A Fast Fourier Transform-based ECG Security Framework

Jusak Jusak
Dept. of Computer Engineering
Institut Bisnis dan Informatika Stikom Surabaya
Raya Kedung Baruk 98, Surabaya 60298, East Java, Indonesia
jusak@stikom.edu

Roy Laurens
Department of Computer Science
University of Central Florida
Orlando, FL, USA
rlaurens@knights.ucf.edu
czou@cs.ucf.edu

Seedahmed S. Mahmoud
Dept. of Eletronics and Electrical Technology
Technical Trainers College (Lincoln College – UK)
Riyadh, Kingdom of Saudi Arabic
seedahmed.sharif@gmail.com

***Abstract*—An electrocardiogram (ECG) signal inherits private information about a particular patient. Therefore in the current online healthcare platform, a secure transmission and storage in the public repository is imperative. Furthermore, a limited power devices for recording and transmitting ECG signal requires low computation algorithm to anonymize the signal. To deal with this specific requirement, in this paper, we propose a fast Fourier transform (FFT) – based ECG anonymization approach to secure the transmission of the ECG signal. Performance evaluation over processing time showed that the proposed algorithm inherited lower processing time compared to the recently proposed wavelet packet-based algorithm. Additionally, processing time of the proposed framework remains the same for several variations of the secret key length. Therefore, the proposed framework offers flexibility for the application to choose the length of secret key in the ECG anonymization phase.**

Keywords—ecg signal, fast fourier transform, anonymization, security.

I. INTRODUCTION

Based on the latest data released by the World Health Organization (WHO) in 2014, deaths caused by cardiovascular disease in 2012 have reached 17.5 million, or 46% of the total number of non-communicable diseases deaths in the world and 37% of the total number of deaths in Indonesia [1]. Furthermore, in another WHO report states that in 2020, it is estimated that the coronary heart disease will be the major killer diseases in countries throughout Asia-Pacific [2]. With such a rising threat of cardiovascular disease (CVD), real-time and mobile ECG monitoring will be one of the most prominent applications in the future.

ECG signal contains important health information of a patient. Therefore, ECG signal was found to be unique for each individual over a long period of time [3] [4]. Furthermore, ECG signal can act as a biometric identity to distinguish specific information that belongs to a particular person [5]. This feature brings direct consequence to ECG signal transmission from sensor nodes to health care providers via public networks that make it vulnerable to spoof attack. Hence, an Internet-based e-Health platform [6,7] that ignores protection of private health information is a threat to patients' privacy. Unfortunately, none of the existing e-Health platforms implement any obfuscation or anonymization techniques to protect the transmission of the ECG signal.

An unsecure ECG signal can be subjected to *man in the middle* attack where fraudsters can use the spoofed recorded ECG data to gain access to a secured service [8] [9]. A scenario where a man in the middle attack can be a real threat for health information transmission is presented in Fig. 1. The figure illustrates possible attack points that are including: (i) wireless link between sensor nodes that collects health information data from wireless body area networks (WBAN) and gateway, (ii) wire/wireless link between gateway and the edge router, (iii) wire/wireless link between the other side of the edge router and health care provider router, and (iv) repository in the data center/public server or health care provider. When a malicious actor launches a man in the middle attack and gains access to the system, for example stealing data from data center, it can sell the health information to the wrong person or organization. In order to minimize such security threat to a system, a health care provider needs to comply with certain widely accepted standards to protect medical records safely. For example, US Government passed the Health Insurance Portability and Accountability Act (HIPAA) in 1996 for protecting medical privacy users [10], the European Union adopted the Directive on Data Protection in 1995 [11], the Health Information Privacy Code passed by New Zealand Government in 1994 which sets specific rules for agencies in the health sector to ensure protection of individual privacy [12], and the Personally Controlled Electronic Health Record (PCEHR) eHealth system launched by Australian Government in 2012 [13].

Several studies have been proposed to secure ECG signal by way of anonymization. For example in [8], a wavelet packet-based ECG anonymization method was proposed to decompose the ECG signal, replaced the coefficients of the low frequency node with zeros and reconstruct the ECG signal for anonymization. However, using this method the anonymized ECG signal did not fully conceal the fiducial features since the RR interval (related to heart rate variability, HRV) was present. Furthermore, the size of the anonymized signal was similar to the size of the original ECG signal.

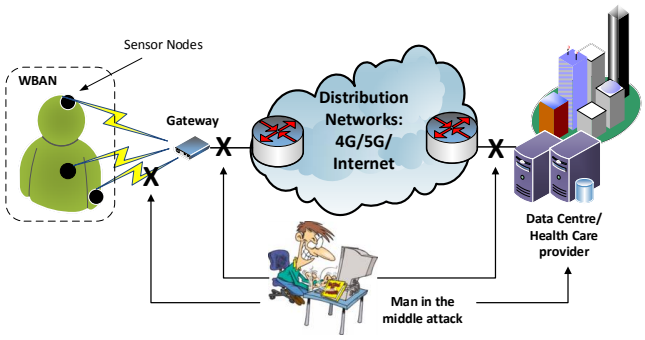

Fig. 1. Possible attack points for unsecure ECG signals subjected to man in the middle attack.

To increase the performance of the previous algorithm, subsequently a generalized wavelet packet method was proposed by the same author. The proposed algorithm was equipped with a reversible function and/or operation to conceal fiducial and non-fiducial features from normal and abnormal ECG signals. At the receiver end, only an authorized personnel who has a secret key and knows the reversible function will be able to reconstruct the original ECG from the anonymized ECG [14]. The paper showed that the reconstructed ECG was highly correlated with the original ECG, which achieved a lossless reconstruction of the ECG data and proved the robustness of the proposed method. It was also found from the performance analysis results that the proposed anonymization scheme provides high-security protection to ECG data and patient privacy.

In this paper, a novel low processing time ECG anonymization method based on the fast Fourier transform (FFT) algorithm is proposed. In contrast to the previous method [14], the FFT based ECG anonymization technique aims to achieve a lower processing time security algorithm for obfuscating the ECG signal. Hence, major modifications of the existing algorithm had been done thoroughly, including: (i) replacement of wavelet packet algorithm (that transforms time domain into time-frequency domain) with FFT algorithm (that transforms time domain into frequency domain only), (ii) major modifications of anonymization method following FFT algorithm features, and (iii) modification of reversible function in eq. 6.

II. A Proposed ECG Security Framework

A. An ECG Anonymization approach

The proposed ECG security system comprises of the following three main processes, i.e. ECG signal transformation, frequency domain component partition and ECG anonymization that involves several sub-processes. Fig 2. describes the ECG anonymization process and Algorithm 1 depicts a pseudocode of the proposed method, while the step by step process of anonymizing the ECG signal sequence is elaborated as follows:

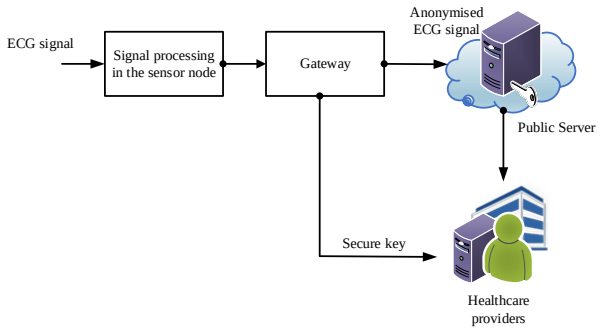

Fig. 2. The proposed ECG anonymization method

Step 1. Firstly, transformation process is accomplished by applying Discrete Fourier Transform (DFT) to the ECG signal sequence $\{x[n]: n = 0 \cdots N-1\}$ to produce frequency domain signal that is represented by $\{X[k]: k = 0 \cdots N-1\}$, where N is the length of the ECG signal sequence. The DFT of a finite-length ECG sequence of length N is defined as

$$X[k] = \sum_{n=0}^{N-1} x[n] e^{-j\left(\frac{2\pi kn}{N}\right)}, \qquad k = 0,1,\cdots,N-1. \tag{1}$$

On the other hand, the inverse DFT is given by

$$x[n] = \frac{1}{N} \sum_{k=0}^{N-1} X[k] e^{j\left(\frac{2\pi kn}{N}\right)}, \qquad n = 0,1,\cdots,N-1. \tag{2}$$

A FFT algorithm is employed to compute the Discrete Fourier Transform (DFT) of an input ECG sequence, $x[n]$. Compared to other methods in calculating the DFT, the FFT produces incredibly more efficient and substantially low computational load algorithm. Hence, the FFT is suitable for signal processing in low power devices such as those in sensor nodes. Furthermore, in the proposed method, the variable N is strictly confined to any positive power of two integer, for example 128, 256, 512, 1024, etc. There are two reasons for choosing this number for N. Firstly, it is a natural way to keep the power of two signal length in the digital storage as in the sensor nodes. Secondly, it is a basic requirement for the FFT algorithm to calculate the DFT efficiently. By choosing the length of the ECG signal sequence as a power of two integer, we expect to achieve a fast, near real-time and efficient signal processing for the ECG signal.

Step 2. The process of FFT transformation is then followed by frequency domain partitioning. It should be noted that the frequency domain partitioning is the most crucial phase in our proposed ECG anonymization framework, where in this phase the frequency domain signal, $X[k]$ is separated into two sub-bands, i.e., $X_1[k]$ and $X_2[k]$. The first segment, $X_1[k]$ signifies low frequency components of the transformed signal, while the second sub-band, $X_2[k]$ represents high frequency components as shown in Eq. 3.

$$X[k] \equiv \left\{ \underbrace{X_1[0 \cdots P]}_{\substack{low\ freq. \\ component}}, \underbrace{X_2[(P+1) \cdots Q]}_{\substack{high\ freq. \\ component}} \right\} \quad (3)$$

where P is the expected secret key length and $Q = N - 1$.

The length of Q in the proposed method consider the following assumptions:

- The length of $X[k]$, i.e. Q in Eq. 3 should be selected carefully to ensure that the ECG signal samples contain high frequency components up to 250Hz. This assumption will guarantee that all the important features extracted from the ECG signal such as QRS complex, P wave and T wave remain intact in the signal [24,25].
- The parameters Q and P are suggested to follow relation in Eq. 4 as

$$0 \equiv Q(\mathrm{mod}\ P). \quad (4)$$

  where $\mathrm{mod}()$ is modulus operation. Applying Eq. 4 in the algorithm will guarantee that Q is always positive natural number multiplication of P. The reason of this suggestion will be explained in *Step 4*.
- Furthermore, selection of the Q length should also consider algorithm efficiency in the reconstruction process of the ECG signal. Therefore, based on the similar reasons in *Step 1*, the length of Q should be set to any positive power of two integer.

Step 3. Exclude $X_1[k]$ from $X[k]$ in Eq. 3 to get an unencrypted and uncompressed key, κ, that contains the lowest frequency components of the ECG signal. The key is defined as

$$\kappa[k] = \{X_1[k] : k = 0, \cdots, P\}, \quad (5)$$

where P is the desired secret key length. Removing $X_1[k]$ from $X[k]$ leaves $X_2[k]$ that holds important information about the ECG signal.

Step 4. Modify $X_2[k]$ component using a certain reversible function. In this work we multiply the $X_2[k]$ component and α in order to maintain the low complexity characteristics of the algorithm. The modified $X_2[k]$ component can be written as follows

$$\overline{X_2}[k] = \{X_2[k] * \Omega : k = P+1, \cdots, Q\}. \quad (6)$$

It should be noted that multiplication of $X_2[k]$ component and vector $\Omega[k]$ is an element-wise multiplication, where vector $\Omega[k]$ is defined according to the following:

$$\Omega[k] = \{\kappa[k] + \mathrm{offset} : k = 0, \cdots, P\}, \quad (7)$$

with $\mathrm{offset} = |\min(\kappa)| + \eta$. The parameter η is a constant value to prevent division by zero in the ECG reconstruction process, while the $|.|$ is an absolute operator. Looking closely at Eq. 6, it should be clear that element-wise multiplication vector $X_2[k]$ by vector $\Omega[k]$ requires both of them to have the same size, for example the vector $\Omega[k]$ might need to be repeated until it reaches the same size as $X_2[k]$. Hence, applying Eq, (4) in Eq. (5) in *Step 2* will ensure that vector $X_2[k]$ and $\Omega[k]$ have same size.

Step 5. Create the key security K and securely distributed the key to authorized healthcare providers. The key security can be accomplished by compressing and encrypting the key, $\kappa[k]$, in Eq. 5 together with the $\Omega[k]$ in Eq. 7 according to the following equation

$$K = E(\Delta(\kappa, \Omega)), \quad (8)$$

where the operator Δ represents a compression operation and the operator E denotes an encryption operation.

Nevertheless, the compression and encryption algorithms will not be discussed further in this paper. In order to maintain system low complexity feature, we suggest to employ industrial standard for efficient compression and encryption that are available in the market. For example, wireless transmission using Bluetooth Low energy (BLE) technology has integrated 128-bit AES encryption in the Bluetooth Core Specification version 4.0 and Wi-Fi Protected Access (WPA) security protocols that are currently used extensively for the Wireless LAN networks that based on the IEEE 802.11i standard.

Step 6. Reconstruct the modified $\overline{X_2}[k]$ utilizing the inverse FFT algorithm to obtain time domain representation, $\overline{x_2}[n]$. The $\overline{x_2}[n]$ is the anonymized ECG signal that encloses part of the original ECG signal. Upload the $\overline{x_2}[n]$ to a secure public server, e.g., cloud server as a healthcare data repository.

B. An ECG Reconstruction approach

In order to retrieve the designated ECG signal, an authorized medical personnel in the healthcare provider requires to perform ECG reconstruction process based on the information which consists of the secure key, K, and the anonymized ECG signal, $\overline{x_2}(n)$. The proposed ECG reconstruction method is elaborated in the following steps and is illustrated in Algorithm 2.

Step 1. Decrypt and decompress the secure key, K to obtain the vector Ω according to

$$\Omega = \Lambda(D(K)), \quad (9)$$

where D represents the decryption and Λ denotes the decompression operation. The same as in the compression and encryption procedure, decryption and decompression operations are beyond the scope of this paper.

Step 2. Transform the anonymized ECG signal, $\overline{x_2}[n]$ using FFT algorithm to acquire $\overline{X_2}[k]$.

Identify applicable funding agency here. If none, delete this text box.

Step 3. Divide each element in the vector $\overline{X_2[k]}$ with each element in the vector Ω. Hence, we get $X_2[k]$ according to Eq. 10 as follows

$$X_2[k] = \left\{\frac{\overline{X_2[k]}}{\Omega} : k = P+1, \cdots, Q\right\}, \quad (10)$$

and retrieve back the key, $\kappa[k]$ using Eq. 11 as

$$\kappa[k] = \{\Omega[k] - \text{offset} : \ k = 0, \cdots, P\}. \quad (11)$$

Step 4. Merge the vector $\kappa[k]$ in Eq. 11 into the vector $X_2[k]$ in Eq. 10 in order to get the un-anonymized ECG signal $X[k]$ as defined in Eq. 3.

Step 5. Reconstruct $X[k]$ using inverse FFT algorithm to obtain the lossless ECG signal, $\hat{x}[n]$ which will be presented to the medical personnel for further analysis.

III. Results and Discussions

In this section, we will evaluate performance of the proposed framework for ECG anonymization by way of computer simulation. The experiment will emphasis on ECG signal processing evaluation in terms of processing time. There are two types of ECG signals that will be utilized in this examination which are comprised of normal ECG signals for healthy subjects and abnormal ECG signals from a patient who suffered arrhythmia. The ECG signals were retrieved from a publicly available PhysioNet repository. The normal ECG signals were taken from PTB [27] database and the abnormal signal was obtained from MIT-BIH database [18].

A. Performance evaluation over normal ECG signal

A normal ECG signal for performance evaluation of the proposed framework was taken from PTB database (i.e., patient245, signal s0474), which encompasses 2 minutes duration was utilized for evaluation. According to [26] the normal ECG signal from PTB database was retrieved using sampling frequency, $f_s = 1{,}000$ Hz.

Fig. 3 shows ECG anonymization processing time as a function of ECG signal length, Q. In order to provide efficient calculation of the proposed algorithm, a power of two integer ECG signal length was chosen for each simulation. In this simulation, ECG signal lengths, Qs were set to $2^{12} = 4{,}096$ points up to $2^{16} = 65{,}536$ points signifying time duration between 4.096 seconds and 65.536 seconds. The processing time for each data point in Fig. 4 was run over 100 simulations.

It is clearly seen from Fig. 3 that ECG anonymization processing time of the proposed framework, which was run for different values of secret key length outperforms the preceding wavelet packet-based algorithm. The proposed framework utilizing FFT algorithm is approximately 5 times faster than the wavelet packet based. For example, for ECG signal length $Q = 2^{14} = 16.384$ points, the proposed framework took approximately 6 milliseconds to anonymized the ECG signal. In contrast, the wavelet packet based algorithm spent longer processing time, which is approximately 33 milliseconds.

Moreover, Fig. 3 shows that the processing time of the proposed framework remains the same for several variations of the secret key length. Based on this fact, it can be inferred that the proposed framework offers flexibility for the application to choose the length of secret key in the ECG anonymization process. In contrast, the previous wavelet packet-based approach can only provide the key size that was regulated by a factor of $\frac{N}{2^j}$, where N is the ECG signal length and j is the decomposition level.

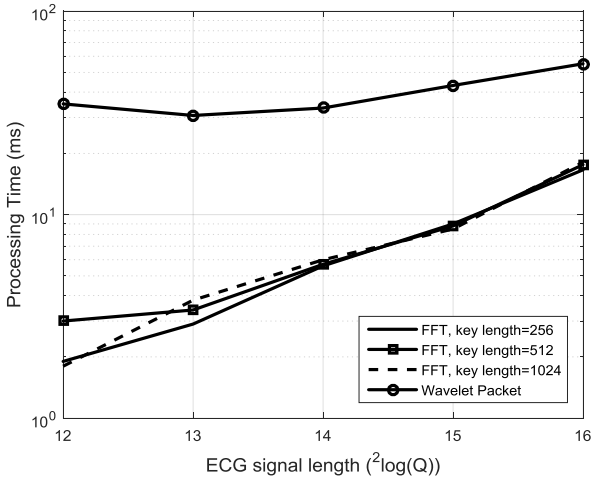

Fig. 3. Processing time of a normal ECG signal anonymization using the proposed algorithm for different key lengths compared to the wavelet packet anonymization technique.

B. Performance evaluation over abnormal ECG signal

An arrhythmia is an abnormal heart beat pattern, which is caused by problems in the heart's electrical system. This abnormality is commonly classified into two basic patterns, i.e., slower electrical impulses than normal ECG signal called bradycardia and faster electrical impulses than normal ECG signal called tachycardia. Heart rate in bradycardia is less than 60 beats per minute, while heart rate in tachycardia is more than 100 beats per minute [27, 28].

In this study, an abnormal ECG signal was taken from MIT-BIH arrhythmia database (i.e., signal 105m) with approximately 3 minutes signal duration. This abnormal ECG signal was retrieved using sampling frequency, $f_s = 360$ Hz and classified as a tachycardia syndrome. The Qs were set to $2^{12} = 4{,}096$ points up to $2^{16} = 65{,}536$ points signifying time duration between 11.37 seconds and 182 seconds used in the experiment to maintain efficient computation of the FFT and the inverse FFT algorithms.

Fig. 3 depictss ECG anonymization processing time for abnormal ECG as a function of ECG signal length, Q. It can be seen that the FFT-based algorithm was able to anonymize the ECG signal at around 40 times faster than the wavelet packet based algorithm. For example, for ECG signal length

$Q = 2^{14} = 16.384$ points, the proposed FFT-based algorithm took approximately 1.2 milliseconds to anonymized the ECG signal. On the other hand, the wavelet packet based algorithm spent approximately 44 milliseconds to anonymize the signal. The figures shows similar behavior for variations of the secret key length.

Based on the performance evaluation shown in Fig. 3 and Fig. 4, it can be concluded that the proposed FFT-based ECG security framework outperforms the existing method that employed the wavelet packet based algorithm. Low processing time can be considered as an important parameter to conserve energy in mobile and sensor node platforms. Therefore, an ECG anonymization algorithm that preserves low computational of the overall system is desired.

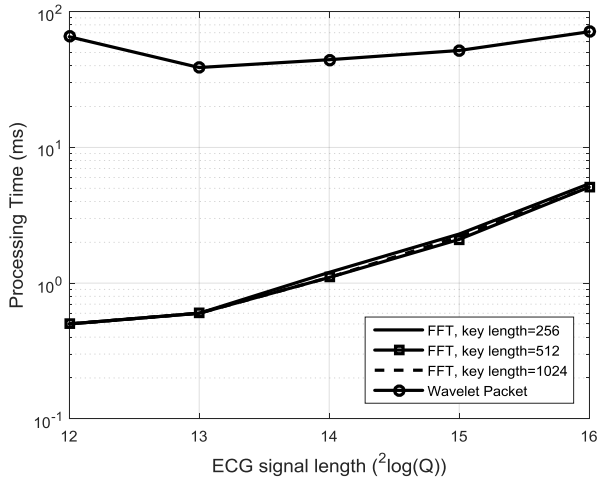

Fig. 4. Processing time of an abnormal ECG signal anonymization using the proposed algorithm for different key lengths compared to the wavelet packet anonymization technique.

IV. CONCLUSIONS

In this work, a novel ECG anonymization model has been proposed and examined to address two major constraints in the online healthcare system, i.e., immediate need for securing ECG signal transmission and efficient method for overcoming physical limitation of sensor nodes. Performance evaluation over processing time showed that the proposed algorithm inherited lower processing time compared to the recently proposed wavelet packet-based algorithm. Additionally, processing time of the proposed framework remains the same for several variations of the secret key length. Therefore, the proposed framework offers flexibility for the application to choose the length of secret key in the ECG anonymization phase.

REFERENCES

[1] WHO, Global status report on non communicable diseases (NCD) 2014, Geneva, Switzerland: WHO Press, 2014.

[2] WHO, Health in Asia and the Pacific, World Health Organization - Western Pacific & South-East Asia, 2008.

[3] L. Biel, O. Petersson, L. Philipson, and P. Wide, "ECG analysis: a new approach in human identification," *IEEE Trans. Instrum. Meas.* Vol. 50, no. 3, pp. 808–812, Jun. 2001.

[4] G. Wubbeler, M. Stavridis, D. Kreiseler, R.D. Bousseljot, and C. Elster, "Verification of humans using the electrocardiogram," *Pattern Recognit. Lett.* Vol. 28, pp. 1172–1175, Jul. 2007.

[5] I. Odinaka, P. Lai, A.D. Kaplan, J.A. O'Sullivan, E.J. Sirevaag, J.W. Rohrbaugh, "ECG biometric recognition: a comparative analysis," *IEEE Trans. Inf. Forensics and Security* vol. 7, no. 6, pp. 1812–1824, Aug. 2012.

[6] J. Jusak and I. Puspasari, "Wireless tele-auscultation for phonocardiograph signal recording through the zigbee networks," in *Proc. IEEE Asia Pacific Conference on Wireless and Mobile (APWiMob)*, Bandung, Indonesia, 27-29 Aug. 2015.

[7] J. Jusak, H. Pratikno, and V.H. Putra, "Internet of Medical Things for cardiac monitoring: paving the way to 5G mobile networks," in *Proc. IEEE Int. Conference on Communication, Networks and Satellite (COMNETSAT 2016)*, Surabaya, Indonesia, Dec. 2016.

[8] K.S. Fahim, S.S. Mahmoud, and I. Khalil, "A novel wavelet packet-based anti-spoofing technique to secure ECG data," *Int. J. Biometrics* vol.1, no. 2, pp. 191–208, Aug. 2008.

[9] E. Reinsmidth, D. Schwab, and L. Yang, "Securing a connected mobile system for healthcare," in *Proc. the 17th IEEE International Symposium on High Assurance Systems Engineering (HASE)*, Orlando, FL, USA, Jan. 2016.

[10] Department of Health & Human Services USA, "Security 101 for covered entities HIPAA Security Series (2)," *Department of Health & Human Services, USA*, pp. 1-11, 2007.

[11] European Parliament and of the Council, "Directive 95/46/EC of the European Parliament and of the Council: on the protection of individuals with regards to the processing of personal data and on the free movement of such data," *Official J. European Communities (1)*, no. 281, pp. 31-50, Oct. 1995.

[12] Privacy Commisioner, *Health information privacy code 1994 Ed. 2008*, Auckland, New Zealand: KB Printed Ltd., 2008.

[13] C. Pearce and M. Bainbridge, "A personally controlled electronic health record for Australia," *J. Am. Med. Inform. Assoc.* vol. 21, no. 4, pp. 707-713, Mar. 2014.

[14] S.S. Mahmmoud, "A generalized wavelet packet-based anonymization approach for ECG security application," *Sec. Comm. Net.* Vol. 9, no. 18, pp. 6137-6147, Dec. 2016.