A HIGH PRECISION DATA ENCRYPTION ALGORITHM IN WIRELESS NETWORK MOBILE COMMUNICATION

AIWAN FAN*
School of Computer, Pingdingshan University
Pingdingshan, China

QIMING WANG
College of Information Engineering, Pingdingshan University
Pingdingshan, China

JOYATI DEBNATH
Dept. of Mathematics and Statistics, Winona State University
Winona, MN 55987, USA

ABSTRACT. At present, the MD5 based data encryption algorithm for wireless network mobile communication cannot effectively detect the intrusion data in the mobile communication. Redundant data is not removed, the efficiency of data encryption is low, and the overall communication security is poor. In this paper, a MDEA based data encryption algorithm for wireless network mobile communication is proposed. By applying normalization of communication data to DBN model, using the way of changing one parameter while keeping others, the optimal DBN detection model is built to achieve high-precision detection of intrusion data. Using the signal intensity at different times, the speed and process time of the data level movements are estimated. By estimating the results, the redundant data and inappropriate data are removed, and performed the MDEA operation based on the secret data, introduced random numbers and timestamps to prevent the foreign infiltrations. Experiments show that the algorithm can not only improve the detection quality of intrusion data, but also enhance the cleaning effect of redundant data and in the communication, and enhance data security.

1. Introduction. Broadband wireless mobile communication has become one of the most concerned industrial fields in the development of global communications industry [3]. In the future, broadband wireless mobile communication technology’s evolution, intelligent terminals and business applications will form broad market space, which is an important driving force for the development of global communication industry. National key projects have been explicitly requested, that is, to grasp the core technology and independent intellectual property rights of mobile communication as a breakthrough for upgrading the core competitiveness of China’s communications industry [7,18]. It is of great significance to develop the broadband wireless mobile communication industry. Wireless communication is divided into two types: wireless mobile communication and wireless LAN communication, and

2010 Mathematics Subject Classification. 19J25.
Key words and phrases. Wireless network, mobile communication, high precision, data encryption.
* Corresponding author: Aiwan Fan.
their transmission facilities are fundamentally different [9]. Among them, wireless mobile communication needs telephone office or other public services, to provide users with facilities, and use packet radio, cellular network and satellite station to transmit and receive signal [2].

With the rapid development of computer technology and database technology matures, a large number of useful data are accumulated, especially extensive application of cloud computing and storage technology, privacy information security problems are more worrying, how to effectively protect the privacy information database, has aroused widespread concern from all walks of life [8, 14]. Research shows that most people are unwilling to provide their privacy information to the website, while some people are willing to provide it to the website under the condition that only the privacy information is protected. Therefore, the effective protection of personal privacy has become a very meaningful research topic as well as taking full advantage of the accumulated data and mining the potential laws.

In a word, the security of data in wireless network mobile communication is one of the problems that need to be solved urgently. Data encryption is a long history technology. It means converting plaintext to ciphertext through encryption algorithm and encryption key, and decryption is to restore ciphertext to plaintext by decryption algorithm and decryption key, and its core is cryptography [13,15]. Data encryption is still the most reliable way for computer systems to protect information. It uses cryptography to encrypt information to realize information concealment, thus protecting the security of information. At present, data encryption algorithm based on chaotic sequence can not get high accuracy encryption results. This paper proposes a data encryption algorithm based on MDEA for wireless network.

2. High precision data encryption algorithm in wireless network mobile communication. A series of processing of the data before the communication data encryption is carried out. Based on the detection of the intrusion data and the cleaning of the intrusion data, the encryption algorithm is used to encrypt the data with high precision.

2.1. Intrusion detection data detection in wireless network mobile communication. In a wireless network mobile communication data set, the feature data are often not at the same order of magnitude, so data normalization needs to be processed to [0, 1] data.

Assuming that a selected data set contains \( N \) samples, each attribute column of all the samples can be mapped to:

\[
x = (x_1, x_2, \ldots, x_N)
\]  

In this case, if \( x_i \) is the corresponding attribute value of \( i \)th samples, the data is normalized by Maximum normalization, which is numeric type data.

\[
f(x_i) = \frac{(x_i - \min (x))}{(\max (x) - \min (x))}
\]

Where, \( \min (x) \) and \( \max (x) \) represent the minimum and maximum values of the \( x \), respectively.

After the normalization of the data, the DBN method is used to detect the data intrusion. The detection methods of unknown types of attacks by using the DBN method, mainly uses DBN model including multilayers to make RBM feature extraction, and the reverse update of CD learning method to optimize update network.
Generally speaking, the dimension of intrusion detection data is relatively high. The presence of some features can not only identify the types of attacks, but also reduce the accuracy of classification [17,22]. In order to get better results, it is often necessary to select the data that can identify the characteristics of the category. Therefore, the DBN model for feature extraction generally includes multi-layer RBM structure, and the learning process of multi-layer RBM can be described by Figure 1.

The processed data \( x \) is as the visible input data of the first RBM in DBN model (generally the number of first RBM visible layer unit equal to the dimension of the training data). CD algorithm is used to train the RBM layer by layer, and a output value of the previous RBM layer is as the input of the next layer, until the multi-layer RBM training is ended. The CD algorithm trains the RBM model step by layer as follows:

Input: a training sample \( x \), the number of unit in hidden layers \( n \), the learning rate \( \varepsilon \), the maximum training period \( T \);  
Output: the connection weight matrix \( w \), the offset \( a \) of the visible unit, and the offset \( b \) of the hidden unit.

Training phase: initialization, the initial state of the visible layer unit \( v = x \), \( w \), \( a \), \( b \) takes a very small number. The parameters are updated in accordance with the formula (3), formula (4) and formula (5).

\[
\begin{align*}
   w &\leftarrow w + \varepsilon (v - T) \quad \text{(3)} \\
   a &\leftarrow a + \varepsilon (v_1 - v_2) \quad \text{(4)} \\
   b &\leftarrow b + \varepsilon (a - w) \quad \text{(5)}
\end{align*}
\]

According to the calculation of the formula (3), the formula (4) and the formula (5), after the training of the multilayer RBM, the top-level BP layer is back propagating, and the parameters obtained from training RBM are finely adjusted.
according to the reconstruction error, so as to get the optimal RBM parameter \( b = b + \varepsilon (a - w) \). In this process, because in the practical application of the amount of data is often large, it needs to meet the real-time detection. In order to speed up the training process, generally the batch training modes used, where each of random sampling needs the fixed quantity of training data to input to the DBN. The number of samples each time corresponds to the value of the min-batch set in the program. The training of an min-batch, the network weights are updated, until all training completed.

In the intrusion detection process, data dimension of test samples is same as the training data. In the trained network structure, test data and the corresponding attribute are input. Through forward propagation, it can be calculated to obtain the actual classification results of each test data. Then, the attribute classification results and the input attribute label are made comparison, to complete the wireless network data intrusion detection in mobile communication.

2.2. **Cleaning of intrusion data and redundant data.** In this step, it will clean the following data:

1. dirty data: intrusion data in wireless network mobile communication;
2. redundant data: redundant data in wireless network mobile communication;
3. the data can not be used in the network mobile communication.

By considering the process time of data labels in the reader’s radiation range, the data processing and data output are executed separately, so as to clean dirty data and redundant data in wireless network mobile communication. According to the cleaning of data, the efficiency of data encryption can be improved. Figure 2 is the radiant range of the reader:

Figure 2 shows the vertical surface mapping of the work radiation when the reader is working normally, of which \( \vartheta \) represents the radiation angle of the reader’s reading range, and \( h \) represents the vertical distance from the reader to the labeled...
data, and $L$ represents the process distance. As shown in Figure 2, the signal and intensity model is built.

In this paper, the data propagation path model is used to describe the communication process of wireless network mobile communication.

$$PL(d) = PL(d_0) - 10n \log \frac{d}{d_0} + \partial$$ \hspace{1cm} (6)

Among them, $PL(d)$ represents that the signal intensity received by the label that distance reader is $d$. $d_0$ represents the approximate reference distance, and $\partial$ represents the random variable obeying normal distribution. In the practical application, the simplified model is generally used.

$$PL(d) = PL(d_0) - 10n \log \frac{d}{d_0}$$ \hspace{1cm} (7)

According to the formula (7), the relationship between distance and strength can be used to simplify the calculation, improve the efficiency of data cleaning and take $d_0$ as the 1km, then the further evolution formula (7) is obtained.

$$PL(d) = PL(1) - 10n \log d$$ \hspace{1cm} (8)

Among them, $PL(d)$ is rewritten to $RSSI_d$, and $PL(1)$ is rewritten to $RSSI_1$.

It can be arranged as:

$$d = 10^{\frac{(RSSI_1 - RSSI_d)}{(10n)}}$$ \hspace{1cm} (9)

The formula (9) reflects the relationship between the signal intensity and the distance, and $RSSI_1$ represents a measured value, which is a constant. The distance between the label and the reader is obtained on the basis of the signal intensity of the known label.

According to the above content, the cleaning of data is carried out. This algorithm is mainly composed of two parts: data processing and data output, and the two part is concurrent execution [12]. Among them, data processing is to make dirty processing for the label data read by the reader, to determine the expiration time of the label data, that is, the data that is not available, and make the redundant processing [4,5,10]. The output of the data is to read the data in the cache queue by the timer, and output the detection of the overdue label and the real data. When there is overdue label data, the comparator determines whether the overdue label data is a real label, and the output is submitted to the upper application system.

The data processing structure is shown in Figure 3.

In Figure 3, the conflict detection mechanism is to check whether or not there is the same label data. First, a table data $Q$ is obtained from the reader, through the comparison of the same label data in the read cache queue, whether the conflict occurs is to determine. When there is a conflict, it can get the $M$ value of reading the conflict data $P$ in cache. When the $M$ value is 1, the newly entered label data $Q$ must be processed by the calculator, then the expire time and $M$ value in the cache queue are modified to make $P(M) = P(M) + 1$. When the $M$ value is greater than 1, the $M$ value of the conflict data in the cache queue is read by modifying $P(M) = P(M) + 1$; When there is no conflict, data $Q$ is processed directly through the converter to read the format required by the cache, which is directly inserted into the end of the read cache queue, of which $Q$ (expiretime) is defaulted to an appropriate value.
The converter is used to format the new data read by the reader to make it unified and facilitate the processing of the label data \([6, 16]\). Calculator is to calculate the expiretime of label data. The process speed \(V\) of label and process time \(t\) are calculated by combining distance—signal strength propagation model. The specific ideas are as follows: first, the signal intensity value \(\text{RSSI}\) of that it is firstly collected by two times. According to the formula of the distance—signal intensity propagation model (9), the label is calculated at time \(t_1\) and time \(t_2\), and the distance from the reader is \(d_1\) and \(d_2\), respectively.

\[
d_1 = 10^{\frac{\text{RSSI}_1 - \text{RSSI}_{d1}}{10^n}} \quad (10)
\]
\[
d_2 = 10^{\frac{\text{RSSI}_1 - \text{RSSI}_{d2}}{10^n}} \quad (11)
\]

As shown in Figure 3, by the knowledge of image geometry, the interval distance \(A\) at different positions that the calculated label is first read for the first time can be expressed as:

\[
A = \sqrt{d_1^2 - h^2} - \sqrt{d_2^2 - h^2} \quad (12)
\]

The process speed \(V\) can be expressed as:

\[
V = \frac{A}{(t_2 - t_1)} \quad (13)
\]

The process time of label can be obtained as follows according formula (10) to (13):

\[
t = \frac{L \ast (t_2 - t_1)}{\sqrt{10^{\frac{\text{RSSI}_1 - \text{RSSI}_{d1}}{10^n}}} - \sqrt{10^{\frac{\text{RSSI}_1 - \text{RSSI}_{d2}}{10^n}}}} \quad (14)
\]

The results is saved to the end of the read cache queue.

According to the above calculation results, the data is output. The data output is composed of a timer, a redundant caching queue, an non-available data detection, comparator, and so on. The specific data output structure is shown in Figure 4.

![Figure 3. data processing structure](image)
Timer is used to control timing obtain the expired label data from the read cache queue, and output to the detection mechanism to process, so as to output the required data to the application system [1,19,23].

The comparator mainly compares the label data 1 with the prescribed threshold 2 to determine whether the label data is true of the label data. If it is real data, output and submit to the upper application system; if it is not real data, it will not be exported to the upper application system [11,20,21].

The overall data output is described as follows:

1. start;
2. initialization of data setting;
3. determine whether the redundant noise cache queue has data, when there is no data, turn to step (9), and turn to step (4) when there is data.
4. the label data in the read caching queue will be cleaned and detected, if there are expired data, to step (5), otherwise, to the step (8);
5. obtain the label data to be cleaned;
6. the outdated data is processed by the comparator, and the result is the real label data, to the step (7), or else to the step (8).
7. output the label data to be cleaned to the upper application system and then turn to the step (8).
8. delete the label data that should be cleaned in the read cache and turn to the step (9).
9. end.

2.3. High precision data encryption algorithm for wireless network mobile communication based on MDEA. Based on the data processing in 2.1 and
2.2, the MDEA algorithm is used to encrypt the mobile communication data of the wireless network, which is essentially a hash function mapping operation.

Assuming that $H(\cdot)$ represents a one-way hash function, $H(\cdot)$ is the client, $S$ is the authentication server, $AS$ is the application server, $pubs$ is the public key of authentication server, $pris$ is the private key of authentication server, $pubs$ is the public key of application server, $AS$, $pris$ is the private key of application server, $AS$, $pubc$ is the public key of client, $pric$ is the client’s private key, $R_s$ is the generated random number of the client, $R_s$ is the random number of the authentication server, $k$ is the shared key of the application server and the authentication server, $K_s$ is the session key, $id$ is the user ID, $S_{id}$ is the authentication service ID, $AS_{id}$ is the application server ID, $pw$ is the user password, $ts$ is the time stamp, $ACL$ is the access control list, $TGC$ is the bill license and $ST$ is the service bill.

The structure of the MEDA algorithm is shown in Figure 5.

When the client user visits the application system for the first time, it will be redirected to the authentication server, to enter his username and password, and the $e$ encrypted by the formula (15) will be sent to the authentication server through the secure channel to request authentication, that is, the process (1). The authentication server is decrypted after receiving $e$. If the timestamp is valid, it will retrieve whether the user information database exists $id$ or not, and decide if the saved $id$ is equal to the formula (15). If the same is equal, the next step is continued; otherwise, the user’s identity is illegal and the user is denied login.

$$e = pubs\{id, ts, H(pw), ts, id\}$$ (15)

The authentication server uses the formula (16) to encrypt the generated random numbers $R_s$, $S_{id}$, and $t + 1$, and sends $B$ to the client. After decrypting the $B$, the client enters the process (3), and sends the $j$ from the formula (17) to the authentication server. After the authentication server decrypts $j$, the comparison is made to judge whether $H(R_s)$ is equal to the hash value of $R_s$ generated by the authentication server. If the assumption is equal, the user is a legitimate user, allowing the user to log in; assuming that the user is not equal, it indicates that the
user is illegal and refuses its access.

\[ B = \text{pubs} \{ id, R_c, ts + 1, R_s, S_{id} \} \]  \hspace{1cm} (16)

\[ j = \text{pubs} \{ id, R_c, ts + 2, H(R_s), id \} \]  \hspace{1cm} (17)

The authentication server sends \( D \) encrypted by formula (18) to the client, which is decrypted by the client and whether the hash value of \( R_c \) in the client is equal to the \( H(R_c) \) is compared. If it equals, it shows that the authentication server is legal; if not, it indicates that the authentication server is not legal. At this point, a two-way authentication has been completed, and the user’s login is successful.

\[ D = \text{pubs} \{ S_{id}, ts + 3, H(R_c), ST, TGC, K_s, S_{id} \} \]  \hspace{1cm} (18)

After authenticated, users can access the application server. The client will be sent to the application server by the \( E \) encrypted by formula (19), the application server will decrypt the \( E \), and then enter the process (6). The \( F \) is sent to the authentication server by the formula (19).

\[ E = \text{pubs} \{ ts1, id, pric, \{ id, ST, ts1 \} \} \]  \hspace{1cm} (19)

\[ F = \text{pubs} \{ AS_{id}, ts2, prs \{ ts2, ST \} \} \]  \hspace{1cm} (20)

The authentication server decrypt \( F \). If \( ST \) is valid, the user’s identification information and session key and other related information will be encrypted, and \( G \) obtained by the formula (21) can be returned to \( AS \). The access control list \( ACL \) can be obtained according to the user identification information. According to the application server \( ACL \), it is possible to decide which users to provide services. Next, \( ts \) obtained from the formula (22) is sent to the client in the process (8), and the client decrypts it. Within the valid time period of \( TGC \), which allows users to access the authorized application server according to the access control list. Assuming that \( TGC \) is overdue, the user needs to re-authenticate.

\[ G = \text{pus} \{ S_{id}, ts2, pris \{ S_{id}, \{ id, K_s \} \} \} \]  \hspace{1cm} (21)

\[ ts = \text{pubc} \{ AS_{id}, ts1 + 1, prs \{ ACL, AS_{id} \} \} \]  \hspace{1cm} (22)

3. Experimental results and analysis. In order to verify the effectiveness of the encryption algorithm, a simulation experiment is carried out on a computer with the dual core CPU processor, 2.85GHz main frequency, 4GB RAM, 1TB hard disk and Windowd operating system. VC++ programming is used to implement the encryption algorithm. At the same time, in order to make the results of the algorithm more convincing, the current encryption algorithm is used to compare the experiments. The experiment is carried out from the following aspects:

(1) the quality of intrusion data detection in wireless network mobile communication;
(2) the effect of data cleaning;
(3) security after data encryption.

The results of the experiment are as follows:

Figure 6 (a) shows a running signal waveform in wireless network mobile communication, and the signal contains intrusion data, so as to verify the quality of intrusion detection by different algorithms. Where, cross mark represents the intrusion data that has been detected.

From Figure 6, we can see that the detection effect of the proposed intrusion detection algorithm is better than that of the current SVM based intrusion detection
(a) detection effect of intrusion detection algorithm based on SVM

(b) detection effect of intrusion detection algorithm based on BP neural network

(c) the detection effect of the intrusion detection algorithm in this paper

Figure 6. Comparison of the effects of different algorithms on Intrusion Detection

algorithm and the BP neural network based intrusion detection algorithm. The intrusion detection algorithm used in this paper uses the normalization of the mobile communication data in the wireless network, and then applies it to the DBN model. The unknown attack type is detected by selecting the relatively optimal DBN structure by fixing the changes of other parameters. Through the experimental results, it is proved that the DBN intrusion detection algorithm has good adaptability and strong ability to detect intrusion data.
The communication network of Figure 7 (a) contains four kinds of data, such as redundant data, non-available data, intrusion data and normal data. The current data cleaning algorithm and the data cleaning algorithm used in this paper are tested to verify the effectiveness of the algorithm for data cleaning.
The analysis of Figure 7 shows that when the current algorithm is used to clean the data, the results of the redundant data, the intrusion data and the non available data are poor, and the cleaning is not thorough. In this paper, the distance-signal model is applied to the data cleaning, and the process time of the label is calculated. At the same time, data processing and data output are executed separately and parallel. The output time is supported by timer and time cycle, which shortens the execution time of the algorithm and makes data cleaning more thorough.

In Figure 8, the black dots represent the external attack data signals. By using different encryption algorithms to compare to verify the algorithm’s ability to resist foreign attacks, that is, security.

In Figure 8, the security of the data encryption algorithm based on CAS is the worst which can not be a good defense against attacks on the server; data encryption algorithms based on DES and RSA have better security, which is a good defense.
against a part of a foreign attack data. This proposed algorithm can not only improve the communication security between the client and the server. Moreover, after the completion of authentication, protection measures are also applied to the communication security between users and application servers, which improves the overall effectiveness of the proposed algorithm.

4. Conclusions. The security of more and more used data of mobile communication in wireless network is not good, the information security problem has become increasingly prominent. Users pay more attention to data privacy. It is a good choice to upload encrypted data to the cloud server and store it on the cloud server. In view of the current problems existing in data encryption algorithm, this paper presents an encryption algorithm of data in mobile communication wireless network based on MDEA. Based on the detection of intrusion data and the cleaning of data, the two-way authentication is to achieve through data encryption and decryption in client and server. Experiments show that the algorithm compared with the current algorithm is more reliable.

Acknowledgments.

1. Project of scientific and technological breakthrough in Henan (No. 152102210193);
2. The project of funding plan for the young backbone teachers of universities (No. 2013GGJS-209);
3. Key scientific research projects in Henan colleges and Universities (No. 15A5 20091).

REFERENCES

[1] P. A., System and method for combining deduplication and encryption of data, 2015.
[2] J. Ahmad and S. O. Hwang, Chaos-based diffusion for highly autocorrelated data in encryption algorithms, Nonlinear Dynamics, 82 (2015), 1839–1850.
[3] A. Argyris, E. Pikasis and D. Syvridis, Gh/s one-time-pad data encryption with synchronized chaos-based true random bit generators, Journal of Lightwave Technology, 34 (2016), 5325–5331.
[4] J. L. Baril, Avoiding patterns in irreducible permutations, Discrete Mathematics and Theoretical Computer Science, 17 (2006), 13–30.
[5] L. Bossuet, N. Datta, C. Mancillas-López and M. Nandi, Elmd: A pipelineable authenticated encryption and its hardware implementation, IEEE Transactions on Computers, 65 (2016), 3318–3331.
[6] M. D. Champañí, S. Sajjadi, S. H. Moussavizadehgan and F. Moodi, A fuzzy system for evaluation of deteriorated marine steel structures, Journal of Intelligent & Fuzzy Systems, 32 (2017), 1945–1958.
[7] H. Chen, X. Du and Z. Liu, Optical hyperspectral data encryption in spectrum domain by using 3d arnold and gyrator transforms, Spectroscopy Letters, 49 (2016), 103–107.
[8] B. Cui, Z. Liu and L. Wang, Key-aggregate searchable encryption (kase) for group data sharing via cloud storage, IEEE Transactions on Computers, 65 (2016), 2374–2385.
[9] W. D. H., Data authentication and security assurance based on distributed storage system, Journal of China Academy of Electronics and Information Technology, 1 (2015), 613–619.
[10] M. Gomez-Barrero, E. Maiorana, J. Galbally, P. Campisi and J. Fierrez, Multi-biometric template protection based on homomorphic encryption, Pattern Recognition, 67 (2017), 149–163.
[11] Y. Jiang, G. Li, W. Che, Y. Liu, B. Xu, G. Shan, D. Zhu, Z. Su and M. R. Bryce, A neutral dinuclear ir(iii) complex for anti-counterfeiting and data encryption, Chemical Communications, 53 (2017), 3022–3025.
[12] M. Khan, A novel image encryption scheme based on multiple chaotic s-boxes, Nonlinear Dynamics, 82 (2015), 527–533.
A. Khedr, G. Gulak and V. Vaikuntanathan, Shield: Scalable homomorphic implementation of encrypted data-classifiers, *IEEE Transactions on Computers*, 65 (2016), 2848–2858.

K. Lata, Secure data aggregation in wireless sensor networks using homomorphic encryption, *International Journal of Electronics*, 102 (2015), 690–702.

M. A. Lei, H. X. Yang and J. P. Liu, User privacy data storage method under big data environment, *Computer Simulation*, 465–468.

H. Li, D. Liu, Y. Dai and T. H. Luan, Engineering searchable encryption of mobile cloud networks: When qoe meets qop, *IEEE Wireless Communications*, 22 (2015), 74–80.

M. Li, D. Xiao, A. Kulsoom and Y. Zhang, Improved reversible data hiding for encrypted images using full embedding strategy, *Electronics Letters*, 51 (2015), 690–691.

H. Y. Lin, Location-based data encryption for wireless sensor network using dynamic keys, *Wireless Networks*, 21 (2015), 1–8.

S. T. Opitz, K. Neumann, S. Bernholt and U. Harms, How do students understand energy in biology, chemistry, and physics development and validation of an assessment instrument, *Journal of Mathematics Science and Technology Education*, 13 (2017), 3019–3042.

S. T. Opitz, K. Neumann, S. Bernholt and U. Harms, Students’ energy understanding across biology, chemistry, and physics contexts, *Journal of Interdisciplinary Mathematics*, 20 (2017), 397–415.

Z. H. Qian, D. Feng, X. Wang and Q. Li, Multipath routing algorithm in m2m network based on load balancing, *Journal of Jilin University(Engineering and Technology Edition)*, 46 (2016), 934–940.

S. Trejos, J. F. Barrera, A. Velez, M. Tebaldi and R. Torroba, Optical approach for the efficient data volume handling in experimentally encrypted data, *Journal of Optics*, 18 (2016), 065702.

J. Xu, Data distributed mandatory secure access method in cloud computing environment, *Bulletin of Science & Technology*, 189–192.

Received July 2017; revised December 2017.

E-mail address: faw19780163.com
E-mail address: wqm8157@126.com
E-mail address: jdebnath@winona.edu