I. J. Computer Network and Information Security, 2016, 7, 17-22
Published Online July 2016 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2016.07.03

Spam Reduction by using E-mail History and Authentication (SREHA)

Adwan F. Yasin
Faculty of Engineering and Information Technology Arab American University – Jenin, Palestine
E-mail: adwan.yasin@aauj.edu

Abstract—Spam messages are today one of the most serious threats to users of E-mail messages. There are several ways to prevent and detect spam message, the most important way is filtering spam. Sometimes Filtering fails to discover some spam messages or even fails in the classification of non-spam messages as a spam messages. In this paper, we suggest a new effective method that reduces the spam messages by integrating prevention and detection techniques in one scheme. The reduction achieved by considering history and user authentication. This method based on issuing a certificate to each reliable user during the process of Email account Creation. The certificate used by Email servers to discard or forward ingoing or outgoing Emails. Each Server has to maintain white, gray and blacklist according to Email classification spam or ham, which determined by the user or by the contents examination of the message in terms of empty or contained only links without any text or by searching for a specific keywords in the subject and in the content. We believe that there are no bad or good E–mails forever, so the proposed model dynamically allows the transition of E-mail from one state to another state based on the number of received spam and ham messages.

Index Terms—Authentication, Certification, Whitelist, Graylist, Blacklist, Spam, and Ham.

I. Introduction

Nowadays, emails became the fastest and the cheapest way that used by persons and companies for information exchange, email messages and electronic commerce. The main problem that faces email messages is unsolicited email which known as spam that arrive to users without knowing them. Spams are the undesirable Emails, which overflow the internet with considerable copies of the same message. Sometimes spam carries malicious content that harms our system and reduces the performance [1]. The number of internet users growing very fast and the emails are becoming one of the most popular means of communications. The SMTP designed for trusted word so it can be used to send spam messages.

The spam considered one of the most serious problem that faces email exchange systems, as it is money squandering, waste of time and computing system resources in addition to spreading viruses. The person who sends spam message called the spammer and his aims may be commercial, trick, religion, sexual, and advertising due to cheaper prices, or hacking purposes in order to destroy or hurt any device by spreading viruses.

According to Kaspersky Lab statistics bulletin during the first quarter of 2014 about 66.34% of total email traffic was spam [2].

According to University of California Irvine statistical [3] the total number of blocked messages reached 690,849,027.

The number of spam messages may increase or decreased according to political, economical and sport events, for example, in mid-2003 about 83% of the email message received by Microsoft Hotmail were spams [4]. According to the Message Anti-Abuse Working Group, the amount of spam email was between 88–92% of email messages sent in the first half of 2010 [5].

There are many anti spam techniques that use the principle of filtering, which is the most famous method in the world. Unfortunately, filtering fails in detecting all spam and as a result some legitimate emails blocked.

The basic concept of spam filter illustrated in figure 1.

Nowadays there are many email spam filtering tools exists in the world, but due to the existence of spammers and adoption of new techniques, email spam filtering becomes a challenging problem to the researchers by rising the needs to integrate more than one anti spam techniques to overcome this problem.

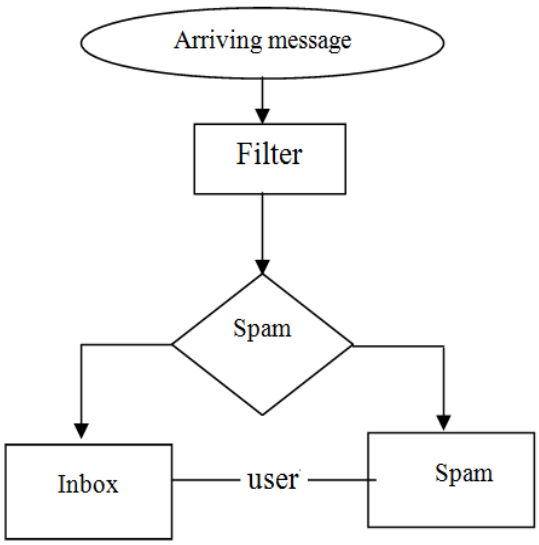

Fig.1. Block Diagram of Spam Filter.

The rest of the paper organized as follows:

Section II: Discussion of related works.
Section III: Description of suggested Technique
Section IV: Conclusion.
Section V: Future work.

II. Related Works

There are many techniques currently used to detect the spam messages. The most important technique is spam filtering which removes a lot of spam, but this technique still faces the problem of preventing non-spam message and blocks legitimate users.

One of the most important filtering techniques is "Bayesian Filter" [6] that uses the probabilities approach where the divide message for token, then calculate the probability for each token that came in spam list and non-spam list. Finally, it calculates percent of whole probability to decide if the email message is spam or non-spam. Another way to prevent spam is IP blacklist which is the oldest method of anti spam that prevents spam messages depending on the IP address [7].

Cash architecture technique [8] contains two lists. The first is blacklist that contains unsolicited email that considered as spam. The second whitelist that contains solicited emails that considered as non-spam (ham). The concept of Cash Architecture illustrated in figure 2.

Another way to detect spammer is SNARE which depends on studies features for distinctive spammers from legitimate email senders that are depends on the network-level, spatio-temporal behavior of email sending patterns, rather than the email's content [9].

A number of techniques benefit of clustering as a part of their spam detection approach like: clustering followed by KNN classification [10], [11] and clustering followed by SVM classification [12]. In [13], Jung and Sit check the use of DNS blacklists for address-based filtering of spams.

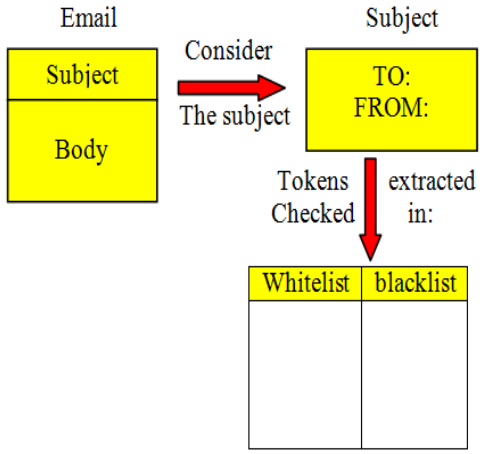

Fig.2. Block Diagram of Cache Architecture.

There are some advantages and disadvantages of whitelists and blacklists. The advantages for blacklists are easy to manage, easy to install and can download update quickly while the advantages for whitelists are minimize false positives, can be created at global, administrative or individual user level, more secure, more accurate, and easy to customize.

The disadvantages for blacklists are exponential growth chews up resources, creates false positives and denies legitimate senders, updates are futile, as spammers constantly change identities and hard to switch from a default blacklist to a whitelists model. While the disadvantages for whitelists are taking longer to install and requires more time to manage.

Other techniques based tend to delay the spam by organizing the messages into two queues, suspicious messages directed to the lowest priority queue and hams in the highest priority one [14][15]

ZhangYing et al [16] discuss the application of feedback judgment of Bayesian algorithm in anti-spam system by using genetic algorithm.

Xin Liu. Et al [17] proposed a spam filtering approach in which a collaborative and personalized spam filter based on social networks. This approach reflects the collaboration and personalization the of users with similar interest. By enabling them to push spam reports to their social network.

Most spam fighting approaches are content or behavior based techniques and they intended to detect the spam messages. The proposed work integrates prevention and detection techniques in order to prevent the spreading of spam messages.

III. Description of the Proposed Model (SREHA)

The proposed SREHA integrates prevention and detection approaches in order to reduce spam, where the prevention approach based on verification of the identity of the user and creating a digitally signed certificate by Email server. The detection approach is flexible and uses very simple filtering rules that reduce the filtering time.

A User Verification

At the beginning, the approach aims to prevent the creating of fake email accounts without the knowledge of their real owners and these emails can be used to send spam email messages.

Our proposed approach will reduce the spam email messages by verifying and issuing a certificate for each new created Email.

During the creating of the new email account, it is required to fill in personal information from the user side, and the mobile phone number should be included in this information. Then the site sends a text message to the phone user that contains a verification code (VC) and request from the user to enter the verification code in order to complete the registration process on the web site and complete creating the email account.

Verification code, here is should be a large number and not less than 128 bits. The user then should send this code to the Email server via a secure communication channel. At the next stage the server will verifies and confirms the authenticity of the sender verification code

and completes the registration process by issuing a certificate that contains VC and personal info, this certificate will be used in the following E-Mails exchange.

Creating a certified E-Mail account using verification code illustrated in figure 3. The proposed model uses asymmetric encryption system that is more convenient for digital signature than other systems and there are no problems in sharing the keys. In order to a digitally signs user information and creates user certificate the server uses its private key while the public key is known to the others and used for decryption purposes The user certificate contains many information that used for authentication and verification purposes but mainly the verification code and personal information will be extracted and checked. When the user sends an email message to another user account, the server will sends the message along with the user certificate to the receiving party.

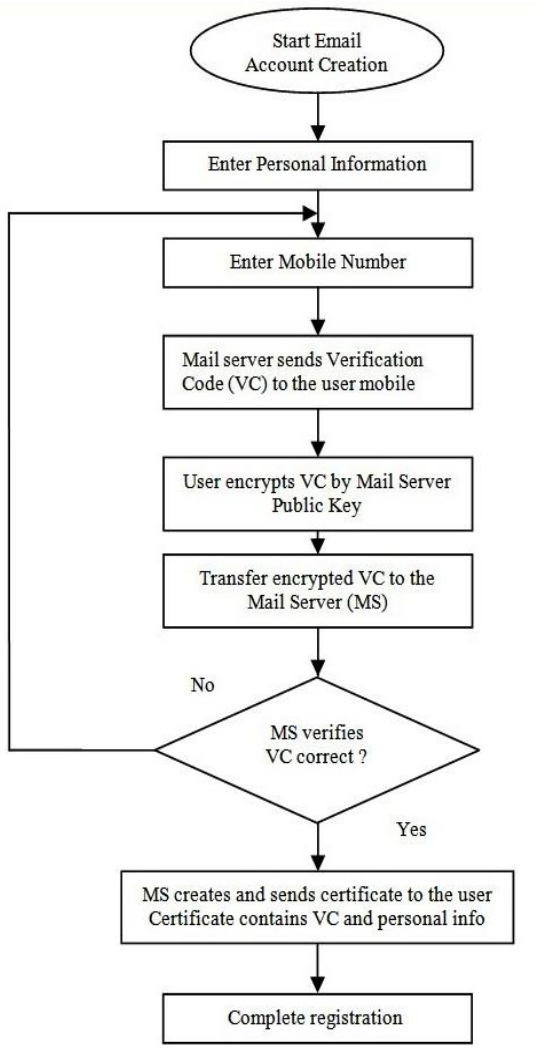

Fig.3. Creation Certified Email Account

The destination server uses the sender's public key to decrypt the certificate and extracts the verification code and personal information of the sending user. This process is shown in algorithm 1.

In this way the message exchange between users will be more reliable and it is an effective approach to reduce the annoying spam messages.

1. *User gets certificate (Ucer).*
2. *User sends the email to another user account.*
3. *Sending server append User with email messages.*
4. *Destination Server (DS) fetches the Ucer from the received message.*
5. *DS decrypt the certificate by using the public key of sending server.*
6. *DS gets VC and personal info.*
7. *DS verify and confirm certificate info.*
8. *If verification passed Start Filtering Process.*
9. *Else Discard this email and inform sending server*

Algorithm 1. Certificate Verification

Sometimes, the email accounts hacked and become accessible to unauthorized parties that use it to spread viruses or sending a lot of unsolicited messages without the knowledge of email account owner. Applying the proposed technique efficiently used to detect and stop unauthorized activities at an early stage. The system will automatically send to the user an alert and new verification code and the old one revoked. The user has to start updating his account password and getting new certificate which includes the new verification code. The account will be unable to send emails until the owner of the account completes the updating process.

The next stages are message classification and filtering.

B. Email classification

In addition to authentication the proposed model uses the content base filtering technique in order to reduce spams. The following rules have been considered to classify the message:

The message is a spam

If its content is empty, some spammers use this empty message to confirm that this address is active and the user may replay.

If its content contains only link.

If it Contains Spams keywords.

The format of the keywords list illustrated in table 1. The keywords categorized into three groups, high, medium and low degree and every category assigned predefined weight. The words of high degree are considered spams and strongly affect the classification decision, the words with medium degrees have medium effect and the words with lowest degree have the least effect on the email classification. In order to build the list of spams keywords the server has to trained and test many samples of hams and spam messages.

The proposed scheme allows the users to contribute in spams keywords decision making as their interests are not identical and may be changed along the time. Building the spams keywords table is a result of client and server

collaboration so the server dynamically updates its tables according to gained experience over the time and by using the feedbacks obtained from the users.

The criteria that should be adopted to classify the email according to the proposed list structure is to consider the sum of weights of all existed spam keywords and by considering the occurrence number of each keyword category. The threshold(Tr) that shouldn't be overreached determined by the spam fighting policy adopted by mail server administration.

To compute the total weight (Tw) we suggest the following formula:

$$Tw= \sum_{i=1}^{k} Wh+\sum_{i=1}^{n} Wm+\sum_{i=1}^{h} Wl \quad (1)$$

Where: k, n, h - the number of high, medium and low degree words respectively.

Wh,Wm,Wl – the weights of high, medium and low degree words respectively.

The classification decision depends on the follows constraint:

$$Tr \geq 6 \quad (2)$$

$$Tw \leq Tr \quad (3)$$

We suggest that Tr should be multiple of 6 in order to achieve integer numbers of k, n and h.

From (3) it is obvious that the proposed scheme can be easily scaled to meet the different security requirements. The Tr should be carefully selected to exclude false positive alerts.

Table 1. List of Spams Keywords

Keyword	Degree	Weight
Murder	H	6
Bomb	H	6
Wheel	M	3
Car	M	3
Tree	L	1

Our approach considers the constraint (3) for hams or spams classification and depending on the sent spams and hams number the user account can be in white, gray or black list. The proposed model allows the account transmission from one state to another, and this reflects the real life in which there is a good account that can be used to deliver spams in inadvertent manner, so it is necessary to give them a chance to change their status as shown in Figure 4. The account that is in the whitelist(WL) are the most trusted and the blacklist(BL) accounts have the least trust so they are blocked from sending messages for a period of time determined by the mail server administrator of the host server. The recipient mail server blocks all incoming blacklisted email until it obtains a new certificate of the blocked account and this leads to changing the account state from black to gray state. The accounts in the graylist (GL) are in the transition state and they should be carefully monitored and handled.

Initially, all certified email accounts are trusted and have the WL state. The status of the accounts changed according the number of sent spams and hams, if email address exist in graylist after a certain number of spams messages the state changes to BL state but if it sends many hams the state changes to WL. On the other hand, any user in the blacklist state who gets a new certificate and begins to send ham messages after a certain number will be transferred to the GL state. See figure 4.

The mail server only maintains the accounts that send more than one spam in order to reduce the size of the state account table. See table 2. Each record of this consists of Email account, Valid Certificate, Spam Number (SN), Ham Number(HN) and Email State which is dynamically changed according to the type of sent or received messages.

In order to exclude the false positive and false negative the proposed approach enable the user to classify a specific massage as spam or ham and this will be considered by the Email server during the email state transition process.

Table 2. Contents of Accounts Table

E-mail account	Certifi-cate	SN	HN	Email State
mickl19@yahoo.com	Cer.1	3	5	GL
jonral45@live.com	Cer.2	6	1	BL
rawan78@gmail.com	Cer.3	2	17	WL
George3@yahoo.com	Cert?	10	3	BL
Alice1@gmail.com	Cert?, Cert2	20	6	Blocked

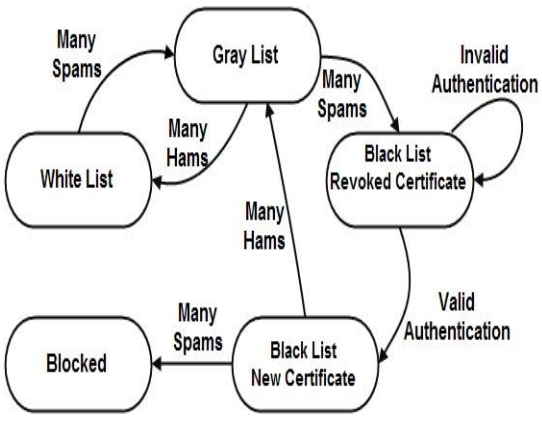

Fig.4. E-mail Transition State Diagram

C. Updating Account State.

Initially, the states of all accounts are WL and the Spams Number (SN) and Hams Number (HN) for each account reset to zero, the administrator sets the SN and HN thresholds SNT, HNT respectively as follows:

$$HNT=F*SNT \quad (4)$$

Where: F– Forgiveness factor which depends on the protection level and the number of transitions from the worse to the better state (Backward Transitions).

In order to update the accounts state the mail server uses the following algorithm 2:

```
For Each Account
Initialize F, SNT
If certificate is valid
{
  For each inbound or outbound email
  R=Result Of Message Classification;
  If  (R= Spam) SN=SN+1;
  Else    HN=HN+1;
HNT=F*SNT;
   If (State==WL)&& (SN >SNT)
      {
         State=GL;
        SN=HN=0;
       }
  Else if (State===GL) &&(SN>SNT)
       {
         State=BL;
          SN=HN=0;
         Block Account;
         Revoke Certificate;
         If (account local) request certificate update
           Else Inform Remote Mail Server;
         }
 If (State== GL) &&(HN>HNT)
      {
         State=WL;
         SN=HN=0;
          F=F+1;
       }
Else If (State== BL) &&(HN>HNT)
    {
    State=GL;
    SN=HN=0;
    F=F+2;
    }
} else Account Blocked;
```

Algorithm 2. Updating Account State.

The proposed algorithm saves the forgiveness factor F and increase it every transition from the worse to the better state in order to complicate the backward transition, which is an effective deterrence strategy.

D. Message Content Filtering

The proposed Model employs a set of rules to classify the message as spam or ham according to its content. The process of filtering starts by removing any inserted symbols between characters as many spammers use these techniques to change the spelling of the keywords to prevent spam detection for example the word BOMB may be written B-OM-B or BO*M*B. The following Algorithm describes the Process of Content Filtering.

```
Initialize
Tw=h=k,n=0
For each inbound or outbound email
Remove Inserted Symbols;
Scan the subject and content
For each found Spam keyword (FSW)
{
If  (FSW== High Degree)
      K=K+1;
   Else if (FSW==Medium Degree)
            N=N+1;
          Else  H=H+1;
}
Tw= K*Wh+N*Wm+H*Wl;
 If (Tw>=Tr)
Classification Result= Spam;
    Else Classification Result= Ham;
```

Algorithm 3. Content Filtering.

The proposed Approach doesn't detect all spam messages for the first time, as the spammer may replace some letters of keywords, for Example the keyword Chair may be written in other forms like Ch@ir or Cha!r, nevertheless these keywords well be detected in the next time. The proposed approach very flexible as it allows the user to add or delete spam keyword and consequently the gained knowledge will propagate to all mail system components.

The proposed model considered the sharing of spams information in order to build and maintain distributed or centralized database that can be used to recognize spams. Spam prevention is the responsibility of all mail servers so the collaboration between them has a crucial role in the spam reduction. It is very important to set well defined criteria that should be adopted by all E-mail servers to determine the spammers and to fight against them. Global and local policies should be adopted to rule and control the information flow between servers, and this is very important as it is not necessary that the definition of the spams in all servers identical, although there are many common factors. To maintain the privacy of each server and to reduce the traffic load each spam should has local and global attributes and the mail servers only share the information of the spams that match the global attributes. Collaborative fighting against spams and spammers is a very efficient method as it is employs the outputs of many filtering techniques to recognize the spam Emails.

Table 3. Notations Description.

Notation	Description
VC	Verification Code
MS	Mail Server
WL	White List
BL	Black List
GL	Gray List
Tr	Threshold of the
Tw	Total weight of the spams world
SN	Spams Number
HN	Hams number
Wx	Weight of the spam words of x degree
SNT	Spams Number Threshold
HNT	Hams Number Threshold
F	Forgiveness Factor
R	Classification Result
Cer	Certificate
Cer?	Revoked Certificate

IV. Conclusion

In this paper proposed a new model SREHA that reduces and confines spam spreading. In order to achieve the highest degree of spam reduction SREHA integrates two level of protection. The first level is a prevention technique, which is an authentication and verification code based approach, the second level based on a simple and efficient content filtering method. SREHA is an adaptive and flexible model that meets different security requirements. The clients in addition to the mail server can update and share the gained knowledge with the others. We believe that not all users who generate spam are spammers as many hacked accounts used to send spam emails. SREHA considers these cases and gives these users the ability to use their emails normally. Proposed model allowed and enabled each E-mail server to disseminate gained information about the spams and the spammers in order to share these information with other servers that enable them to timely respond and act against spammers.

V. Future Work

So far, there is no way to prevent spam messages completely. The proposed approach can detect and prevent a lot of spam text messages. On the other hand SREHA does not detect spam messages that contain images. In the future, it will be possible to extend this approach in order to detect these types of spam messages.

References

[1] Toshihiro Tabata, "Spam Mail Filtering: commentary of Bayesian filter," The journal of Information Science and Technology Association, Vol.56, No.10, pp.464-468, 2006.

[2] http://securelist.com/analysis/monthly-spam-reports/64869/, spam-in-june-2014/

[3] UC Irvine Spam Statistics. (2013). http://www.oit.uci.edu/email/spam/stats/

[4] Guido Schryen. "Fighting Spam: Motivating an Account Based Proceedings of the IADIS International Conference WWW/Internet 2004, Madrid, Spain, 2 Volumes; 01/2004.

[5] http://en.wikipedia.org/wiki/Email_spam

[6] Bayesian filter. P. Graham, A Plan for Spam, http://paulgraham.com/better.html

[7] J.M.Gomez Hidalgo and M. Mana Lopez. Combining text and heuristics for cost-sensitive spam filtering. In Proceedings of the 4th Computational Natural Language Learning Workshop, pages 99-102, Lisbon, Portugal, 2000.

[8] Sahil Puri1, Dishant Gosain2, Mehak Ahuja3, Ishita Kathuria4, Nishtha Jatana5. "Comparison and Analysis of Spam Detection Algorithm". 1,2,3, India. ISSN 2319 – 4847. Volume 2, Issue 4, April 2013.

[9] Nadeem A.S, Shuang H, Nick F, Alexander G. Gray, Sven K. "Detecting Spammers with SNARE: Spatio-temporal Network-level Automatic Reputation Engine". College of Computing Tech. Georgia.

[10] Firte, L., Lemnaru, C. and Potolea, R. 2010. ―Spam Detection Filter Using KNN Algorithm and Resampling,‖ in Intelligent Computer Communication and Processing (ICCP), 2010 IEEE International Conference, pp. 27 – 33.

[11] Rasim M. A lgulie v, Ramiz M. Aliguliye v, a nd Saadat A. Na zirova. Classification of Textual E-mail Spam Using Data Mining Techniques. Applied Computational Intelligence and Soft Computing, vol. 2011, Article ID 416308, 8 pages.

[12] Antonia Kyriakopoulou and Theodore Kalamboukis, "Text Classification Using Clustering" in ECML-PKDD Discovery Challenge Workshop Proceedings. 2006.

[13] J. Jung and E. Sit, "An Empirical Study of Spam Traffic and the Use of DNS Black Lists", in the proceeding of ACM IMC' 04, Oct. 2004.

[14] Li, K., Pu, C. and Ahamad, M., "Resisting spam delivery by TCP damping," Proceedings of the First Conference on Email and Anti-Spam, CEAS'2004.

[15] Saito, T., "Anti-spam system: Another way of preventing Spam," Proceedings of the 16th International Workshop on Database and Expert Systems Applications, DEXA 2005, pp. 57–61, 2005.

[16] ZhangYing, YangXi, Liu Yanqiu "Improvement and Optimization of Spam Text Filtering System" 2nd International Conference on Computer Science and Network Technology, p 448-451, 2012 IEEE, China.

[17] Xin Liu, Zhaojun Xin, Leyi Shi, Yao Wang," A Decentralized and Personalized Spam Filter Based on Social Computing" pp.887-894, Aug 2014, IEEE, Nicosia.

Authors' Profiles

Adwan Yasin is an associate Professor, Former Dean of Faculty of Engineering and Information Technology of the Arab American University of Jenin, Palestine. Previously, he worked in Philadelphia and Zarka Private Universities, Jordan. He received his PhD degree from the National Technical University of Ukraine in 1996. His research interests include Computer Networks, Computer Architecture, Cryptography and Networks Security.

How to cite this paper: Adwan F. Yasin,"Spam Reduction by using E-mail History and Authentication (SREHA)", International Journal of Computer Network and Information Security(IJCNIS), Vol.8, No.7, pp.17-22, 2016.DOI: 10.5815/ijcnis.2016.07.03

