node in the coverage area can receive the radio signals. Moreover, in Wireless mesh networks (WMNs), the external environment can be much harsher due to the lack of central administration [11]. Security is a crucial and urgent problem in a wireless network as now a days the activity of unlawful event is happening in every part of the world and security of the transmission line is also a great concern for the nation. The present paper focused on the development of security system in wireless network using data cryptography technique. We are working on the security of a system which constitute Central data base” i.e. commander and a data collection vehicle (sensor , UAV, MAV, Robot) , the all conversation between Commander and date collection vehicle (sensor , UAV, MAV, Robot) to be held within the complete secure system so that unauthorized access to be neglected.

Bit commitment from any one-way function: one can create a bit commitment scheme from any one way function. The scheme relies on the fact that every one-way function can be modified to possess a computationally hard core predicate. Let w be a one way function, with j a hard core predicate. Then to commit to a bit e Participant picks a random input t and sends the triple (j, ω(t) , e+j(t) to robot where + denotes XOR, i.e. addition modulo2. To decommit Participant simply sends t to robot. This scheme is concealing because for robot to recover e he must recover j(t) .Since j is computationally hard core predicate , recovering j(t) from ω(t) with probability greater than one-half is as hard as inverting ω. The scheme bindingness depends greatly on whether or not w is injective.[13,14,15]

If participant wants to commit to some message m he just put in to the sealed envelope, so that whenever participant want to reveal the message to Robot, he opens the envelope. First of all the digital envelope should hide the message from: Robot should be able to learn m from the commitment. Second , the digital envelope should be binding , meaning with this that Participant can not change his mind about m , and by checking the opening of the commitment one can verify that the obtained value is actually the one Participant had in mind originally[12].

PRELIMINARIES

a. A polynomial of degree (u-1) f(x)= a_{u-1} x^{u-1} + $^{\cdots\cdots\cdots}$$a_1$ x + a_0 mod p in the finite field GF(p) is chosen , where $a_{u-1,}$……, a_1 are random integers and a_0= SK. Then , the key pieces SK_i = f(d_i) mod p can be calculated and delivered to each and every responding participant through secure channels.

b. u coordinates (d_1,SK_1), (d_2,Sk_2), ……., (d_u, SK_u) can be acquired through the cooperation from any u participants . According to Lagrange interpolation polynomial

$$SK= f(0)= \sum_{i=1}^{u} SK_i \prod_{j\neq i, j=1}^{u} \frac{d_j}{dj-di} \text{ mod p}$$

Definition 1. A metric space is a set C with a distance function

$$dist : C \times C \to R^{+} = [0,\infty) \, ,$$

Which obeys the usual properties (symmetric, triangle inequalities, zero distance between equal points).

Definition 2. Let C{0, 1}^{n} be a code set which consists of a set of code words c_i of length n. The distance metric between any two code words c_i and c_j in C is defined by

$$dist(c_i, c_i) = \left| c_{ir} - c_{jr} \right|, C_i, C_j \in C$$

This is known as Hamming distance [17].

Definition 3. An error correction function f for a code C is defined as

f (c_i)= {c_j |dist (c_i,c_j) is the minimum, over C\{c_i}} .
Here, c_j = f (c_i) is called the nearest neighbor of c_i.

Definition 4. The measurement of nearness between two code words c and c' is defined by
nearness(c, c')= dist(c, c')/n,
it is obvious that 0 ≤ nearness(c, c') ≤ 1.

Definition 5. The fuzzy membership function for a codeword c' to be equal to a given c is defined as [18]

$$Fuzz(c') = \begin{cases} 0 \text{ if } nearness(c,c') = z \le z_o < 1 \\ z \text{ Otherwise} \end{cases}$$

from papers.

OUR PROCESS

a. A polynomial of degree (u-1) f(x)= a_{u-1} x^{u-1} + $^{\cdots\cdots\cdots}$$a_1$ x + a_0 mod p in the finite field GF(p) is chosen , where $a_{u-1,}$……, a_1 are random integers and a_0= SK. Then , the key pieces SKi = f(di) mod p can be calculated and delivered to each and every responding participant through secure channels.

b. u coordinates (d_1,SK_1), (d_2,Sk_2), ……., (d_u, SK_u) can be acquired through the cooperation from any t participants . According to Lagrange interpolation polynomial

$$SK=f(0)= \sum_{i=1}^{u} SK_i \prod_{j\neq i, j=1}^{u} \frac{d_j}{dj-di} \text{ mod p}$$

c. There are several disadvantages when traditional secret sharing is used in WMNs :
   (a) If a dishonest participant may deliver an incorrect key piece or if there is anything wrong in date transmission , the correct secret key SK cannot be reconstructed
   (b) If there is a malicious attacker among the n participants , it may deliberately deliver a fake key piece to other and , at the same time , receive all the correct key piece from others. Then , only it can reconstruct the correct secret key SK while others who receive a faked piece cannot
   (c) In a wireless mobility environment, an attacker can attack a holder and break one key piece in a limited time and then move to attack all u holders and acquire the u key pieces so as to calculate the shared secret key SK.

Let us consider the matrix equation of the form WUQ where W is a (u x u) , U is (u x1) and Q is a random (1 x 1) matrix.

$$W = \begin{bmatrix} d_1^{u-1} & - & - & d_1 & 1 \\ d_2^{u-1} & - & - & d_2 & 1 \\ - & - & - & - & 1 \\ - & - & - & - & 1 \\ d_u^{u-1} & - & - & d_u & 1 \end{bmatrix},$$

$$U = \begin{bmatrix} a_{u-1} \\ a_{u-2} \\ - \\ - \\ a_0 \end{bmatrix}, \quad P_u = \begin{bmatrix} SK_1 \\ SK_2 \\ - \\ - \\ SK_u \end{bmatrix} \text{ and}$$

$$\overline{W} = \begin{bmatrix} d_1^{u-1} & - & - & d_1 & 1 & SK_1 \\ d_2^{u-1} & - & - & d_2 & 1 & SK_2 \\ - & - & - & - & 1 & - \\ - & - & - & - & 1 & - \\ d_u^{u-1} & - & - & d_u & 1 & SK_u \end{bmatrix}$$

The substance of the Lagrange interpolation polynomial is that there exist a unique feasible solution A in the matrix equation W and P_u are given . A necessary sufficient condition is that the rank of the augmented matrix $\overline{W}$ is the same as that of W which is equal to u, hereby marked as

$R(\overline{W})=R(W)= u$

a. If $R(\overline{W})=R(W) =u$ there is a unique solution for the equation , there is no fault/cheater is detected / existed follow the process (1).

b. If $R(\overline{W})=R(W) < u$ there are more than one solution for the equation warning bell is ringing so more parameter needs to be gathered until step 1.

Process (1)

Public Key = P_u = WUQ

Encryption : c = m P_u + e

Where m is a u bit message , c is n-bit ciphertext , and e is an n bit random error vector of weight a

Decryption: The receiver first calculates

c = cQ^{-1} = mW T + eQ^{-1} ,

Where Q^{-1} is the inverse of Q. Because the weight of eQ^{-1} is the same as the weight of e, the receiver uses the decoding algorithm of the original code T to obtain m' =mW . Finally, the receiver recovers m by computing m = $m'W^{-1}$, where W^{-1} is the inverse of W .

A tuple {P, H, M, f} where M $\subseteq$ $\{0, 1\}^u$ is a message set which consider as a code, P is a set of individuals, generally with three elements A participant as the committing party, Robot as the party to which commitment is made and TC as the analysis wing of the Robot as trusted party, f is error correction function and H = $\{t_i, a_i\}$ are called the events occurring at times t_i, i =0, 1, 2, as per algorithm a_i, i =0, 1, 2. The scheme always culminates in either acceptance or rejection by A and B.

In the setup phase, the environment is setup initially and public commitment key CK generated, according to the algorithm setupalg (a_0) and published to the parties sender and robot at time t_0. During the commit phase, Participant commits to a message m M then robot finds g : m → P_u(m)

Encryption: E = m P_u + e, where m is the u -bit message, E is an u -bit cipher text and e is an n -bit random error vector of weight a.

According to the algorithms commitalge into string c i.e. sender commitment

c = commitalg(XOR, g(m),E),

Then after participant sends c to robot , which Robot will receive as t(c), where t is the transmission function which includes noise.

In the open phase, Participant sends the procedure for revealing the hidden commitment at time t_2 and robot use this.

So Participant discloses the procedure g(m) and E to robot to open the commitment.

openalg: Robot constructs c' . using commitalg, message t(m) and opening key

i.e.

c' = commitalg(XOR, t(g(m)),t(E))
and checks whether the result is same as the received commitment t(c).

Then after acceptance, robot calculates f (c') $(P_u)^{-1}$ and finally gets the message.

Decryption : The robot first calculates c' = commitalg (CK, t(g(m)),t(E)), where t is the transmission function. The robot checks the dist(t(c),c') $\neq$ 0, then apply Error Correction function f to c' and finds f(c') . Then after apply

Fuzzy decision making:

If(nearness (t (c) ,f (c') $\leq$ Z_0))

Then sender is bound to act as in m
Else free not to act as m.

Then robot uses the decoding algorithm of the original code T to obtain

$$m' = m (P_u)$$

Finally, the robot recovers m by computing $m = m' (P_u)^{-1}$, where $(P_u)^{-1}$ is the inverse of (P_u).

CONCLUSION

Our process has advantage that it is using for (u-1) independent variable, then form public/private key. It also reduce noise introduced by the environment during the transmission.

REFERENCES

[1]. D. Kang, "On the study of the defective insulator detection on the power distribution line" Korea inf. Commun. Soc. Vol.25,no.6, pp.46-51 Jun.2000.

[2]. J.Jin, C.S.Chang, T. Hoshino, M. Hanai, and N. Kobayashi, "Classification of partial discharge event is gas insulated substations using wavelet packet transform and neural network approaches," Proc. Ins.Elec. Eng. Sci., Meas., Technol., vol.153 no.2,pp 55-63 Mar.2006

[3]. Z.Li, Y. Ruan , and F. Zhang , " A new posture plan for the inspection robot capable of clearing obstacles in power transmission line maintenance," in Proc. IEEE Int. Conf. Power Energy Eng.,Mar.2009 ,pp1-4

[4]. Y.Cheng, C.Li , and X. Huang, Study of Corona discharge pattern on high voltage transmission lines for inspecting faulty porcelain insulators," IEEE Trans. Power Del., vol.23 ,no.2, pp. 945-952 , Apr.2008

[5]. M. Naghedolfeizi, S. Arora, S. Garcia, "Performance analysis of a high-end CPU under a Heavy computational load and varying RAM amount using thermal imaging techniques" in Proc. IEEE Int. Conf. Autitestcon, Sep.2005 ,pp. 574-577

[6]. G.C. Carter and P.B. Abraham , "Estimation of source motion from time delay and time compression measurements." J. Acoust. Soc. Amer., vol.67,no.3 ,pp.830-832 , Mar. 1980

[7]. P.C. Meuse and H.F.Silverman , "Characterization of talker radiation pattern using microphone array ,"in Proc. IEEE Int. Conf. Acoust., Speech , Signal Process., May'1998 , vol.1 pp 245 -248.

[8]. T. Yamada , S. Nakamura , and K. Shikano , " Hands-free speech recognition based on 3-D viterbi search process., in Proc. IEEE Int. Conf. Acoust., Speech , Signal Process., May 1998 ,vol.1,pp.245-248

[9]. Future Inspection of the Overhead Transmission line.EPRI, Palo Alto, CA:2008 , 1016921

[10]. International Energy Agency (IEA Statistics © OECD/IEA, http://www.iea.org/stats/index.asp), Energy Statistics and Balances of Non-OECD Countries and Energy Statistics of OECD Countries, and United Nations, Energy Statistics Yearbook.

[11]. Peng Xiao, Jinghsa He and Yingfang Fu "Distributed group key Management in Wireless Mesh Networks," in International Journal of Security and its Applications, vol.6, No.2, April'2012

[12]. "A fuzzy commitment scheme with McEliece's Cipher" [ISSN 1842-6298 (electronic) volume 5 (2010) 73-82 http://www.utgjiu.ro/math/sma

[13]. M. Alabbadi and S.B. Wicker , " A digital signature scheme based on linear error correcting block codes, In Josef Piperzyk and Reihanah Safavi –Naini, editors , Asiacrypt '94, 238-248 . Springer –Verlag, 1994. LNCS No. 917.

[14]. V. Guruswami and M. Sudan , Improved decoding of reed –solomon and algebraicgeometeric codes , In FOCS'98, 28-39 , IEEE Computer Society ,1998

[15]. W.W. Peterson , "Encoding and error correction procedures for Bose-Chaudhuri codes (Russian. English original) [J] Kibern. Sb. 6, 25-54 (1963); translation from IRE Trans. Inform Theory IT-6 , 459-470 (1960) . MR0118576 (22#9349).

[16]. Ramveer Singh and D.B.Ojha, "An Ordeal Random Data Encryption Scheme (ORDES)"*International Journal of the Computer, the Internet and Management Vol.18.No.3 (September-December2010pp38-50*.

[17]. V Pless, Introduction to theory of Error Correcting Codes Willey , New York 1982

[18]. A.A. Al-saggaf and H.S. Acharya, A Fuzzy Commitment Scheme, IEEE International Conference on Adavances in Computer Vision and Information Technology 28-30 November 2007 – India

Short BioData for the Athour

Ravinder Gaur received the Bachelor of Engineering degree in Electronics and Communacation Engineering from Institution of Engineers , Kolkata (India) in 2007 , Currently working as Scientist with Department of Science & Technology , New Delhi. His current research interests include development of indegenous electrical instrument , microprocessor application and advanced sensor networks