Chaotic stream cipher-based secure data communications over intelligent transportation network

Chaotic Stream Cipher-Based Secure Data Communications over Intelligent Transportation Network

Wei Zhang, Shanyu Tang*, *Senior Member, IEEE*, Liping Zhang, Zhao Ma, and Jun Song

Abstract

Intelligent Transportation Systems (ITS) are advanced applications in which the transportation industry is adapted to the information technology revolution. As an important development direction of ITS, the Electronic Toll Collection (ETC) subsystem, which enables an efficient and speedy toll collection, has gained widespread popularity in the world. In an ETC system, toll transaction data are transmitted over intelligent transportation networks, which is vulnerable to eavesdropping, interfering, and tampering attacks. To address the above security problems, we proposed a chaotic stream cipher-based cryptographic scheme to realise secure data communications over Wireless Sensor Network (WSN), which is a part of ITS. The proposed cryptographic scheme allowed ITS to achieve key negotiation and data encryption between sensor nodes in the WSN, whileas reduced

This work was supported by the National Natural Science Foundation of China under Grant 61272469 and Grant 61303237, and the Wuhan Scientific Research Program under Grant 20113010501010144.

Wei Zhang is with China University of Geosciences, Wuhan, 430074, China (e-mail: 1002324821@qq.com).

Shanyu Tang * is with China University of Geosciences, Wuhan, 430074, China (e-mail: shanyu.tang@gmail.com; Tel: +86 (0)27 6784 8563).

Liping Zhang is with China University of Geosciences, Wuhan, 430074, China (e-mail: carolyn321@163.com).

Zhao Ma is with China University of Geosciences, Wuhan, 430074, China (e-mail: mazhao@cug.edu.cn).

Jun Song is with China University of Geosciences, Wuhan, 430074, China (e-mail: songjun@cug.edu.cn).

computational costs and power consumption. Security analysis and experimental results showed that the proposed scheme could protect data transmission between wireless sensor nodes from being attacked, and significantly reduced the communication overhead for the whole system compared to the existing ECC_AES scheme, thus satisfying the real-time data transmission requirement of ITS.

***Index Terms*—Intelligent Transportation Network, Secure Communication, Chaotic Stream Cipher, WSN.**

I. INTRODUCTION

Intelligent Transportation Systems (ITS) provide real-time, accurate, effective and comprehensive transportation management services by integrating advanced communications, sensing, automation, and information processing technologies into transportation infrastructure and vehicles [1]. Users of ITS include motorists, commercial operators, and public transport customers, who rely on ITS to make travel decisions, are informed based on such factors as traffic conditions, road maintenance or construction work, and weather conditions that could potentially impact travel time and safety. Policy makers and road or highway operators also utilize the information from ITS in the management and future planning of the road networks.

Intelligent transport systems vary in technologies applied, and mainly comprise seven subsystems: Electronic Toll Collection System (ETC), Advanced Transport Information Service (ATIS), Advanced Transportation Management System (ATMS), Advanced

Public Transportation System (APTS), Advanced Vehicle Control System (AVCS), Freight Management System (FMS), and Emergence Rescue System (ERS), in which ETC has already become an important development direction of ITS [2].

Electronic Toll Collection system has greatly improved the toll collection process by making use of transponder with RFID technology, and license plate recognition system to identify vehicles, and by transmitting information in relation to toll transaction over ETC network to collect the final tolls without stopping or slowing traffic. ETC system helps eliminate or minimize chock points along the routes with toll booths, thus effectively accelerating the speed of toll collection, enhancing traffic capacity of the toll roads, and conserving energy. Due to the advantages mentioned above, ETC is gaining widespread use throughout the country and even the world.

A. Electronic Toll Collection System

As shown in Fig. 1, an Electronic Toll Collection system is generally divided into two subsystems: a foreground system, and a background system. The former mainly comprises three parts [3]: Automatic vehicle identification (AVI) system, Automatic vehicle classification (AVC) system, and Violation enforcement (VE) system. The On Board Unit (OBU) is a box installed in the car, capable of collecting location information that is sent to the Road Side Unit (RSU) via Dedicated Short Range Communication (DSRC) protocol. The latter is primarily responsible for the initialization of OBU, receiving and processing the transaction data from the foreground, storing communication data, computing the prices associated with the roads, and forming the final payment information, and so on. An automatic toll collection process is completed smoothly with the deliberate cooperation of foreground and background.

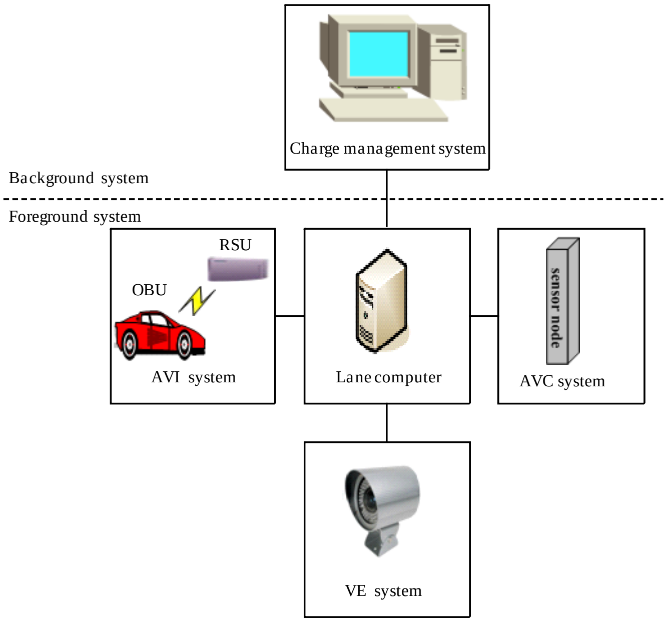


Fig. 1. ETC intelligent transportation system.

B. ETC Intelligent Transportation Network

Information on tolls is transmitted over an ETC intelligent transportation network, which is regarded as a derivative of the Internet of Things [4], thereby possessing its structural characteristics. The layered structure of ETC intelligent transportation network is illustrated in Fig. 2, in which the data perception level collects the vehicle information and OBU information, and then forwards those data to the background system through the data transport level after the process of the data protection level. Finally, the data application level takes full use of those data gathered.

Data communications between OBU and RSU over an intelligent transportation network are carried out using DSRC technology [5]; data transmission among sensor nodes uses Wireless Sensor Network (WSN) technique; the exchange of information between RSU and the processing centre is based on Wireless Local Area Network (WLAN) and so on. All of the communication links collaboratively realize the transaction information transmitted favourably.

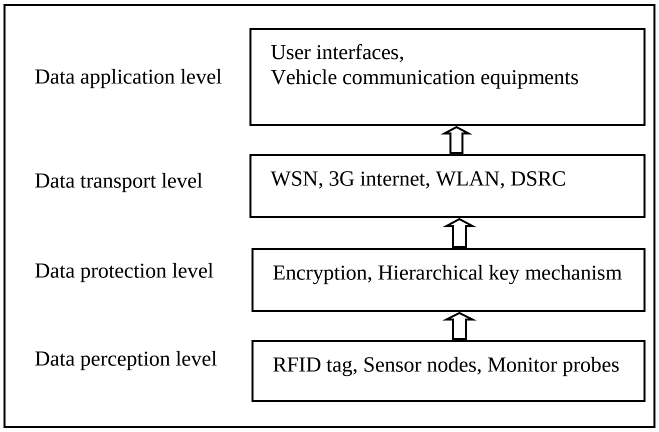

Data application level
User interfaces,
Vehicle communication equipments
Data transport level
WSN, 3G internet, WLAN, DSRC
Data protection level
Encryption, Hierarchical key mechanism
Data perception level
RFID tag, Sensor nodes, Monitor probes

Fig. 2. Four layers of ETC intelligent transportation network.

C. Security Requirements

As Dimitrakopoulos *et al.* stated, the popularization of ETC intelligent transportation network has arisen numerous information security issues [2]. Data packets carrying private and valuable information about the driver and the car transmitted over an intelligent transportation network are subject to eavesdropping, tampering, and decoding attacks by adversaries. This is owing to the fact that an ETC system uses many traditional communication technologies with inherent security problems.

The inherent vulnerabilities of Wireless Sensor Network, which is deployed in ETC lanes, could compromise the whole security of an intelligent transportation network. Moreover, the DSRC protocol that is used to connect OBU and RSU has several shortcomings, such as bypass interference, and car-following interference. Therefore, it is urgent to improve data transmission security for ETC intelligent transportation networks.

With the aim of improving the security of data communications over an ETC intelligent transportation network, we focused on creating a safe environment for WSN as a part of it to protect the information in relation to the drivers and the vehicles in the ETC lanes from being eavesdropped, tampered, and / or interfered.

D. Motivation for Giving a Priority to WSN

In an ETC system, a large number of wireless sensor nodes are deployed at ETC lanes, and they are small in size and operate on small sized battery with very limited data processing power. Those wireless sensor nodes constitute a WSN by means of self-organization [6]. The sensor nodes are used to apperceive (acquire), dispose, and transmit information about the driver and the driving vehicle in ETC lanes. Meanwhile, they are also used to store, manage, and fuse information which is retransmitted by other sensor nodes. The above information is then converged at a sink node, and forwarded to the processing centre (server) for central fusion and processing through exterior networks. Depending on the received information, the processing centre determines the final tolls that should be deducted from the vehicle owner’s Intelligent Card.

The maintenance and monitoring of sensor nodes is quite difficult due to its deployment environment, and so the sensor nodes could be easily compromised by adversaries. The security of the information collected by the sensor nodes has a direct impact on the privacy of vehicle owners, thus a priority should be given to secure data communication over WSN.

Encrypting sensitive data such as vehicle information on deduction standards could effectively resist some attacks on WSN. As secure key management is the premise of information encryption, encryption techniques and key management are the central gravity for the security of WSN. There has been extensive literature in researching WSN security, which can be divided into two categories in the cryptography field. One uses symmetric encryption; although existing symmetric encryption schemes provide a good level of security, key maintenance remains difficult. The other emphasizes asymmetric encryption (public-key cryptography). When asymmetric schemes are used, key management becomes easier, but they provide a lower level of security compared to the former. No matter which kind of protection method is adopted, the low battery power, limited memory space, and less processing capabilities of sensor nodes should be taken into account. In this study, we proposed an efficient symmetric key negotiation, data encryption and key update scheme based on a Logistic chaotic stream cipher algorithm.

The rest of this paper is organized as follows: Section II presents the related research work on WSN security protection. Our proposed cryptographic scheme is described in detail in Section III. Section IV shows the security analysis of the proposed scheme. The experimental results and performance comparisons of the proposed scheme are discussed in Section V. Finally, the conclusion of the paper is given in Section VI.

II. RELATED WORK

The security aspects that have been attracting a vast of attention in WSN are the areas of information encryption and key management, which are mainly achieved by using symmetric cryptography and public key cryptography.

Currently, security in Wireless Sensor Network is provided mostly through symmetric cryptography. LEAP protocol [7] was designed to prevent security threats and localize the possible damages based on symmetric cryptography. This protocol supports the establishment of some types of keys for each sensor node, in which pair wise keys are used for secure data transmission between a sensor node and its direct neighbours. To share the key with neighbours, sensor node A broadcasts a ‘hello’ message to discover its direct neighbours (one hop node), and then waits for each neighbour to replay with their identities. After receiving replay from neighbour B, A computes a key KAB. Sensor node A generates KB = f Ki(B), and then computes KAB as KAB = f KB (A). Node A erases the key Ki after neighbour discovery or time expiration. Thus no other node can compute KAB after erasing the key. Sensor node B computes KAB in the same manner without transmitting any message. Finally, each pair of adjacent sensor nodes possesses a unique secret key. The protocol effectively enhances the security of information transferred between sensor nodes. However, the number of neighbour nodes is abundant for each sensor node, which results in the difficulty of key maintenance. In addition, the workload for computing those secret keys is tremendous. The defects mentioned above are contradictory with the features of sensor nodes.

A RSA-based asymmetric algorithm was used to solve the problem of information security in Wireless Sensor Network [8]. This encryption algorithm contains two phrases: a sensor node to shakehand with another sensor node in which the two sensor nodes setup a session key; the use of the session key for data encryption. However, this encryption algorithm is not practical, since under the assumption that the nature of sensor node could not support asymmetric encryption algorithm due to the limitations of sensor battery and CPU power. Furthermore, the public key algorithm with low encryption speed could not meet the real-time data transmission requirement, which is vital to WSN.

The above analysis shows that both symmetric and asymmetric encryption algorithms have shortcomings. To cope up with the shortcomings, Ganesh et al. [9] proposed to combine Elliptical Curve Cryptography (ECC) with Advanced Encryption Standards (AES) to form an information protection method for WSN. The equation of standard Elliptic Curve is $y^2 = x^3 + ax + b(a, b \in F_q)$, in which the values of *a* and *b* are fixed. AES is of a symmetric encryption, and decryption is similar to the encryption process, but in reverse direction. In the method, sensor nodes A and B first negotiate a session key for ECC algorithm. Second, the communication initiator (sensor node A) uses an ECC algorithm which is mainly designed for encrypting a random number generated in the sensor node A to consult a key for AES algorithm, and then sends the cipher to sensor node B. The sensor node B obtains a random number by ECC decryption. Subsequently, the sensor node A uses ECC to encrypt plaintext and primary ciphertext is then obtained, which is further encrypted using AES algorithm. Finally, at the receiver side, the ciphertext is first decrypted by AES decryptor, and then decrypted by ECC decryptor, and the plaintext is obtained.

Although the existing ECC_AES scheme is pretty secure, the whole process is complicated and time-consuming. As wireless sensor nodes possess the inherent limitations of sensor battery and CPU power, the practical application of this scheme is limited. The increase in the elapsed time of finishing this complicated scheme has a negative effect on the quality of real-time communication.

So in this study, we devoted to improve key management and information security for WSN by proposing a more reliable, speedy, and secure cryptographic scheme.

III. PROPOSED CHAOTIC STREAM CIPHER-BASED CRYPTOGRAPHIC SCHEME

In this section, at first, we describe a logistic chaotic algorithm briefly. Subsequently, we detail our proposed chaotic stream cipher-based cryptographic algorithm for Wireless Sensor Network.

A. Logistic Chaotic Algorithm

A wide range of ciphers are included in the chaotic stream cipher, which is a hybrid algorithm of chaotic system and stream cipher. Chaotic system is an important subdiscipline of nonlinear science, which includes a unidimensional Logistic map, bidimensional Duffing equation and Henon chaotic system, three-dimensional Lorenz system, Chua’s system and CLHE hyperchaos system, four-dimensional Rössler hyperchaos system, etc.

Chaotic systems can be roughly classified into two types: chaos and hyperchaos. The essential difference between chaos and hyperchaos lies in the number of positive Lyapunov exponents associated with them. There is a positive exponent in a dynamical system, which is usually taken as an indication that the system is chaotic. A chaotic system with at least two positive Lyapunov exponents is typically defined as hyperchaos.

In mathematics the Lyapunov exponent of a dynamical system is a quantity that characterizes the rate of separation of infinitesimally close trajectories. In a dynamical system, there is a spectrum of Lyapunov exponents - equal in number to the dimensionality of the phase space, in which the more positive the Lyapunov exponent is, the more chaotic the dynamic system is. So in a hyperchaotic system, the directions of trajectories are more unstable and the pseudo-random sequences generated are more random than a chaotic system. Although the research on hyperchaotic systems is in the budding stage, with their strong chaotic characteristics they are getting well application prospects in many fields, such as secure communication [10], electronic implementation [11], chaotic neural networks, weather forecast, economics, etc.

With the newest advances in communication technology, secure communication has gained more and more attention. The emerging technology of chaotic secure communication has opened up a new approach to information secure communication. Secure communication is achieved through either masking of a weak analog message signal by adding it into a chaotic coupling signal or modulation of the parameters of the drive system by a digital message signal [10]. The early algorithms for chaotic secure communication mostly employed low-dimensional chaotic systems; however, the space of pseudo-random sequences generated is limited and its complexity is quite low. So the chaotic communication systems could not effectively resist phase space reconstruct and brute force attacks (e.g. using predictive modelling or noise reduction methods from nonlinear dynamics). The use of hyperchaos system could generate pseudo-random sequences of an ultra high degree of randomness. Meanwhile, the structure of the hyperchaos system is pretty complexity, which makes the phase space reconstruct attack on the hyperchaos communication system could be effectively reduced, meaning that hyperchaos could strengthen the security of communication process. However, there is a defect in chaos and hyperchaos systems that the speed of generating pseudo-random sequences is low, which is serious for hyperchaos due to its complexity structure. This means that use of hyperchaos will delay the communication significantly.

To meet the real-time data transmission requirement of ETC intelligent transportation network and the limitations of wireless sensors in computation and energy, we chose a straightforward logistic chaotic system rather than a hyperchaotic system. The stream cipher used is one kind of symmetric cryptography, which encrypts and decrypts plaintext or ciphertext in one or several bits. Taking performance into account, RC4 algorithm was chosen as a component of chaotic stream cipher in this study.

1)Logistic chaotic system

The logistic chaotic system [12] is one of the most popular models for discrete nonlinear dynamical systems. Its expression and computation process are straightforward. A logistic chaotic map can be described in equation of

$$X_{n+1} = \mu X_n(1-X_n), \qquad \mu\in[0,4] \quad X_n\in[0,1] \qquad (1)$$

where μ is a control parameter on the interval $[0,4]$ and X_n is a real number on the interval $[0,1]$.

Figure 3 depicts a bifurcation diagram of a logistic chaotic map. As Fig. 3 shows, when $\mu\in(0,1]$, the value of *X* is equal or close to 0. When $\mu\in(1,3]$, the value of *X* quickly approaches the value of $\mu-1/\mu$. When $3.57<\mu\le 4$, $x_0\in(0,1)$, the sequence generated by using (1) is in a chaotic status, which is similar to the probability nature of white noise, so the logistic chaotic system is a ideal way to act as a key sequence generator [13].

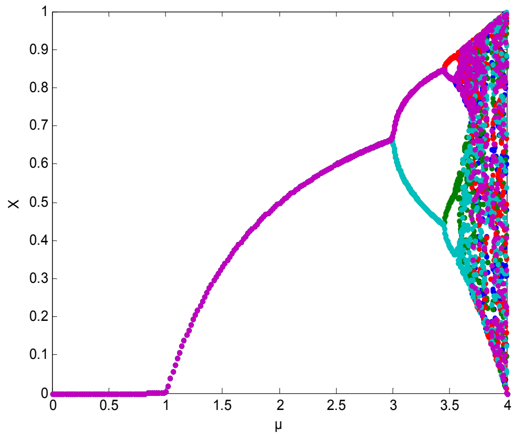


Fig. 3. Bifurcation diagram of logistic chaotic map.

In addition, the logistic chaotic system is sensitive to the initial value. Fig. 4 shows the deviations of two logistic chaotic sequences at two initial values. As Fig. 4 illustrates, when $\mu = 4$, the initial value X_0 = 0.6634890 and X_0 = 0.6634891 respectively with a scanty margin, the deviations of the two logistic chaotic sequences generated by the logistic chaotic map described by (1) is blindingly obvious. The deviations vary as the iteration n increases between (0, 80]. For the first thirty iterations, the deviations of the two logistic chaotic sequences are equal or close to zero, while the deviations are evident since then. Therefore, the act of fixing the initial element position of a key sequence at the beginning of the iteration should be avoided when the logistic chaotic map is used as a key sequence generator.

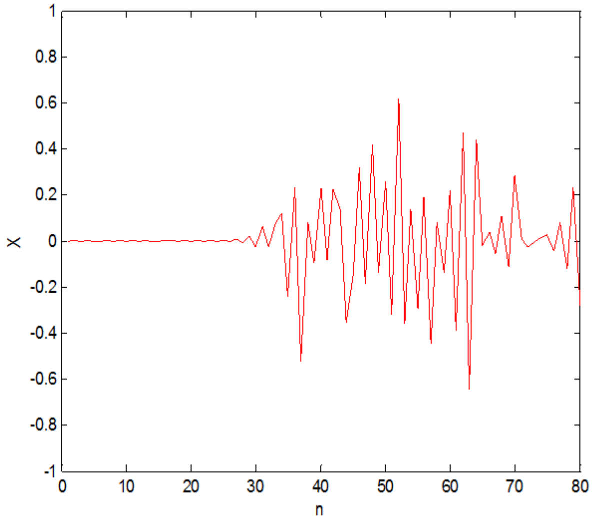


Fig. 4. Deviation of two logistic chaotic sequences (x_0 = 0.6634890, x_0 = 0.6634891).

2) RC4 encryption algorithm

The RC4 algorithm is composed of two components: Key-scheduling algorithm (KSA) and pseudo-random number generation algorithm (PRGA). RC4 is regarded as a variable key-size stream cipher based on a 256-byte secret internal state and two one-byte indexes. Information is encrypted by XORing data with the key sequence which is generated by RC4 from a seed key. For a given seed key, KSA generates an initial permutation state S. PRGA is a repeated loop procedure with each loop generating a one-byte pseudo-random output as a key stream. At each loop, a one-byte key stream is generated and XORed with one-byte of plaintext, in the mean time a new 256-byte permutation state S as well as two one-byte indexes i and j are updated, which are defined by

$$\left(S_{k+1}, i_{k+1}, j_{k+1}\right) = PRGA\left(S_k, i_k, j_k\right)$$

where i_{k+1} and j_{k+1} are the indexes, and s_{k+1} is the state updated from i_k, j_k and s_k by applying one loop of PRGA.

Since RC4 is probably the most widely used stream cipher nowadays due to its high efficiency and simplicity, attacks on RC4 have gathered pace in recent years. The attacks can be mainly classified into three types [14-17]: week key attacks, force attacks, and related key attacks. The primary method of enhancing the anti-attack ability of RC4 is to improve the complexity and randomicity of key sequences. To address this problem, we proposed to use the logistic chaotic RC4 algorithm below.

3)Logistic chaotic RC4 algorithm

Logistic chaotic RC4 algorithm is made of a logistic chaotic algorithm and a RC4 stream cipher. To explore the advantages of RC4 and to improve the randomicity of the pseudo–random number generated by pseudo-random number generation algorithm in RC4, we in this study designed a new scheme by embedding a logistic chaotic system into the PRSA component of RC4 algorithm without modifying the KSA algorithm of RC4. The function of KSA in RC4 is to complete initialization of RC4 key, while the function of PRSA is to produce a pseudo-random number. Fig. 5 shows the comparison of the pseudo codes of PRGA in RC4 algorithm and Logistic chaotic RC4 algorithm.

```
i = 0, j = 0
while(true)
    i= (i+1) mod 256
    j= (j+S[i]) mod 256
    Swap(S[i], S[j])
    T = (S[i]+S[i]) mod 256
    K = S[t]
```

(a)

```
i = 0, j = 0
while(true)
    i = (i+1) mod 256
    $X_{n+1} = X_n(1-X_n)$
    $X_n = X_{n+1}$
    j= (j+S[j]+$X_{n+1}$*256) mod 256
    Swap(S[i],S[j])
    T = (S[i]+S[j]) mod 256
    K = S[t]
```

(b)

Fig. 5. Pseudo codes of PRGA. (a) In RC4 algorithm; (b) In the proposed logistic chaotic RC4 algorithm.

B. Chaotic Stream Cipher-Based Cryptographic Scheme

The proposed chaotic stream cipher-based cryptographic scheme not only possesses the inherent advantages of symmetric cipher but also settles the problem of key management.

The proposed scheme includes four stages: regional division, the initialization of sensor nodes, the creation of session key and data encryption, and key updating.

1)Regional division

Regional division of the deployment area of sensor nodes is dominant for key management, and so it needs to pick up an appropriate division method firstly. According to the mosaic principle (2), it is possible to judge which polygon can connect seamlessly and cover the whole WSN area.

$$(n-2)*180/360 \qquad (2)$$

where the parameter *n* represents the number of edges in a polygon. When the result of (2) is an integer, the corresponding polygon can realize a seamless connection, and vice versa. Regular hexagon is an optimum in dividing the WSN area due to every vertex having the least adjacent domains, which means that the critical sensor nodes can prestore less information of the adjacent domains.

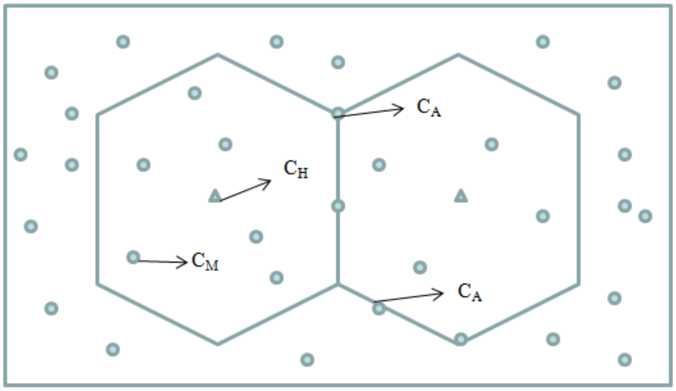


Fig. 6. Regional division of WSN area.

Assuming that the base station is an unconditionally trusted entity, which manages keys for sensor nodes in WSN. The base station sends flooding broadcast to the whole WSN, and then collects the information including the number and location of sensor nodes. Subsequently, the base station divides the WSN area in the form of regular hexagon. Fig. 6 depicts the specific regional division of WSN area, in which $C_{H,}$ C_M and C_A represent the cluster head, member node, and critical node, respectively. After the initialization of sensor nodes, it creates session keys which confidentially communicate with others.

2)Initialization of sensor nodes

The sensor nodes deployed in ETC lanes can be divided into three types after the regional division. The initialization processes vary for different types of wireless sensor nodes.

a) C_H: It is the cluster head of every partition, which is used to manage the whole non C_H sensor nodes within a partition. Each cluster head needs to be loaded the information: the identity id_x assigned by the base station which has an Identity Repository (IR) used to restore the identities of all cluster heads. In addition, it also needs to prestore two sets of keys $\{x_B, \mu_B\}$ and $\{x_R, \mu_R\}$. One is a shared key with the base station, which includes the initial value $x_0 = x_B$ and the control parameter $\mu_0 = \mu_B$ of logistic chaotic system. The other one is a shared key with all non cluster head nodes within a partition, which includes the initial value $x_0 = x_R$ and the control parameter $\mu_0 = \mu_R$ of logistic chaotic system.

b) C_A: There are three adjacent domains at the most for every critical sensor node according to the above regional division method. Thus, C_A needs to prestore two or three pairs of keys $\{x_R, \mu_R\}$ shared with every adjacent domain.

c) C_M: It is a general member sensor node that only needs to prestore a pair of keys $\{x_R, \mu_R\}$ shared with the partition domain to which C_M belongs.

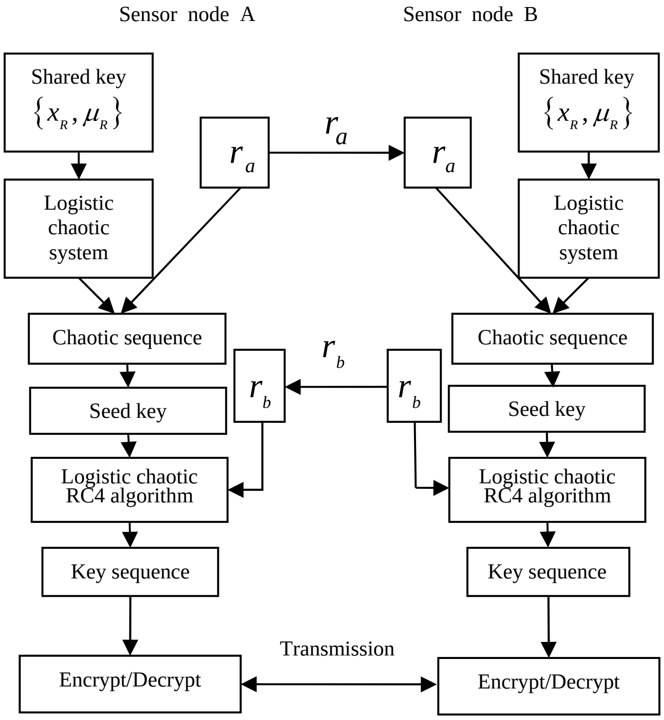


Fig. 7.   Creation of session key and data encryption.

3)Creation of session key and data encryption

When a wireless sensor node A wants to transmit vehicle information to a sensor node B, there are two situations according to the specific position of the sensor node B. One case is that sensor nodes A and B are in the same partition, in which they can negotiate a session key directly. The other case is that the two sides of communication are in different partitions, since both of them possess different shared keys prestored, in which the creation of session key depends on the C_A as a medium. The creation of session key is completed by sensor nodes that belong to the same partition step by step no matter which situation it is. Fig. 7 illustrates the creation process of session key and information encryption. The specific steps of using the proposed scheme are described as follows:

a) Sensor node A sends a random number r_a to sensor node B, when receiving r_a from A, B transmits a random number r_b to A.

b) Sensor nodes A and B use the logistic chaotic map (1) and key $\{x_R, \mu_R\}$ owned jointly to generate a chaotic sequence. Subsequently, sensor nodes A and B choose seed keys for Logistic chaotic RC4 algorithm. The use of the random number r_a is to determine the position of the initially selected value in the chaotic sequence and the length of the selected seed key.

c) Sensor nodes A and B employ Logistic chaotic RC4 algorithm to produce a key sequence based on the seed key, respectively. The function of the random number r_b is to decide the position of the initially selected value in the chaotic sequence generated by the imbedded logistic chaotic system in Logistic chaotic RC4 algorithm. The shared key $\{x_R, \mu_R\}$ is used by the embedded logistic chaotic system again.

d) Sensor node A encrypts and decrypts vehicle information by XORing it with the key sequence, while sensor node B decrypts and encrypts the cipher text by XORing it with the key sequence.

4)Key updating

In the proposed scheme, keys are updated within the scope of a partition instead of the whole WSN area. The key update process includes two kinds of key updating: $\{x_B, \mu_B\}$ and $\{x_R, \mu_R\}$. The C_H of each partition is responsible for the process of key update, in which the steps involved are described as follows:

a) At first, C_H sends its identity id_x and a random number r_a to the base station, and then the base station determines whether the identity id_x is legal or not by matching the value with its Identity Repository (IR). In addition, C_H also sends an indication number U_R or U_B that indicates which kind of keys is to be updated, respectively. The number U_R denotes the update of $\{x_R, \mu_R\}$ and another number U_B means the updating of $\{x_B, \mu_B\}$.

b) If the identity id_x is legal, the base station sends a random number r_b to the initiator of the communication, and then generates a pair of new keys $\{x_{NR}, \mu_{NR}\}$ or $\{x_{NB}, \mu_{NB}\}$ according to the value of indication number U_R or U_B.

c) At this time, CH and the base station have a pair of shared random numbers r_a and r_b. The base station sends the new keys to CH after the process by using the proposed scheme in the stage of the creation of session key and data encryption.

d) CH decrypts the cipher and obtains the new keys $\{x_{NR}, \mu_{NR}\}$ or $\{x_{NB}, \mu_{NB}\}$. If the update keys are the former, CH also needs to send it to all non CH sensor nodes in its partition. To protect $\{x_{NR}, \mu_{NR}\}$ from malicious attacks, CH needs to negotiate a session key with all of the non CH sensor nodes within a partition, and then to encrypt $\{x_{NR}, \mu_{NR}\}$. This process is slightly different from the above stage of session key creation and data encryption, taking into account the low battery power, limited memory space, and less processing capabilities of sensor nodes. CH first sends flooding broadcasts carrying a random number r_{C_H} to other sensor nodes in the same partition. The random number r_{C_H} acts as the functions of r_a and r_b in the stage of session key creation and data encryption. Subsequently, CH transmits the new key $\{x_{NR}, \mu_{NR}\}$ after the process by using the proposed scheme in the stage of the creation of session key and data encryption.

IV. SECURITY ANALYSIS

This section provides a security analysis of the proposed chaotic stream cipher-based cryptographic scheme used to realise secure data communications over a wireless sensor network. The use of logistic chaotic system in this study enhances key sequence randomness, thus preventing WSN from malicious attacks.

A. Dos Attacks

In the proposed scheme, the use of clustering that consists of building partitions of sensor nodes to form a logistical structure with respect to a given metric. So sensor nodes communicate directly inside a partition and use a cluster head C_H to communicate between the partitions. The workload of the base station is then reduced, i.e. it is only used in regional division and key updating. By this way, the proposed scheme can effectively withstand Dos attacks aimed at the base station.

B. Interference Attacks

Because of the application context of intelligent transportation systems, the transmitted information can be easily interfered by the perpetual noise of traffic and even other noises from the adversary. However, the proposed cryptographic scheme can resist interference attacks, because the statistical nature of the key sequence generated by the use of Logistic chaotic system in our proposed scheme is similar to the white noise's possessing anti-interference, as discussed by Wu et al [18].

C. Replay Attacks

Analysis shows the proposed scheme can resist replay attacks. In the key sequence negotiation process, only two random numbers are transmitted over the unsecure Wireless Sensor Network. Any action that an adversary attempts to deceive another wireless sensor node by reusing the intercepted random number cannot be successful because the adversary does not possess the shared key $\{x_R, \mu_R\}$, and so she or he could not obtain the key sequence.

D. Man-in-the Middle Attacks

According to the proposed scheme, the adversary is infeasible to pretend to be a sensor node to communicate with another sensor node by using the intercepted random numbers. Assuming that the adversary successfully shared two pairs of random numbers r_a and r_b with legal sensor nodes A and B, respectively, it still could not communicate with both of them. As the adversary could not decrypt the cipher coming from sensor nodes A and B, and vice versa, it does not have the prestored values $\{x_R, \mu_R\}$.

E. Session Key Security

In case a wireless sensor node wants to transmit vehicle information to another sensor node, it can obtain a session key sequence by using the proposed scheme, which is fairly secure. First, the negotiated session key sequence is not known to the third party but only to the two communicating wireless sensors. Second, it possesses a better pseudorandom owing to the use of Logistic chaotic system in the proposed scheme, which prevents the adversary from launching ciphertext-only attacks.

V. EXPERIMENTAL RESULTS AND DISCUSSION

To evaluate the efficiency and availability of the proposed chaotic stream cipher-based cryptographic scheme, we set up experiments simulating WSN in a real environment.

The communications between sensor nodes were implemented with the proposed scheme, and the associated encryption algorithm functions were supported by the OpenSSL cryptographic library. In our experiments, we measured the elapsed times of session key negotiation and data encryption using the proposed scheme, and then compared the experimental results with the results obtained from the experiments using the existing ECC_AES scheme.

Fig. 8 illustrates the experimental environment / setup for performance measurements. As Fig. 8 shows, the communication between senor nodes A and B was based on our proposed scheme, while the communication between sensor nodes A* and B* was based on the existing ECC_AES scheme [8].

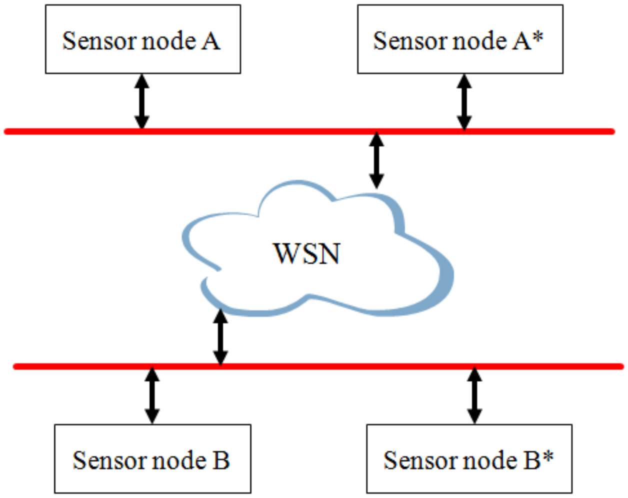
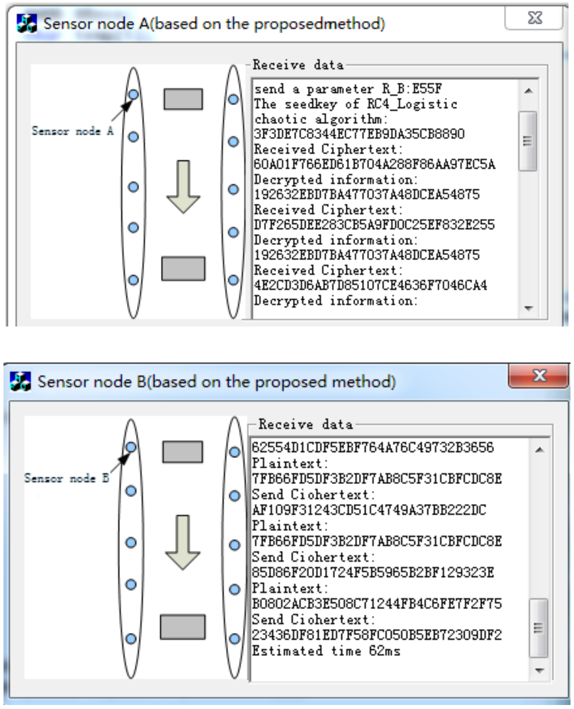


Fig. 8. Experimental setup.

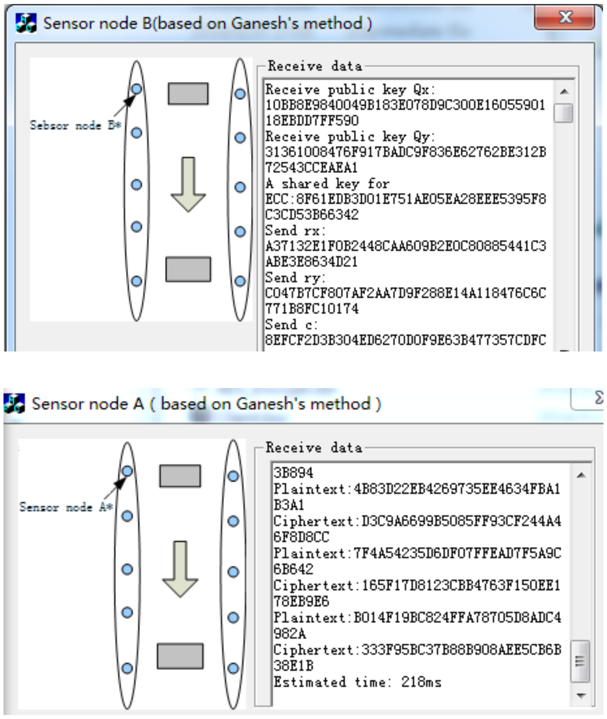
The processes of session key negotiation and data encryption are illustrated in Fig. 9 and Fig. 10. Figures 9 and 10 were based on our proposed scheme and the existing ECC_AES scheme, respectively. For comparing the elapsed times, the two schemes encrypted information with the same length. With regard to the elapsed time of finishing one round session key creation and data encryption, each run obtained a slightly different result. As shown in Figs 9 and 10, the elapsed times were measured to be 62 ms and 218 ms for the proposed scheme and the existing ECC_AES scheme, respectively.


Sensor node A(based on the proposedmethod)
Sensor node A
Receive data
Sensor node B(based on the proposed method)
Sensor node B
Receive data

```
send a parameter R_B:E55F
The seedkey of RC4_Logistic
chaotic algorithm:
3F3DE7C8344EC77EB9DA35CB8890
Received Ciphertext:
60A01F766ED61B704A288F86AA97EC5A
Decrypted information:
192632EBD7BA477037A48DCEA54875
Received Ciphertext:
D7F265DEE283CB5A9FD0C25EF832E255
Decrypted information:
192632EBD7BA477037A48DCEA54875
Received Ciphertext:
4E2CD3D6AB7D85107CE4636F7046CA4
Decrypted information:
```

```
62554D1CDF5EBF764A76C49732B3656
Plaintext:
7FB66FD5DF3B2DF7AB8C5F31CBFCDC8E
Send Ciohertext:
AF109F31243CD51C4749A37BB222DC
Plaintext:
7FB66FD5DF3B2DF7AB8C5F31CBFCDC8E
Send Ciohertext:
85D86F20D1724F5B5965B2BF129323E
Plaintext:
B0802ACB3E508C71244FB4C6FE7F2F75
Send Ciohertext:
23436DF81ED7F58FC050B5EB72309DF2
Estimated time 62ms
```

Fig. 9. Key negotiation and data encryption using the proposed scheme.



```
Receive public key Qx:
10BB8E9840049B183E078D9C300E16055901
18EBDD7FF590
Receive public key Qy:
31361008476F917BADC9F836E62762BE312B
72543CCEAEA1
A shared key for
ECC:8F61EDB3D01E751AE05EA28EEE5395F8
C3CD53B66342
Send rx:
A37132E1F0B2448CAA609B2E0C80885441C3
ABE3E8634D21
Send ry:
C047B7CF807AF2AA7D9F288E14A118476C6C
771B8FC10174
Send c:
8EFCF2D3B304ED6270D0F9E63B477357CDFC
```

```
3B894
Plaintext:4B83D22EB4269735EE4634FBA1
B3A1
Ciphertext:D3C9A6699B5085FF93CF244A4
6F8D8CC
Plaintext:7F4A54235D6DF07FFEAD7F5A9C
6B642
Ciphertext:165F17D8123CBB4763F150EE1
78EB9E6
Plaintext:B014F19BC824FFA78705D8ADC4
982A
Ciphertext:333F95BC37B88B908AEE5CB6B
38E1B
Estimated time: 218ms
```

Fig. 10. Key negotiation and data encryption using the ECC_AES scheme.

After 40 times repeated tests, we obtained the elapsed times of finishing one round session key creation and data encryption for the proposed scheme and the existing ECC_AES scheme, respectively, and the results are listed in TABLE I.

TABLE I

ELAPSED TIME OF COMPLETING ONE ROUND

Round	Elapsed time (ms)	
	ECC_AES scheme	Proposed scheme

R=1	220	78
R=2	230	78
R=3	201	78
R=4	230	62
R=5	210	94
R=6	230	94
R=7	210	62
R=8	210	63
R=9	210	93
R=10	231	62
R=15	210	63
R=20	210	78
R=25	211	62
R=30	210	62
R=35	230	62
R=40	210	78

Close analysis of the results listed in the table, the average elapsed time for finishing one round of our proposed scheme and the ECC_AES scheme are 70.53 ms and 214.58 ms, respectively. It is obvious that our proposed scheme is more time saving compared with the existing scheme. Since intelligent transportation networks have a strict requirement in real-time data transmission, Wireless Sensor Network as a component of ITS network should also meet the real-time data transmission requirement. Taking into account the experimental results, the elapsed times for finishing one round with our proposed scheme were much shorter than the existing ECC_AES scheme. In other words, our proposed chaotic stream cipher-based cryptographic scheme could realise secure data communications over a wireless sensor network without compromising the real-time data communications over Intelligent Transportation Systems.

Figure 11 shows the average elapsed times and standard deviations for finishing one round of our proposed cryptographic scheme based on Logistic chaotic RC4 encryption / decryption algorithm, and the ECC_AES scheme, respectively. As the results show, the proposed cryptographic scheme reduced the average elapsed time up to 67% in comparison with the existing ECC_AES scheme, indicating that the proposed scheme is remarkably effective in terms of security and performance.

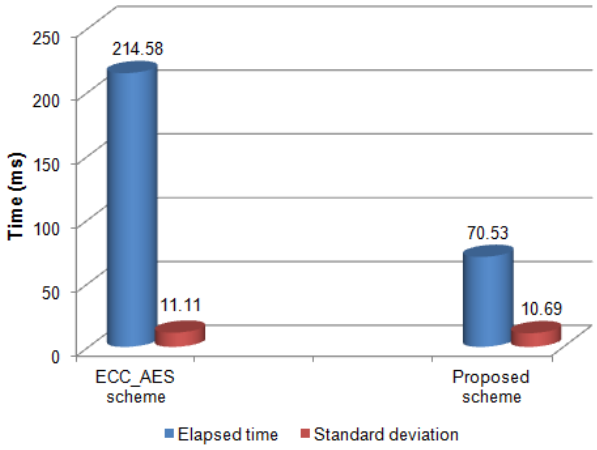


Fig. 11. Average elapsed times and standard deviations for finishing one round of each scheme.

VI. CONCLUSIONS

In this study, we suggested a new chaotic stream cipher-based cryptographic scheme to achieve secure data communications over a wireless sensor network for Intelligent Transportation Systems. The proposed cryptographic scheme not only provided key negotiation and data encryption between sensor nodes in the WSN, but also reduced computational costs and power consumption. Security analysis indicated that the proposed scheme could protect data transmission between wireless sensor nodes from malicious attacks, such as Dos attacks, Interference attacks, Replay attacks, and Man-in-the middle attacks. Experimental results showed that, in comparison with the existing ECC_AES scheme, the proposed scheme reduced the average elapsed time (the communication overhead) up to 67%, thus meeting the real-time data transmission requirement of ITS.

Further experiments should investigate how the steganography technology could be applied to ITS so as to improve data communications security further on the basis of the proposed scheme.

ACKNOWLEDGMENT

This work was supported in part by the National Natural Science Foundation of China under Grant 61272469, and Grant 61303237, and the Wuhan Scientific Research Program under Grant 2013010501010144.

REFERENCES

[1] World Road Association, "ITS Handbook," http://road-network-operations.piarc.org/index.php?option=com_content&task=view&id=38&Itemid=71&lang=en

[2] G. Dimitrakopoulos and P. Demestichas, "Intelligent transportation systems," Vehicular Technology Magazine, IEEE, vol. 5(1), pp. 77-84, 2010.

[3] F. Don, "Electronic Toll Collection: An Introduction and Brief Look at Potential Vulnerabilities," SANS Institute infoSec Reading Room, 1.

[4] H. Ning, N. Ning, S. Qu, et al., "Layered structure and management in internet of things," Future Generation Communication and Networking (FGCN 2007), IEEE, vol. 2, pp. 386-389, 2007.

[5] R. Bera, J. Bera, S. Sil, et al., "Dedicated short range communications (DSRC) for intelligent transport system," Wireless and Optical Communications Networks, 2006 IFIP International Conference on. IEEE, 2006: 5, pp. 1-5.

[6] S. Sharma, A. Sahu, A. Verma, et al., "Wireless sensor network security," Advances in Computer Science and Information Technology, Computer Science and Information Technology. Springer Berlin Heidelberg, 2012, pp. 317-326.

[7] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks", CCS'03, Washington, DC, USA, October 2003.

[8] C. Xu and Y. Ge, "The public key encryption to improve the security on wireless sensor networks," Information and Computing Science, ICIC'09. Second International Conference on. IEEE, 2009, 1, pp. 11-14.

[9] A. R. Ganesh, P. N. Manikandan, S. P. Sethu, et al, “An improved AES-ECC hybrid encryption scheme for secure communication in cooperative diversity based Wireless Sensor Networks,” Recent Trends in Information Technology (ICRTIT), 2011 International Conference on. IEEE, 2011, pp. 1209-1214.

[10] K. G. Gopchandran, K. Gopakumar, and B. Premlet, “Information Encryption and Decryption Using Hyperchaotic Systems in Delayed Nonlinear Feedback Systems,” 2010 International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 18-20 Oct. 2010, pp. 855-859, ISBN: 978-1-4244-7285-7.

[11] G. Grassi, and D. A. Miller, “Theory and Experimental Realization of Observer-Based Discrete-Time Hyperchaos Synchronization,” IEEE Transactions on Circuits and Systems—I: Fundamental theory and Applications, vol. 49, no. 3, pp. 373-378, March 2002.

[12] N. K. Pareek, V. Patidar, and K. K. Sud, “Image encryption using chaotic logistic map,” Image and Vision Computing, vol. 24(9), pp. 926-934, 2006.

[13] M. Andrecut, “Logistic map as a random number generator,” International Journal of Modern Physics B, vol. 12(09), pp. 921-930, 1998.

[14] S. Fluhrer, I. Mantin, and A. Shamir, “Weaknesses in the key scheduling algorithm of RC4,” Selected Areas in Cryptography. Springer Berlin Heidelberg, 2001, pp. 1-24.

[15] N. Couture and K. B. Kent, “The effectiveness of brute force attacks on RC4,” Communication Networks and Services Research, Proceedings, Second Annual Conference on. IEEE, 2004, pp. 333-336.

[16] A. Klein, “Attacks on the RC4 stream cipher,” Designs, Codes and Cryptography, vol. 48(3), pp. 269-286, 2008.

[17] S. Paul and B. Preneel, “A New Weakness in the RC4 Keystream Generator and an Approach to Improve the Security of the Cipher,” Fast Software Encryption. Springer Berlin Heidelberg, 2004, pp. 245-259.

[18] Z. Wu and N. E. Huang, “A study of the characteristics of white noise using the empirical mode decomposition method,” Proceedings of the Royal Society of London, Series A: Mathematical, Physical and Engineering Sciences, 2004, vol. 460(2046), pp. 1597-1611.