International Journal of Advancements in Computer Networks and Its Security– IJCNS
Volume 4 : Issue 4 [ISSN 2250-3757]
Publication Date : 27 December,2014

Security Improvement in ETC Network Using RC4−Logistic Chaotic Encryption

Wei Zhang, Qing Chen, Jia Li, Liping Zhang, Shanyu Tang

***Abstract*—Electronic Toll Collection (ETC) is a charging method in intelligent transportation systems, which transmits information over ETC network. The information is subject to eavesdropping and interfering on ETC network owing to the defects of mutual authentication standard in Dedicated Short Range Communication (DSRC) protocol, the inherent security vulnerabilities of WSN and some other problems associated with the ETC network. In order to improve information security for ETC network and ensure every toll transaction could be successfully finished, we paid more attention to Wireless Sensor Network (WSN) as a part of the whole ETC network and proposed an information protection method based on a RC4-Logistic chaotic encryption algorithm. The proposed method not only enhanced the security of WSN in key manage and information encryption, but satisfied the limitation in battery and CPU power of wireless sensor nodes. The results from our experiments demonstrated that our propose method not only provided secure ETC transaction, but met the real-time requirement of ETC network, which is vital to ETC applications. In addition, the proposed method could be applied to the rest of communication techniques in ETC network to improve the information security of the whole ETC network.**

***Keywords*—Information security, ETC network, RC4-logistic chaotic algorithm, WSN**

I. Introduction

One of the heaviest complaints of motorists using toll roads is the congestion and delay caused by stopping to pay at tollbooths. Electronic Toll Collection (ETC) improves the toll collection process by reducing speed to automatically complete toll collection and transmitting information referring to toll transaction over ETC network, which effectively accelerates the speed of toll collection, enlarges traffic capacity of toll roads and conserves energy. By virtue of those advantages, ETC system is gaining widespread use throughout our country and even the world. ETC has already become a main development direction of Intelligent Transportation System (ITS) [1], and the Internet of Things.

ETC is generally divided up into three parts [2]: automatic vehicle identification (AVI), automatic vehicle classification (AVC), and violation enforcement (VE). The three parts complete toll transaction through deliberate cooperation.

Wei Zhang, Qing Chen, Jia Li, Liping Zhang, Shanyu Tang
China University of Geosciences
P. R. China

The AVI component of the ETC system consists of On Board Unit (OBU), Road Side Unit (RSU), and Dedicated Short Range Communication (DSRC) protocol. OBU is located in the windscreen of automobile, and RSU is deployed at the toll gantry. The main components, OBU and RSU authenticate and communicate with each other by using the DSRC protocol.

Automatic classification of the vehicle is important for the whole toll transaction in which the fare is dependent on the number of axles on the vehicle and other ingredients of the vehicle. Wireless sensors are embedded in the ETC lanes to apperceive the related information of the vehicle. Such sensors use the latest technologies including treadles, magnetic induction loops, and laser imaging.

Violation enforcement gathers information from the vehicle whose owner violate ETC system to allow authorities to persecute the vehicle owner.

In an ETC system, information is transmitted over ETC network, which includes many communication techniques. ETC network is a derivative of the Internet of Things [3], which can be divided into four layers depending on its functions.

In an Electronic Toll Collection network, there are the communications between On Board Unit and Road Side Unit using DSRC technology[4], the information transmission among sensors using Wireless Sensor Network (WSN) technique, and the information exchanges between RSU and the center of settling account based on Wireless Local Area Network (WLAN) and so on. In order to improve information security for ETC network and ensure every toll transaction can be successfully finished, more attention should be paid to WSN as a part of the whole ETC network, which is the main motivation of this study.

There are lots of wireless sensors deployed at Electronic Toll Collection lanes which constitute Wireless Sensor Network [5] by means of self-organization. Those wireless sensor nodes apperceive, dispose and transmit information about the driving vehicle in ETC lanes. At the same time, they also store, manage and fuse information which is retransmitted by other sensor nodes. Then the above information is converged on a sink node and forwarded to the processing center through exterior network. Depending on the received information, the processing center determines how much money should be deducted from the vehicle owner's Intelligent Card.

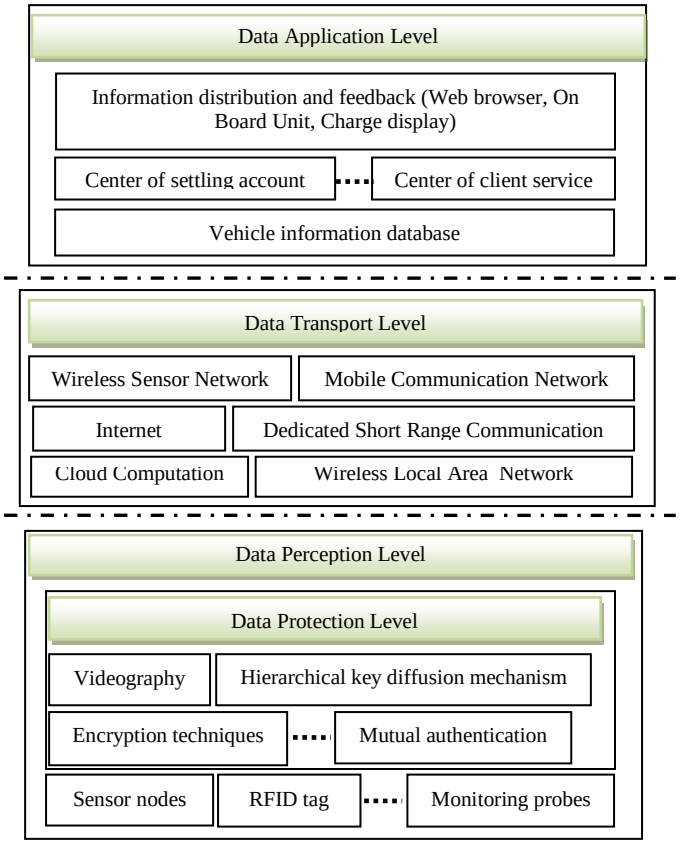

Figure 1. Four layers of ETC network.

With the popularization of ETC, numerous information security issues have surfaced [2]. Transmitted data packets over ETC network which carry private and valuable information are subject to eavesdrop, tamper, and decode by adversaries owing to ETC network composed of many traditional communication technologies. Such as WSN is deployed in ETC lanes, the inherent vulnerabilities of WSN could compromise the whole secure performances of ETC network. In addition, the related Dedicated Short Range Communication (DSRC) protocol is applied to connect OBU and RSU owning some defects, which include bypass interference and car-following interference. Under this circumstance, enhancing information security for ETC network is urgent.

In order to improve information security for ETC network, we focused on creating a safe environment for WSN to protect the information about related driving vehicles in the ETC lane from being eavesdropped, or tampered. Encryption techniques and key management are central for the security of WSN. There has been extensive literature in researching WSN security, which can divide them into two categories. One lays stress on symmetric encryption. Although existing symmetric encryption schemes provide a good amount of security, keys maintenance is difficult. The other one emphasizes on asymmetric schemes. When asymmetric schemes are used, keys management is easier, but they provide a lower level of security compared to the former. In this study, we proposed a method using symmetric cipher as well as settling the problem of key management.

The rest of this paper is organized as follows: the second section discusses the related research work about WSN security protection. Our proposed method and its security analysis are described in the third section and the fourth section in detail. The experimental results and performance of the proposed method are shown in the fifth section. Finally, a conclusion of the paper is given in the final section.

II. Related Work

Currently the security in Wireless Sensor Network (WSN) is provided mostly through symmetric key cryptography [6]. These protection methods are based on the idea that keys are prestored before the deployment of the wireless sensor network. However, these methods are not able to achieve good security due to the limitation on memory resources of wireless sensor nodes, and also face a key management problem in large scale wireless sensor networks.

Xu et al. [7] tried to solve the problem of information security in WSN by the use of asymmetric encryption algorithm RSA. There are two phrases in their method: the first is a sensor node to shakehand with another sensor node in which the two sensor nodes setup a session key. The second phrase is the use of this session key for data encryption. However their proposed method is not practical, since under the assumption that the nature of the sensor node could not support asymmetric encryption algorithm due to the limitation in battery and CPU power. In addition, the low encryption speed of public key algorithm does not satisfy the requirement of real-time, which is vital to WSN and ETC system.

As mentioned above, both symmetric and asymmetric encryption algorithms all have shortcomings. In order to cope up with those shortcomings, Ganesh et al. [8] proposed an information protection method for WSN, which is a combination of Elliptical Curve Cryptography (ECC) with Advanced Encryption Standards (AES). The equation of standard Elliptic Curve is $y^2 = x^3 + ax + b(a, b \in F_q)$, and the value of a and b is fixed. AES is of a symmetric encryption, and decryption is similar to the encryption process, but in the reverse direction. In their scheme, first sensor nodes A and B negotiate a shared key for ECC algorithm. Second, the communication initiator sensor node A employs ECC algorithm which is mainly used for encrypting a random number generated in the sensor node A to consult a key for AES algorithm and then sends the cipher to the sensor node B. The sensor node B obtains a random number by ECC decryption. Subsequently, the sensor node A use ECC to encrypt plaintext and primary ciphertext is then obtained, which is further encrypted using AES algorithm. Finally, in the receiver side, the ciphertext is first decrypted by AES decryptor, and then decrypted by ECC decryptor and, the plaintext is obtained. Ganesh et al.'s method is pretty secure, but the process is complicated. The availability of this method is a problem due to wireless sensor node possessing the inherent limitations of battery and CPU power. In addition, the quality of real-time is vital to WSN and ETC system. So in

this study, we devoted to improve information security for WSN by proposing a more available and secure method.

III. Proposed Information Protection Method

In this section, we introduce our information protection method for WSN based on a RC4-Logistic chaotic encryption algorithm for WSN in detail.

A. *RC4-Logistic Chaotic Encryption*

1) Logistic chaotic system [9] is a chaotic sequence generator with widespread application. Its expression is simple and the computation process is straightforward. The expression is shown as follows:

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

where μ is a control parameter on the interval $[0,4]$ and X_n is a real number on the internal $[0,1]$. When $3.57 \le \mu \le 4$, $x_0 \in (0,1)$, the sequence generated by using (1) is in the chaotic status, which is similar to the probability nature of white noise, so logistic chaotic system is a ideal way to act as a key sequence generator [10].

2) RC4 algorithm consists of two components: Key-scheduling algorithm (KSA) and pseudo-random number generation algorithm (PRGA). RC4 is a variable key-size stream cipher based on a 256-byte secret internal state and two one-byte indexes. The 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 and each loop generates a one-byte pseudo-random output as a key stream. At each loop, a one-byte key stream is generated and it is XORed with one-byte of the 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 $(S_{k+1}, i_{k+1}, j_{k+1}) = PRGA(S_k, i_k, j_k)$, 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 PSGA.

Although RC4 is probably the most widely used stream cipher nowadays due to its high efficiency and simplicity, the attack on RC4 is also a hot research point. The attack can be mainly divided into three types [11-14]: week key attack, force attack, and related key attack. The primary method of enhancing the anti-attack ability of RC4 is to improve the randomness of key sequence. To address this problem, we proposed the method below.

3) RC4-Logistic chaotic algorithm consists of a Logistic chaotic algorithm and a RC4 stream cipher. In order to use its advantages and improve the randomness of the pseudo–random number generated by PRGA, we proposed to embed a logistic chaotic system into the PRSA component of RC4 algorithm, while KSA remained unchanged. The function of KSA is to complete initialization of RC4 key, while the function of PRSA is to produce a pseudo-random number.

The pseudo code for the proposed RC4-logistic chaotic algorithm is shown below.

```
KSA
begin
i=0, j=0
for i=0 to 255
    S[i]=i
    T[i]=K[i mod seedkeylen ]
for i=0 to 255
    j=(j+S[i]+T[j]) mod 256
    Swap(S[i],S[j])
end

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

B. *Protection method framework*

We proposed the protection method based on RC4-Logistic chaotic stream cipher, which not only possess the inherent advantages of symmetric cipher but settles the problem of key management.

In our proposed method, each wireless sensor only needs to prestore two keys. One is a shared key with the base station, which includes the initial value $x_0 = x_B$ and control parameter $\mu_0 = \mu_B$ of logistic chaotic system. The other one is a shared key with the rest of sensors, which includes the initial value $x_0 = x_R$ and the control parameter $\mu_0 = \mu_R$ of logistic chaotic system. When wireless sensor node A wants to transmit vehicle information to a sensor node B, the steps of using the proposed method are described as follows.

1) 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.

2) A and B use (1) to generate a chaotic sequence by using the shared key $\{x_R, \mu_R\}$. Subsequently, A and B choose seed keys for RC4-Logistic chaotic algorithm. The function of the random number r_a is to decide the position of the initially selected value in the chaotic sequence and the length of the selected seed key.

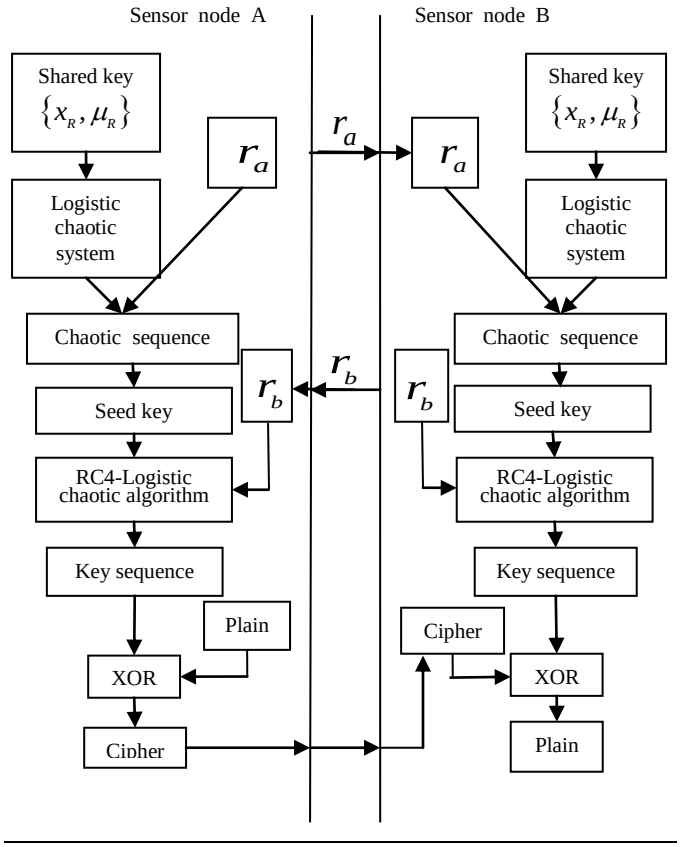

Figure 2. Illustration of our protection method for WSN based on RC4-Logistic algorithm.

3) A and B employ RC4-Logistic chaotic 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 RC4-Logistic chaotic algorithm. The shared key $\{x_R, \mu_R\}$ is used by the embedded logistic chaotic system again.

4) A encrypts vehicle information by XORing it with the key sequence, while B decrypts the cipher text by XORing it with the key sequence.

IV. Security Analysis

This section provides a security analysis of our proposed information protection method for Wireless Sensor Network.

A. *Interference attacks*

Due to the application context of ETC system, the transmittal information is easily interfered by the perpetual noise of traffic and even other noises from the adversary. However, the proposed information protection method can resist interference attacks, since the statistical nature of the key sequence generated by the use of Logistic chaotic system in our proposed method is similar to the white noise's possessing anti-interference [15].

B. *Replay attacks*

The proposed method can resist replay attacks. In the key sequence negotiation process, only two random numbers are transmitted over the unsecure WSN. Any action which an adversary attempts to deceive another wireless sensor node by reusing the intercepted random number will fail since the adversary does not possess the shared key $\{x_R, \mu_R\}$, and so she/he could not get key sequence.

C. *Man-in-the middle attacks*

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

D. *Session Key Security*

When a wireless sensor node wants to transmit vehicle information to another sensor node, they can get a session key sequence by using our proposed method, which is fairly secure. Firstly, the negotiated session key sequence is not known to the third party but only to the two communicating sensors. Secondly, it possesses a better pseudorandom due to the use of Logistic chaotic system in our method, which protects the adversary from **ciphertext-only attacks.**

V. Experimental Results

We evaluated the availability and efficiency of our proposed information protection for WSN in real experiments. We implemented the communication with our proposed information protection method, and the related encryption algorithm functions were supported by the OpenSSL cryptographic library. In our experiment, we tested the total time of key negotiation and encryption, and then compared the experimental results with Ganesh et al.'s results [8].

After 40 times repeated tests, we obtained the experimental results, which are diagramed in Fig. 3. As shown in Fig. 3, the mean elapsed times for finishing one time of our proposed method and Ganesh's method are about 70 ms and 240 ms, respectively. It is obvious that our protection method is more time saving compared with Ganesh's. Due to the application context of ETC network which has a strict requirement in real-time, WSN as a component of ETC network also needs to meet this requirement. According to our experimental results, the elapsed time for finishing our protection method is much shorter than Ganesh's method. In other words, our method can protect the vehicle information transmitted between sensor nodes in WSN without affecting the quality of real-time communication.

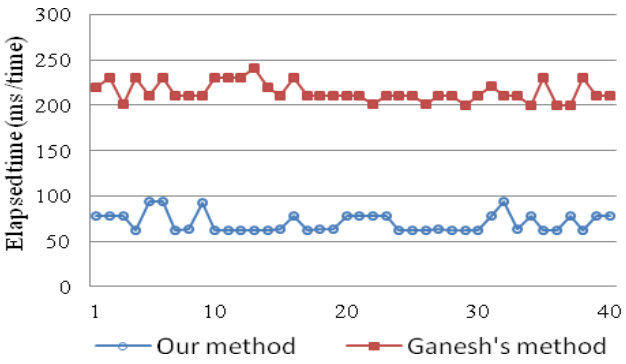

Figure 3. Elapsed times of finishing one time of each method.

VI. Conclusion

In this paper, we briefly introduced the operational principle of ETC system and the components of ETC network. To improve information security for ETC network, we paid more attention to WSN as a part of the whole ETC network and proposed an information protection method based on RC4-Logistic chaotic encryption algorithm. The proposed method not only enhanced the security of WSN in key manage and information encryption, but satisfied the limitation in battery and CPU power of wireless sensor nodes. In addition, the use of logistic chaotic system enhanced key sequence randomness and prevented WSN from interference attacks. Our experimental tests and results analysis showed that the key sequence consulting time and encryption latency are much shorter than other ways, thus meeting the requirement of real-time of ETC network. Therefore, our proposed information protection method can be applied to WSN and even the other parts of ETC network.

Acknowledgment

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.

References

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

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

[3] 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.

[4] 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.

[5] 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.

[6] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," Security and Privacy, Proceedings, 2003 Symposium on. IEEE, 2003, pp. 197-213.

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

[8] 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.

[9] 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.

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

[11] 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.

[12] 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.

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

[14] 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.

[15] 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.

About Author (s):

Wei Zhang received the BSc degree in information security from China University of Geosciences in 2014. Zhang is with China University of Geosciences, 388 Lumo Road, Wuhan 430074, P. R. China. She is currently a postgraduate research student in information security. Her research interests include covert communications, authentication, and multimedia security.

Qing Chen received the BSc degree in information security from China University of Geosciences in 2013. He is currently a master student in information security at CUG. His research interest is information hiding.

Jia Li is with China University of Geosciences (CUG), 388 Lumo Road, Wuhan 430074, P. R. China. She majored in information management and education. She had studied and worked in the United Kingdom before she joined CUG in 2012. Her research interests include information management, and digital media.

Liping Zhang received the Ph.D. degree in information security from Huazhong University of Science and Technology in 2009. Dr Zhang is currently with China University of Geosciences, 388 Lumo Road, Wuhan 430074, P. R. China. She is an associate professor in information and network security. Her research interests include key management, VoIP, and network security. She has published over 30 research papers, most of which are refereed journal papers including IET journal papers indexed by SCI. Dr Zhang is the principal grant holder of three externally funded research projects.

Shanyu Tang (A'08–M'08–SM'10) received the Ph.D. degree from Imperial College London, United Kingdom in 1995. He is Distinguished Professor at China University of Geosciences, and Visiting Professor at University of Salford (UK, 2013). He is dedicated to adventurous research in fractal computing methods for covert communications, network security, and bio-informatics. Dr Tang is the principal grant holder of seven externally funded research projects including three grants from the UK government. He has contributed to 81 scientific publications—41 refereed journal papers including IEEE TRANSACTIONS and IET journal papers.