Journal of Multidisciplinary Engineering Science Studies (JMESS)
ISSN: 2458-925X
Vol. 3 Issue 1, January - 2017

Presentation Of A Hierarchy Algorithm Toward MAC Based Selection For Shielding Application Regarding To Comprehensive Review Of Hash Function Specification

[1]AH. Poursoltan Mohammadi
Department of Electrical Engineering
Urmia University, Urmia, Iran
ah.poursoltan@gmail.com

[2]M. Chehel Amirani
Department of Electrical Engineering
Urmia University, Urmia, Iran
m.amirani@urmia.ac.ir

[3]F. Faghihi
Science and Research Branch
Islamic Azad University,
Tehran
Faramarz_faghihi@hotmail.com

Abstract— Electromagnetic Interference (EMI) is an important part of any design of electrical devices especially when communication data is transferred, it will be so crucial. However, EMI is divided into two main categories: random environmental occurrence and Electromagnetic attack. To achieve data transmission safety, secure route optimization, active and passive shielding are routine approaches. However, there are another type of shielding in the form of software immunity which can be done by cryptography, coding and message authentication code based (MAC-based) Hash function as software shielding of communication data transferring. So several new types of MAC-based Hash functions are introduced and their main parameters are compared. Then suitable MAC-based Hash functions for proposed application are selected and discussed.

Keywords—message authentication code; MAC Hash function; Electromagnetic Interference; Shielding

I. INTRODUCTION

Nowadays, Electromagnetic interference (EMI) has become a gradually more important matter in high-tech mixed system designs [1]. As many user friendly functions are put on communication and electronic devices, such as the amelioration of graphically efficiency and comfort, and the increase of security Contains passive and active, The contents of Information Technology (IT) are brought into the electronic devices and systems in the forms of network, software, and etc. [2]. In this way, cyber-security Troubled Issues produce many harmful impact for malfunctioning data transmission. Cyber-physical networked systems (CPNS) may operate in the hostile environment and the sensor nodes in CPNS lacking Tamper-resistance hardware increase the possibility to be compromised by adversaries [2], [3].

In previous research, a number of project have been made to limit false data injection in communication networks; But those projects have their problems and cannot be used to Good Resistance whit attacks related to CPNS [4]. So, data authentication is required, too. As Hierarchal Algorithm for cyber-attack to communication data transferring between two critical nodes, route optimization considering electromagnetic compatibility (EMC) phenomena, passive and active shielding and then virtual software shielding must be designed and implemented. Firstly, to contribute more attention for probabilistic electromagnetic attack area, the optimized route considering route drop, cost and EMI omission should be obtained. Secondly, using shielded cables, piece wise continuous and discrete conduits are preferred for high risk electromagnetic (EM) field attack area. However, in this paper we focus a virtual shielding based on authentication using MAC-based Hash functions. It is obvious that coding is initially must be done for more data security based on bit error rate (BER) calculation that it is designed convolutional codes or turbo codes [5]. All of the software operation including cryptography, coding and Hash functions can be called software shielding effectiveness (SSE). This paper only emphasizes the recent MAC-based hash function for SSE. So several MAC-based types except standard types such as ECBC, FCBC, XCBC and HMAC is discussed and compared for proposed application.

II. EMI AND DATA TRANSMITION

The probability of intentional electromagnetic interference has been perceived and searched in different and scientific papers [6]-[8]. In this regard, intentional electromagnetic environments (IEME) are classified by technical properties of the source, these properties include: [9]–[12]:

1) The threat level or Peak electric field;

2) Bandwidth classification or Frequency coverage;

3) Average power density

4) Energy content;

5) Coupling mechanism such as radiated or conducted [13].

Specification of EMI sources and the definition of their effect has a high preference during the Step Design and for electromagnetic compatibility (EMC) of each system [14]. It is clear that modeling technique is not proper to forecast the EMI problems (noise levels) in EM-attack [15].due to the widespread use of electronic and communication equipment in Industrial applications and high security places, Research in the field of electromagnetic shielding materials every day becomes more and more important. [16]. Due to probability EM attack to data transferring from EM source to destination electronic-communication devises, route optimization, shielding and then SSE must be analyzed. In the following sub-section, above methods are introduced briefly.

A. EMI simulation

To achieve Electromagnetic situation of an environment, field distribution simulation should be done. Especially flux density distribution simulation for magnetic field detection is taken to account as primary research work. In past research paper, several numerical techniques such as Finite Element Method (FEM), Finite Difference Time Domain (FDTD) method of moment (MOM), Time Domain Physical Optics (TDPO) are used. Also, the hybrid method such as improved Finite Element Boundary Integral (FE-BI) method with TDPO for precise 3D field simulation of combinative-complex objects presented in many researches [17]. A key research paper presents a hybrid methodology that combines an extended from FDTD method with TDPO for analysis of 3D scattering of combinative objects in complex EMC problem [pier time domain].

B. route optimization

The important reason for redesigning the cable route is to find ‘‘interference field’’ locations that are creating disturbances for control cables and LV equipment or other sensitive transmission conductors [18]-[20]. Considering EMC design, Great benefits of optimal routing cables with shielding are:

(a) The use of existing shield in the system.

(b) An optimal route with less interference fields to reduce the cost of shielded cable.

(c) Shielding performance is improved by creating an optimal path and extra protection.

(d) Using optimized cable routing, as an incentive to reduce the degree shielding effectiveness on electromagnetic compatibility considerations. The advantages of this method is in using less rigid cables. [21]. different optimization methods for conductor’s route selection are Analytical Hierarchy Process (AHP), fuzzy logic, Artificial Neural Network [22].

C. shielding effectiveness (SE)

Magnetic materials such as iron, copper, zinc are used for passive shielding. Main formula for shielding effectiveness are described as [23]-[25]:

$$SE_E = 20\,log_{10}\left|\frac{E_i}{E_t}\right|\ dB \qquad (1)$$

$$SE_B = 20\ log_{10}\left|\frac{H_i}{H_t}\right| \qquad (2)$$

Where, E and H are Electrical Field and Magnetic field. After field simulation such as Fig. 1, SE can be achieved and for a cavity, graph of SE-f plotted. Sample graphs are shown in Fig. 2 for conceptual cavities.

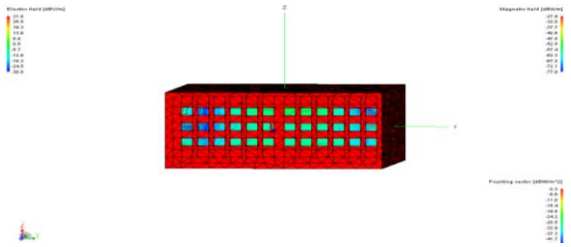

Fig. 1. The magnetic field distribution in Enclosure with Three rows and twelve apertures

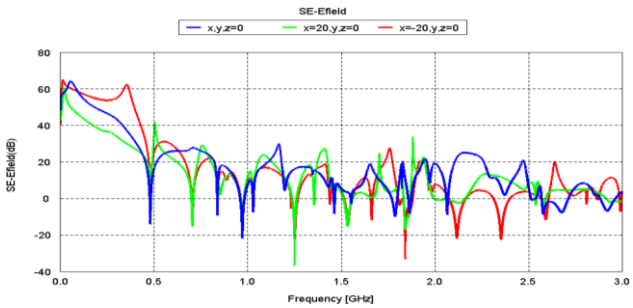

Fig. 2. SE-f curve

However, active shielding is also can be considered for closed enclosure including core and windings. It is obvious that data transmission safety can be discussed by route optimization, shielded conductor and SSE. In this paper, we focus on SSE in following sub-section.

D. software shielding effectiveness (SSE)

The use of error-correcting codes for error-free system design can increase the reliability of the entire system from the point of view of EMC, Which is called “Secondary Shielding” [26]. On the other hand, using of data authentication function can be attractive for passive defense designers. In this way hash function such as message authentication code (MAC), and similar type is so crucial. We define software shielding effectiveness (SSE) as follow: set of coding algorithm, cryptography, and hash function which can be applied to software system of data transferring to achieve high reliability secure system. In this paper, we deal with hash function especially, however coding algorithm is expressed briefly.

1. coding algorithm

There are two types of coding algorithm which is applied to software system normally for SSE purposes. Firstly, convolutional code which is explained in [26] for secondary shielding. In this study, a hybrid algorithm based on channel coding method for error-free

electromagnetic interference (EMI) caused by inside and outside fields of current injection transformer (CIT) and its control system for short circuit tests provided. For this aim, the classic convolution encoder whit code rate ½ is employed [26]. Secondly, turbo codes can be used for some special application. In a cited research [27] 20 years of turbo coding and energy-aware design guidelines for energy-constrained wireless applications is presented. Therefore, due to its extensive use of operational communications standards such as LTE [28] and WiMAX [29], turbo codes are acceptable and reliable for energy-constrained wireless communication applications.

2. hash function

If we use hash function, bandwidth must be increased especially, cost of secure channel also will be added hash function causes low speed data transmission, so choosing of appropriate hash function which is created tradeoff between collision-free and data transferring speed is so crucial. In this way, probability of attacker noise and change to transferred data is considered. The main deal of this paper discusses about this subject for data authentication as secondary shielding. Data origin authentication and data integrity protection are extensively necessary in several practical application, e.g. banking communications (MACs) [30-34] can used these two services. MAC is asymmetric key incipient, requiring its Person that use to share a secret key K in Continuation. For sending a message M, the sender computes Tag=MACk(M), after that send (M,Tag) out. In the following, On receiving of such a pair, the receiver re-computes Tag´=MACk(M) and believes the pair (M,Tag) to be valid, if Tag=Ta(g)´[35].

III. SURVEY OF APPROPRIATE MAC BASED HASH FUNCTION FOR SSE

As told before, according to several considerations of error-free coding algorithms, possibility of malfunctioning occurrence or faulty operation is also possible. So, hash function, although causes band width increasing and delay creating is so important as final SSE task. Advanced MAC-based is the best alternative for proposed investigation.

A: Hash function definition

Hash function are defined generally as:

1- Given a message $\underline{m}$, it is too easy to calculate the message digest $\underline{d}=\hat{h}(\underline{m})$, where $\underline{d}$ is also called a hash output, so $\hat{h}$ is Obtained.

2- Given a digest $\underline{d}$, it is too hard to compute the message $\underline{m}$ due to $\underline{d}=\hat{h}(\underline{m})$, so $\hat{h}$ is one-way;

3- Given any optional message $\underline{m}$, it is computationally impossible to find another message $\underline{\acute{m}}$ such that $\hat{h}$ (m) =$\hat{h}$ ($\underline{\acute{m}}$), so $\hat{h}$ is weakly collision-free

4- It is computationally impractical to find two optional messages $\underline{m} = \underline{\acute{m}}$ such that $\hat{\mathrm{h}}$ (m) =$\hat{\mathrm{h}}$ ($\underline{\acute{\mathrm{m}}}$), so $\hat{\mathrm{h}}$ is strongly collision-free.

"Impractical" word refers to problems that, cannot be solved in tolerable sub exponential time or polynomial time [36].

B: CBC MAC definition

We know that a block cipher uses an accidental key $a \in \{0,1\}^K$, so a group of functions defined that contain a function for all possible key in $\{0,1\}^K$. this function is called F. It is important, two distinct keys May show the same function. The distribution is a uniform random election of a key in $\{0,1\}^K$ and using the key to specify the function of the block cipher.

Given a group of functions *F* from $\{0,1\}^l$ to $\{0,1\}^k$ (denoted the underlying group of functions) the CBC MAC authentication layout *CBC-MAC*^{F} is specified by selecting at random a function $f \in F$ (unknown to the attacker) due to the distribution of the group, and then the authentication of a message *X* of *m* blocks (i.e., *X* = *x*1, *x*2, ., *xm*), is specified as [37]:

$$f^{(m)}(x_1,.,x_m) = f(f(.f(f(x_1)\oplus x_2)\oplus.\oplus x_{m-1})\oplus x_m \quad (3)$$

It will also be appropriate to specify $f^{(0)}(\varepsilon) = 0^l$ (for the empty series ε). most of the time, we want not to define the length of X, and then we write $f^{(*)}(X)$, that means the same as above with m being the blocks (In terms of number) in the input message X .a kind of family of CBC MAC that we call EMAC (encrypted CBC MAC) is specified as follows. Let F be a group of functions. Pick two functions f_1, $f_2 \in F$ independently due to the distribution of the group. For a message X = x1, x2, xm as above, we describe:

$$EMAC_{f_1,f_2}(X) = f_2\left(f_1^{(m)}(X)\right) \quad (4)$$

We explain by $EMAC_f$ the group of functions gained by using EMAC with the group F. We say that if only one secret function f is assumed instead of the pair f_1, f_2, and one may use the series f (0) and f (1) to identify the two functions f_1, f_2. (We accept that the length of a key is smaller than the length of a block and that f (b) (b = 0, 1) is Not long enough to get the keys. Then, one may take more values of f(0), f(1), f(2), .) It is very easy to display that if F is a unreal random group of functions, then this extra step does not neutralize the security of the system, and we deny this part in what follows.

According to the review above, we would like to comment on the empty string, we describe $f_1^{(0)}\varepsilon$ to be the zero string 0^l, and thus $EMAC_{f_1,f_2}(\varepsilon)$ is specified to be $f_2(0^l)$. our evidence of security assumes this Ability to manage of the empty string [37].

C: new MAC algorithms in recent research:

Several new MAC hash functions are introduced. According to proposed application, three categories are selected and pair wise comparison with conventional MAC scheme are given in tables 1, 2, 3 [36], [38] and [39].

TABLE. 1. BANDWIDTH AND COMPUTATION OF PMAC &SPACE MAC

Scheme	Tag size Per block	Key size per block	MAC &Verify
Space MAC	14 bytes	448 bytes	368.7 μs
PMAC	14 bytes	32 bytes	26.4 μs

Where PMAC and Space MAC are two kind of homomorphic message authentication code [38]. Bandwidth and computation overhead of PMAC and Space MAC Specified in Table. 1.

TABLE. 2. COMPARISON BETWEEN NON ITERATIVE HASHES

	CHP MAC	JUNA MAC
Running time	8589934592 bit operation	52428800 bit operation
Compression rate	50.05%	3.91%
Resistant to birthday attack	No	Yes
Provably strongly collision-free	Yes	Yes

Where JUNA is based on a multivariate permutation problem (MPP) and an unusual subset product problem (ASPP) [40], [41], and There are two algorithms: an initialization and compression algorithm, change a message digest of nbits or a short message into an output series of mbits, where 80 ≤m ≤232 and 80 ≤m ≤n ≤4096, and moreover convinced that the security of the output versus existent collision attacks is to the O (2m) magnitude [40], [36]. Also, The Chaum–Heijst–Pfitzmann (CHP) hash function, a non-iterative one, is admirable. The discrete logarithm problem, is the basis of this method that Determined to be hardly collision-free. Considering the similar security conditions, a comparison between the two cases JUNA non-iterative hash and the Chaum–Heijst–Pfitzmann hash is done. (See Table1) [36].

TABLE. 3. CHOOSING THE MAC ALGORITHMS BASED ON TARGET SCENARIOS

Parallelizability required	Ciper implementation	Average data length $\|M\| \leq 2$	Average data length $\|M\| \geq 2$
No	Flexible	CMAC	Marvin
No	Inflexible	CMAC	CMAC
Yes	Flexible	PMAC1	Marvin
Yes	Inflexible	PMAC1	PMAC1

Where PMAC1, CMAC and Marvin are three cipher-based MAC algorithms analyzed in this document, a selection including all of the algorithms more commonly used in modern applications [39].

D: MAC selection for SSE

Timing delay, band width, hardware facilities, high reliability for secure data transferring are four main factors for MAC selection. The below algorithm (Fig. 3.) is suggested in this paper for optimized MAC selection to achieve appropriate SSE.

Tables 1, 2 and 3 are useful for weight allocation for pair-wise comparison matrix of MAC-based SSE algorithms. AHP algorithm for SSE MAC-based selection is shown in fig. 4.

So, far pair wise comparison matrixes of criteria and alternative, enough comparison of tables 1, 2 and 3 must be applied for below sample matrixes:

$$\text{CM}= \begin{array}{c} \\ TKS \\ RT \\ CF \\ BA \end{array} \begin{array}{c} \begin{array}{cccc} TKS & RT & CF & BA \end{array} \\ \begin{pmatrix} 1 & CM_{12} & CM_{13} & CM_{14} \\ CM_{21} & 1 & CM_{23} & CM_{24} \\ CM_{31} & CM_{32} & 1 & CM_{34} \\ CM_{41} & CM_{42} & CM_{43} & 1 \end{pmatrix} \end{array} \quad (5)$$

CM_{ij} Can be weighted according to specification of data communication system between 1-9

$$\text{AM}= \begin{array}{c} \\ PMAC \\ JUMA \\ CMAC \\ CHP\ MAC \end{array} \begin{array}{c} \begin{array}{cccc} PMAC & JUMA & CMAC & CHP\ MAC \end{array} \\ \begin{pmatrix} 1 & AM_{TKS_{12}} & AM_{TKS_{13}} & AM_{TKS_{14}} \\ AM_{TKS_{21}} & 1 & AM_{TKS_{23}} & AM_{TKS_{24}} \\ AM_{TKS_{31}} & AM_{TKS_{32}} & 1 & AM_{TKS_{34}} \\ AM_{TKS_{41}} & AM_{TKS_{42}} & AM_{43} & 1 \end{pmatrix} \end{array} \quad (6)$$

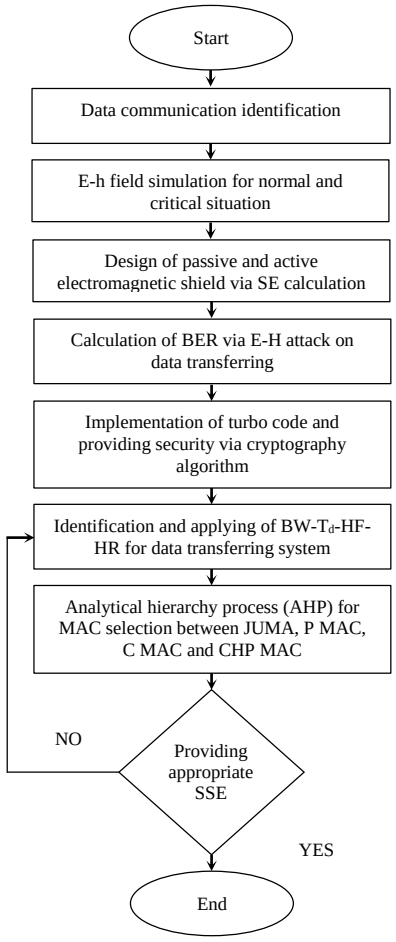

Fig. 3. Algorithm for selection of best MAC for SSE

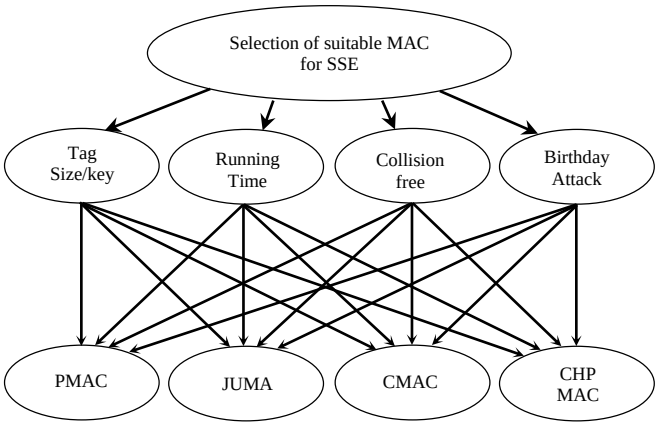

Fig. 4. AHP algorithm for SSE MAC-based selection

For weighting AMTKS and following matrixes AMRT, AMCF, AMBA, using of detailed information of tables 1, 2 and 3 should be done.

IV. CONCLUSION:

In this section, SSE is introduced via focusing on MAC-based hash function as main part of SSE approach. Survey of new MAC-based hash function of recent research, illustrates PMAC, CMAC, JUMA and CHP MAC are four applied MAC hash function for SSE in data transferring system. AHP algorithm is presented for choosing the best MAC-based hash function for SSE.

REFERENCES:

[1] L. Ren, J. Fan, "Modeling Electromagnetic Field Coupling Through Apertures for Radio-Frequency Interference Applications," IEEE Transactions on Electromagnetic Compatibility, vol. 57, no. 5, pp. 1037- 1048, 2015.

[2] Y. Xie, L. Liu, R. Li, X. Peng, "Security-aware Signal Packing Algorithm for CAN-based Automotive Cyber-physical Systems," IEEE CAA Journal Of Automatica Sinica, Vol. 2, No. 4, 2015

[3] H. Chan and A. Perrig, "Security and privacy in sensor networks," in Computer, vol. 36, no. 10, 2003, pp. 103–105.

[4] X. Yang, J. Lin, P. Moulema, W. Zhao, "A Novel En-route Filtering Scheme against False Data Injection Attacks in Cyber-Physical Networked Systems," IEEE Conf. Distributed Computing Systems (ICDCS), 2013.

[5] L. Hanzo, S. X. Ng, T. Keller, and W. T. Webb, "Quadrature Amplitude Modulation: From Basics to Adaptive Trellis-Coded, Turbo-Equalised and Space-Time Coded OFDM, CDMA and MC-CDMA Systems," 3rd ed. Wiley IEEE Press, 2004.

[6] Directed Energy Weapons, Report of the Defense Science Board Task Force, US Department of Defense, Office of the Under Secretary of Defense For Acquisition, Technology and Logistics, Washington, DC. (Jun. 2007). [Online]. Available: http://www.acq.osd.mil/dsb/reports/2007–12-Directed_Energy_Report.pdf.

[7] M. Backstrom, B. Nordstrom, and K. G. Lovstrand, "Is HPM a threat against the civil society?" in Proc. 27th General Assembly URSI, Maastricht, the Netherlands. (Aug. 2002). [Online]. Available: http://www.ursi.org/Proceedings/ProcGA02/papers/p0453.pdf

[8] W. Radasky, C. E. Baum, and M. W. Wik, "Introduction to the special issue on high-power electromagnetics (HPEM) and intentional electromagnetic interference (IEMI)," IEEE Transactions on Electromagnetic Compatibility, vol. 46, no. 3, pp. 314–321, Aug. 2004.

[9] D. V. Giri and F. M. Tesche, "Classification of intentional electromagnetic environments," IEEE Transactions on Electromagnetic Compatibility, vol. 46, No. 3, Aug. 2004.

[10] Electromagnetic compatibility (EMC)—Part 2: Environment—Section 13: High Power Electromagnetic (HPEM) Environments—Radiated and Conducted. Basic EMC Publication, IEC 61000-2–13.

[11] Electromagnetic Compatibility (EMC)—Part 4: Testing and Measurement Techniques—Section 35: HPEM Simulator Compendium, IEC 61000-4– 35.

[12] F. Sabath, "What can be learned from documented intentional electromagnetic interference (IEMI) attacks?" in Proc. General Assem. Sci. Symp., 2011 30th URSI. (Aug. 2011). [Online], Available: http://www.ursi.org/ proceedings/procGA11/ursi/E03-9.pdf

[13] E. Genender, H. Garbe, F. Sabath, C. Schuster, "Probabilistic Risk Analysis Technique of Intentional Electromagnetic Interference at System Level," IEEE Transactions on Electromagnetic Compatibility, Vol. 56, No. 1, 2014

[14] A. Vogt, H. Bruns, F. Gronwald, C. Schuster, " A Measurement Setup for Quantification of Electromagnetic Interference in Metallic Casings," IEEE Transactions on Electromagnetic Compatibility, Vol. 57, No. 6, 2015

[15] M. Rucinski, P. Musznicki, P. J. Chrzan, "Electromagnetic Interference Frequencies Prediction Model Of Flyback Converter for Snubber Design," IET the Institution of Engineering and Technology, Vol. 8, No. 6, 2015

[16] M. Aqeeli, T. Leng, X. Huang, Z. Hu, "Electromagnetic interference shielding based on highly flexible and conductive graphene laminate," IEEE Electronics Letters, Vol. 51, No. 17, 2015

[17] F. Faghihi and H. Heydari, "Time Domain Physical Optics For The Higher Order FDTD Modeling In Electromagnetic Scattering From 3-D Complex And Combined Multiple Materials Objects," Progress In Electromagnetics Research, Vol. 95, 2009.

[18] C. Bayliss, Transmission and Distribution Electrical Engineering, 2nd Edn., Newnes (2001).

[19] H. Heydari, F. Faghihi and M. Farhadi kashi, ‘‘Multi-layer magnetically

shielded room for high current injection system’’, Asian Power and Energy Systems, AsiaPES, 2007

[20] S. Caniggia, and F. Maradei, ‘‘Spice-like models for the analysis of the conducted and radiated immunity of shielded cables’’, IEEE Transactions on Electromagnetic Compatibility, Vol. 46, No. 4, 2004

[21] V. Abbasi, H. Heydari, F. Faghihi, “Heuristic mathematical formulations and comprehensive algorithm for optimal decision making for power system cabling SCIENTIA IRANICA Computer Science & Engineering and Electrical Engineering, Vol. 7, No. 3, 2010

[22] F. Faghihi, f. abbasian, H. zare, “Presentation of Hybrid Method of Hopfield Neural Network and Analytical Hierarchy Process to Achieve Optimal Routing Algorithm in the Presence of Interference Electromagnetic Fields in IT Based System," IRAN 9th International Industrial Engineering Conference, 2013

[23] M. P. Robinson, J. D. Turner, D. W. P. Thomas, J. F. Dawson, M. D. Ganley, A. C. Marvin, S. J. Porter, T. M. Benson, and C. Christopoulos, “Shielding effectiveness of a rectangular enclosure with a rectangular aperture,” Electron. Lett, vol. 32, no. 17, 1996.

[24] Q.-F. Liu, W.-Y. Yin, J.-F. Mao, and Z. Chen, “Accurate characterization of shielding effectiveness of metallic enclosures with thin wires and thin slots,” , IEEE Transactions on Electromagnetic Compatibility, vol. 51, no. 2, pp. 293–300, 2009.

[25] F. Faghihi., and H. Heydari, “Reduction of Leakage Magnetic Field in Electromagnetic Systems Based on Active Shielding Concept Verified by Eigenvalue Analysis,” Progress In Electromagnetics Research, Vol. 96, 2009

[26] F. Faghihi, H. Heydari, A. Falahati, Y. Attar, “Convolutional Codes Acting As EMI Virtual Shields in Current Injection System," Progress In Electromagnetics Research, Vol. 85, 2008.

[27] M. F. Brejz, L. Li, L. Hanzo, “20 Years of Turbo Coding and Energy Aware Design Guidelines for Energy-Constrained Wireless Applications,” IEEE Communications Surveys & Tutorials, Vol. 9, No. 3, 2015

[28] ETSI TS 136 212 LTE; Evolved Universal Terrestrial Radio Access (EUTRA); multiplexing and channel coding, V10.2.0 ed., 2011.

[29] IEEE Standard for Local and Metropolitan Area Networks. Part 16: Air Interface for Fixed Broadband Wireless Access Systems, IEEE 802.16-2004, IEEE Std., 2004.

[30] Special Publication 800-38B. Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication. National Institute of Standards and Technology, 2005

[31] M. Bellare, R. Canetti, H. Krawczyk, “Keying hash functions for message authentication,” BERLIN, Springer Koblitz N, ed. CRYPTO 96. LNCS 1109. 1996

[32] J. Black, S. Halevi, H. Krawczyk, “UMAC: Fast and secure message authentication,” BERLIN, Springer Wiener M J, ed. CRYPTO 99, LNCS 1666, 1999

[33] D. J. Bernstein, “The Poly1305-AES message-authentication code,” BERLIN, Springer FSE 05, LNCS 3557, 2005

[34] ISO 8731-2. Banking—Approved Algorithms for Message Authentication—Part 2: Message Authenticator Algorithm. Second Edition [Replaced by: ISO 16609 2004

[35] Z. L. Ting, W. W. Ling, Z. Lei, W. Peng, “CBCR: CBC MAC with rotating transformations,” SCIENCE CHINA Information Sciences, Vol. 2, No. 3, 2011

[36] S. Su, T. Xie, S. Lu “A provably secure non-iterative hash function resisting birthday attack,” ELSEVIER, Journal of Theoretical Computer Science, Vol. 654, No. 4, 2016

[37] E. Petrank, C. Rackoff, “CBC MAC for Real-Time Data Sources,” Journal of CRYPTOLOGY, Vol. 2, No. 4, 2000

[38] C. Cheng, T. Jiang, Q. Zhang, “Tesla-Based Homomorphic MAC for Authentication in P2P System for Live Streaming with Network Coding,” IEEE Journal on Selected Areas in Communications, Vol. 31, No. 9, 2013

[39] M. A. Simplicio, B. T. Oliveira, C. B. Margi, P. S. Barreto, “Survey and comparison of message authentication solutions on wireless sensor networks,” ELSEVIER Ad Hoc Networks, Vol. 11, No. 3, 2013

[40] S. Su, S. Lu, “A public key cryptosystem based on three new provable problems,” ELSEVIER, Journal of Theoretical Computer Science, Vol. 5, No. 7, 2012

[41] S. Su, S. Lu, X. Fan “Asymptotic granularity reduction and its application,” ELSEVIER, Journal of Theoretical Computer Science, Vol. 2, No. 4, 2011