

Learning an video-based message sharing system for large-scale smart vehicles

Hu Zhen-tao¹ · Zepeng Wang²  · Peng Shu³ · Xinyu Xiang⁴

Received: 19 December 2017 / Revised: 6 February 2018 / Accepted: 8 February 2018
© Springer Science+Business Media, LLC, part of Springer Nature 2018

Abstract With the miniaturization of communication devices, the demand for hours is low power and low cost communications. Therefore, a communication system is designed which allows the device to exchange data using the environment RF as the only signal source. This design avoids the expensive process of generating radio waves. Environmental backscatter communication is more energy efficient than existing radio communication. This approach utilizes existing environmental Wi-Fi signals to eliminate the demand for wires and batteries, thereby contributing to ubiquitous communication. The device can even communicate previously where it cannot be accessed because it cannot provide a dedicated infrastructure. In this paper, a secure environment for backscatter communications, which enables intelligent vehicles to automatically enter a secure building is proposed and simulated.

Keywords Video · Message sharing · Smart vehicles

1 Introduction

The hour's needs are to save energy and protect the environment. This should be considered in the design of communication systems. Since the size of the devices used in communications is decreasing, the provision of power to these devices is an important issue. Large wires are not feasible, batteries are bulky and increase maintenance costs. But, if we use battery free communications, all of these shortcomings can be addressed. Battery free communication is

✉ Zepeng Wang
1422617933@qq.com

¹ College of Computer and Information Engineering, Henan University, Kaifeng, China

² Department of CSIE, Hefei University of Technology, Hefei, China

³ State Grid Zhejiang Electric Power Research Institute, Hangzhou, China

⁴ State Grid Hangzhou Power Supply Company, Hangzhou, China

achieved by energy harvesting. Radio frequency energy harvesting involves capturing free flow of radio frequency energy of interest and converting the energy into a DC voltage. Ambient RF energy is provided by the use of antennas by matching the inputs of network RF-DC converters. The energy converter converts the captured radio frequency energy to a DC voltage. The module can be used as an AC DC converter, not only for AC signals but also for DC voltage levels. The output voltage obtained from the energy conversion module can be used to power the electronic device [1]. The generation of radio frequency signals will only bring more electromagnetic waves to the environment, and increase environmental pollution. As a result, we communicate using existing environmental signals. The energy obtained from environmental radio signals makes wireless sensor networks not only environmentally friendly but also self - sustaining [5]. As a result, energy harvesting can also be used in conjunction with our environment reverse scattering communication system. The available radio frequency signals near mobile towers, TV towers or Wi - Fi routers provide the opportunity to communicate with these signals and gain environmental RF energy [4].

Vehicular Ad Hoc network (VANET) is an infrastructure network. These networks communicate using Bluetooth, Wi-Fi, or WiMax. The application of vehicular ad hoc networks is safe, comfortable and secure [14].

- 1) comfortable applications: this type of application improves passenger comfort and traffic efficiency. Examples of this include weather information, restaurant location information, Internet access, or music downloads.
- 2) security applications: this type of application is used to improve the safety of drivers and passengers by sending security related information [12].

In vehicular ad hoc networks, we have chosen an application, namely access control, to demonstrate the concept of environmental backscatter communications [2]. Now we talk about access control as a system that allows or refuses to enter the commercial, industrial, or governmental structure [3]. The requirement of security in access control affects the operation of network [10]. In communication, data is kept secret in the network. Encryption techniques are used to provide confidentiality. Data confidentiality is the most important issue in network security. Data confidentiality means that data exchange between the sender and receiver is secure, and no third person can access it (neither reading nor writing). Confidentiality can be achieved by using encryption: symmetric key or asymmetric key. Therefore, the data exchange between the intelligent vehicle and the access control system must be guaranteed.

For transmission and reception, we use the method known as backscatter [7]. In backscatter communication, equipment is reflected by the modulation of incident RF signal environment rather than by producing electromagnetic wave communication. In this way, messages are sent to the receiver. The receiver can extract the message and decode it. This is possible because the modulation signal frequency is lower than the ambient Wi-Fi signal.

2 Related works

Liu et al. (5) explained the basic concept of reverse communication using TV signals and its applications in smart cards and grocery stores. The Associated Press samples and others [11] introduced the wireless identification and sensing platform. It is a programmable, battery free sensing and computing platform designed to explore the combination of radio frequency

identification (RFID) applications with sensor enhanced operations. It uses the power sent from the remote (UHF) RFID reader.

S., Yousefi, et al. [14] describe the challenges of vehicular Ad Hoc networks. The authors also outline the application of security and comfort in VANET. S., Hattori, etc. [3] present a dynamic change based content input control mode, such as user, physical, and virtual resources for some embedded device output. The model is based on smart cards, making it possible to access smart cards in a secure space. This is a secure application that allows the vehicle to grant access to the security space based on the vehicle number.

T., Beng, Lim, et al. [5] studied the feasibility of radio frequency energy harvesting in wireless sensor networks. The environmental RF power density of GSM 900 and GSM 1800 band is measured. Y., Kawahara, et al. [4] measured the electrical field strength from the mobile communication system to demonstrate the feasibility of obtaining energy from the surrounding radio frequency signals. The authors show that the radio waves of the broadcast tower are very stable in time, but the intensity depends on the distance of the broadcast tower. M., Arrawatia, et al. [1] designed an energy harvesting system to harvest the energy of the handset signal tower in the 900 MHz band. Test results show that the 2.78v voltage has been obtained from the cell towers and the 0.87v voltage distance 10 m is obtained at distance 50 m.

Y., Liu, et al. [6] present a design scheme for digital demodulator for RFID applications. In this design, the associated operations are introduced into the demodulator to estimate the frequency of the received data and decode them. The communication technique adopts FM0 encoding, which can be used in the environment backscatter communication system to solve the interference.

The article [12] describes the design of Volvo's autopilot system that is so reliable that it can take over driving in all aspects of autonomous driving. Car sharing road and traffic conditions to achieve autonomous driving. Communication between autonomous vehicles is a potential application of environmental backscatter communication.

Yin Puzhang et al. [15] present a design of a synchronous frequency hopping communication system. The system has been validated by SIMULINK. It can be concluded that Simulink is a powerful tool for verifying wireless communication system design.

A.S.K, Pathan et al. [10] mentioned security threats in wireless sensor networks. Wireless sensor networks should ensure overall security. However, cost effectiveness and energy efficiency using this mechanism have brought significant research challenges.

Corollary: low power communication has been completed at the television frequency, i.e., 539 MHz RFID and ambient backscatter communications. However, it is illegal to use a licensed frequency band for communications in India, even if the power delivered by the communication system is very low. So we propose an atmospheric backscatter system operating at 2.4GHz (Wi-Fi frequency), which is in the ISM frequency band. The VANET vehicles are currently produced with roadside devices via Wi-Fi or Bluetooth signals. But we propose the use of backscatter environments to pay attention to environmental protection protocols. The application of communication security in VANET must be secure. However, existing backscatter systems do not use encryption. Therefore, we propose to use RSA and other encryption algorithms to protect the environment from backscatter communications. The existing energy harvesting from the ambient energy shows that the energy obtained is sufficient for low-power devices such as microcontrollers and small sensors. Therefore, the environment backscatter communication system can be driven by energy collection, thus enabling the system to maintain itself.

3 System overview

3.1 Introduction

The system consists of transmitting module and receiving module. The microcontroller is common to all modules and performs logical operations. The transmitter and receiver placed in a vehicle placed in appropriate roadside units (RSU) on the basis of the application. For communications, we use frequency in unauthorized frequency bands, such as Wi-Fi. A dipole antenna is used for sending and receiving signals on a wireless channel.

3.1.1 Emission

The transmitter module is composed of a microcontroller, a reflective radio frequency switch and a dipole communication antenna. The message is transmitted from the sensor. The sensor output is used as the microcontroller input. The microcontroller is programmed with some threshold sensors. The sensor continuously senses that if the sensor value exceeds the threshold, then the message transmission is needed [6]. Messages (depending on the application) are first encrypted to ensure secure communication.

The transmitter includes a RF switch for modulating the impedance of the communication antenna and changing the amount of signal energy reflected by the antenna. The control input signal of the switch is a zero sequence. When the input is zero, the reflected signal is negligible. When the switch input signal is 1, the two branches of the antenna are short circuited, resulting in large scattering signals. Thus, the backscattering between the switching (reflected) and non scattering (absorbing) states is communicated to the bit receiver. Thus, in general, the Wi-Fi signal (2.45, GHz) on the transmitting antenna is modulated according to the signal signal, and the reflected and non reflecting antenna states are generated by turning off and switching the RF switch.

The environment Wi-Fi signal has been modulated by the Internet data. Information from the user of the environment backscatter system modulates the modulated environmental signals. However, due to the low data rate of the backscatter system (i.e., 1 kbps), there is a clear difference between the user data and the Wi-Fi data in the environment of the internet.

3.1.2 Receiver

A dipole antenna at the receiving end receives a backscattered signal from the transmitter. The receiver comprises an average circuit, a threshold calculation circuit and a comparator. The envelope detector and the RC circuit are used to smooth / average the natural variation of the ambient Wi-Fi signal. The circuit eliminates the high frequency environment Wi-Fi components to receive the required low speed user messages. The output of the average circuit produces two signal levels, corresponding to "0" and "1" bits. To be specific, we have two different signal voltages, V_0 and V_1 , $V_1 > V_0$, V_0 and V_1 , corresponding to zero and one bit. To distinguish them, the receiver will calculate the average level of the two signal, that is, the threshold $(V_0 + V_1) / 2$. When the received signal is larger than the threshold, the received signal V_1 is not; otherwise, the received signal V_0 . The output of the comparator is provided to the microcontroller. The microcontroller then decodes and decrypts the signal. Show original message.

3.2 FM0 coding

Since the backscatter transmitter operates between reflected and non reflecting states, it generates a switch keying. However, backscattered signals can constructively or disrupt the interference with the surrounding Wi-Fi signals. Accordingly, an increase or decrease in a received power level may occur at a receiver position according to a “1” bit. To solve this problem, FM0 encoding [7] is adopted. Each point of the FM0 encoding conversion is two symbol coded information using symbol conversions rather than power levels. The transition of FM0 to the symbol of the beginning of each age represents a “0” transition, and there is no such intermediate point at 1. Therefore, bits are encoded at power level conversion rather than actual power levels [11].

3.2.1 Security RSA algorithm

RSA is an encryption algorithm for encrypting and decrypting messages. The RSA algorithms are Rivest, Shamir, and Adleman. It is an asymmetric key algorithm. Asymmetry means that there are two different keys. This is also called public key cryptography. There is a public key, which everyone knows is used to encrypt data. Private keys are known only by the intended receiver and used to decrypt data. It is based on the fact that finding integer factors is difficult (factoring problems). The user of RSA creates and then broadcasts the product of two large primes, and another value as their public key.

3.2.2 Four: Application of vehicular ad hoc network

This proposed environment backscatter module is the best for communication between smart vehicles, because current communication occur using Bluetooth or Wi-Fi signals, which is power consumption. High power systems are not needed to transmit emergency messages. Therefore, we can use the backward scattering module of ultra low power communication systems.

Our application is to allow the use of automobiles in safe buildings. Therefore, in our application, we allow or allow access to only those vehicles that have a secure license. The number of the cars kept in the access control system of the building’s main entrance. Suppose a car is to enter a safe building, and then take the following actions. Only know the number of access control system. So the only way to do that is to enter a message containing the car number. If the driver wants to pass the car number to the gate of the building, he touches the touch sensor. The sensor is connected to the microcontroller. It’s programmed so that whenever the touch sensor is pressed, it must send the car number, saying, “TN 23, AV 2471.”. This information is modulated via radio frequency switches, modulated via ambient Wi-Fi signals, and transmitted to the building gate receiver system via the antenna. At the gate, the receiving circuit demodulates the sending message and obtains the license plate number. If the car number is allowed to enter the building, then the automatic goalkeeper is opened and the car will be allowed to enter..

4 Simulation results

The concept of the whole communication system has been implemented in the Simulink version r2015b. Simulink as a software tool, since it is a graphical programming environment,

you can use the model and Simulation of a multi domain system [15]. This topic mainly uses the radio frequency toolbox to carry on the simulation to the communication system.

The whole block diagram is shown in Fig. 1, which includes the environmental radio frequency signal, the transmitter section and the receiver section.

When the touch sensor output is “1”, the environment RF signal is used as the transmitter input. The surrounding radio frequency signals are encrypted with information signals using the RSA algorithm using FM0 encoding to avoid interference in the environment of coded modulation. The modulation signal is a signal that is scattered from the transmitter block to the receiver portion. Before the signal is received, it declines in the environment. Then, the received signal is demodulated by means of signal averaging, peak detector, threshold circuit and comparator, and decrypted by RSA algorithm.

4.1 Transmitter

The output of the touch sensor and the environment RF signal are inputs in the block. The encrypted and encoded message bits are supplied to the signal generator, which generates the desired message signal that will be modulated with the ambient RF signal and sent to the destination. There is a switch with the threshold set to “1” that is, when the sensor output is “1”, our message is passed to the RF switch as a control signal, or the constant “0” is sent. Another input of the radio frequency switch is the environmental radio frequency signal, that is, the Wi-Fi signal. When the control signal is a user message, the user message and the environment RF signal are modulated, and the output of the transmitter portion, that is, the transmitted signal. When the control signal is not our message, i.e., the constant zero, no signal is transmitted.

It describes the signal produced by the transmitter. The first signal is the real and imaginary part of the surrounding RF signal at the frequency of 2.4GHz. The next signal is the output of the touch sensor. This value is 1 when touching. Followed by encryption and coding of user information, that is, the number. Finally, the sending message, which is the environment RF signal modulated by the user message.

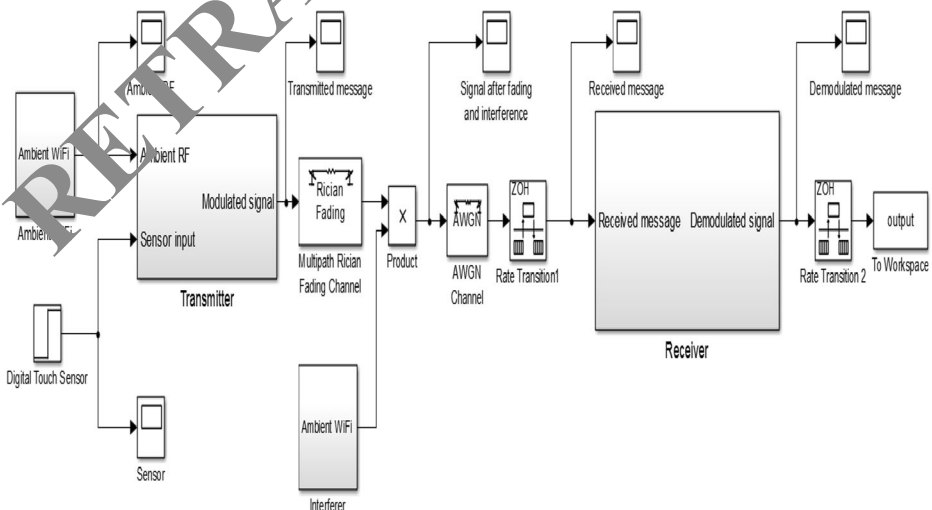


Fig. 1 Full system in Simulink

4.1.1 Receive

The backscattered receive signal acts as a receiver portion input. For demodulation, the received signal has an RF diode-diode1 (forward voltage 0.18v), and then there is a signal overlay circuit. In the signal averaging circuit, we use a resistor ($R1 = 10 \text{ K Ohm}$) and a capacitor ($C1 = 50\text{nf}$). This gives the envelope of the received signal.

Then there is a peak detection circuit in which the limited gain Op, Amp, and diode2 (forward voltage 1 V) are used. This will detect the peak value of the envelope signal at a given rate. In the threshold circuit, there are two resistors ($R2, R3 = 60 \text{ K ohms}$) and capacitors ($C2 = 5$, ultrafiltration, $C3 = 100 \text{ nF}$). Then, the demodulated output signal is obtained by comparing the average signal with the threshold. This is a comparator, in the receiver section. Then again, the output of the conversion rate, which helps to give a specific output bit rate, so you can also decrypt (i.e. RSA decryption), and get the desired output (i.e. input message).

It describes the received signal. The first signal is the additive Gauss white noise and the interference of the received signal with the Rician Fading. The signal below it is the output signal of envelope detection. The next signal is the demodulated signal. The output is displayed in FM0 decryption using the RSA algorithm to decode user messages. The raw user message, TN 23, AV 2471, has been authenticated.

As shown in Table 1, Flickr circles detection based on our feature combination cannot achieve the best accuracies. But its time consumption is very competitive, thus we in our implementation use this scheme. Besides, we believe that our method does not rely on the image coding too much. As shown in Table 1, Comb4, Comb5, and our schemes all achieve satisfactory detection accuracies.

5 Conclusion and futurework

In general, wireless communications use devices that use batteries or electromagnetic sources to communicate, which requires frequent battery replacement and pollution of the atmosphere [16, 17, 20–22, 29–31]. And message sharing system is highly relevant to information security management [33–35]. Optimizing energy consumption and protecting the environment, the communication system between the two devices in the VANET is not implemented with the use of an electromagnetic energy source [8, 9, 13, 18, 23–27, 32]. This can be achieved by using the surrounding RF signals for communication purposes. Radio frequency signals are not needed. This enables inexpensive and low maintenance communications. Thus, in this project, secure backscatter communications are simulated and validated using Simulink. This has been shown to be applicable to access control of vehicles entering safe buildings. The RSA algorithm provides communication security. The use of FM0 coding is reduced due to interference errors, has also been justified. In future this communication system will be implemented in hardware.

Table 1 BER scores using different feature combinations

Architecture	0.6517	0.7332
Window seat	0.7559	0.8441
Movement	0.4893	0.5448
Orange and blue	0.4557	0.5943
Jump project	0.5231	0.6049
Time per image	21.43 ms	49.04 ms

6 Future scope

The system is designed for short message transmission in VANET. In the future, this can even be extended to text files and images [19, 28]. To this end, the data rate of the system must be increased. However, this will yield a tradeoff between the distance the signal is transmitted and its data rate. Power dissipation can be alleviated by using a low power dedicated integrated circuit (ASIC). This is a field of study. As the system does not involve any user interference, there is great room for development in the future of automated vehicles.

Acknowledgements This paper is supported by Guangzhou Key Lab of Body Data Science 201605030011.

References

1. Arrawatia M, Baghin MS, Kumar G (2011) RF energy harvesting system from cell towers in 900MHz band. Natl Conf Commun (NCC) 2011:28–30
2. Hansini V, Edna Elizabeth N, Hemapriya R, Kavitha S (2016) Secured backscatter communication between smart cars in a vehicular Ad-Hoc network. 10th International Conference on Intelligent Systems and Control (ISCO'16), pp 784–787
3. Hattori S, Tezuka T, Tanaka K (2006) Content-based energy control for secure spaces. Mobile data management, 2006. MDM 2006. 7th International Conference, pp 77–98
4. Kawahara Y, Tsukada K, Asami T (2009) Feasibility and potential application of power scavenging from environmental Rf signals. Antennas and Propagation Society International Symposium, 2009. APSURSI '09. IEEE, pp 1–5
5. Lim TB, Lee NM, Poh BK (2013) Feasibility Study of Ambient RF energy harvesting for wireless sensor network. In IEEE MTT-S International Microwave Workshop Series on RF and Wireless Technologies for Biomedical and Healthcare Applications (IMWBS-BIO), 2013, pp 1–3, IEEE
6. Liu Y, Huang C, Min H, Li G, Han Y (2007) Digital correlation demodulator design for RFID reader receiver. IEEE Wireless Communications and Networking Conference, pp 1664–1668
7. Liu V, Parks V, Talla V, Gopalakota S, Wetherall D, Smith JR (2013) Ambient backscatter: wireless communication out of thin air. Proc ACM SIGCOMM, pp 39–50
8. Liu X, Song M, Tao D, Liu Z, Zhang L, Chen C, Bu J (2013) Semi-supervised node splitting for random forest construction. In Computer Vision and Pattern Recognition (CVPR), 2013. I.E. Conference on, pp 492–499
9. Liu X, Song M, Tao D, Zhang L, Bu J, Chen C (2014) Learning to track multiple objects. IEEE Trans Neural Netw Learn Syst Google Scholar.
10. Pathan AS, Lee H-W, Hong CS. (2006) Security in wireless sensor networks: issues and challenges. Advanced communication technology, 2006. ICACT 2006. The 8th International Conference, Phoenix Park, pp 1043–1048
11. Samal AP, Yeager DJ, Powledge PS, Mamishev AV, Smith JR (2008) Design of an RFID-based battery-free programmable sensing platform. IEEE Trans Instrum Meas 57(11):2608–2615
12. Volvo testing Smart cars that share road conditions (2015) In <http://www.itsinternational.com/categories/location-based-systems/news/volvo-testing-smart-cars-that-share-road-conditions/>
13. Yin Y, Shen Z, Zhang L, Zimmermann R (2015) Spatial-temporal tag mining for automatic geospatial video annotation. ACM Trans Multimed Comput Commun Appl (TOMM), 11(2):29
14. Yousefi S, Mousavi MS, Fathy M, (2006) Vehicular ad hoc networks (VANETs): challenges and perspectives. 2006, 6th International Conference on ITS Telecommunications Proceedings, pp 761–766
15. Zhang Y, He J, Wang L, Chen L (2010) The research and simulation on capture technology in synchronous serial of frequency hopping communication system based on Simulink. 2010 International Conference on Future Information Technology and Management Engineering (FITME), vol. 1, no., pp 509–511, 9–10
16. Zhang L, Han Y, Yang Y, Song M, Yan S, Tian Q (2013) Discovering discriminative graphlets for aerial image categories recognition. IEEE Trans Image Process (T-IP) 22(12):5071–5084 (IF:3.199, CCF A, JCR 2)
17. Zhang L, Song M, Zhao Q, Liu X, Bu J, Chen C (2013) Probabilistic graphlet transfer for photo cropping. IEEE Trans Image Process (T-IP) 21(5):803–815 (IF:3.199, CCF A, JCR 2)

18. Zhang L, Song M, Liu Z, Liu X, Bu J, Chen C (2013) Probabilistic graphlet cut: exploiting spatial structure cue for weakly supervised image segmentation. In Computer Vision and Pattern Recognition (CVPR), 2013 I.E. Conference on pp 1908–1915
19. Zhang L, Tao D, Liu X, Song M, Chen C (2014) Grassmann multimodal implicit feature selection. *Multimed Syst*, 20(6):659–674.
20. Zhang L, Gao Y, Ji R, Dai Q, Li X (2014) Actively learning human gaze shifting paths for photo cropping. *IEEE Trans Image Process (T-IP)* 23(5):2235–2245 (IF:3.199, CCF A, JCR 2)
21. Zhang L, Gao Y, Zimmermann R, Tian Q, Li X (2014) Fusion of multi-channel local and global structural cues for photo aesthetics evaluation. *IEEE Trans Image Process (T-IP)* 23(3):1419–1429 (IF:3.199, CCF A, JCR 2)
22. Zhang L, Yang Y, Gao Y, Wang C, Yu Y, Li X (2014) A probabilistic associative model for segmenting weakly-supervised images. *IEEE Trans Image Process (T-IP)* 23(9):4150–4159 (IF:3.199, CCF A, JCR 2)
23. Zhang L, Gao Y, Hong C, Feng Y, Zhu J, Cai D (2014) Feature correlation hypergraph: exploiting high-order potentials for multimodal recognition. *IEEE Trans Cybern (T-CYB)* 44(8):1408–1419 (IF:3.136, CCF B, JCR 1)
24. Zhang L, Gao Y, Ji R, Ke L, Shen J (2014) Representative discovery of structure cues for weakly-supervised image segmentation. *IEEE Trans Multimed(T-MM)* 16(2):470–479 (IF:1.754, CCF B, JCR 2)
25. Zhang L, Song M, Yang Y, Zhao Q, Chen Z, Sebe N (2014) Weakly supervised photo cropping. *IEEE Trans Multimed (T-MM)* 16(1):94–107 (IF:1.754, CCF B, JCR 2)
26. Zhang L, Ji R, Xia Y, Li X (2015) Learning a probabilistic topology discovery model for scene categorization. *IEEE transactions on neural networks and learning systems* 26(8):1622–1634
27. Zhang Y, Zhang L, Zimmermann R (2015) Aesthetics-guided summarization from multiple user generated videos. *ACM Trans Multimed Comput Commun Appl (TOMM)*, 11(2):24
28. Zhang L, Gao Y, Zhang C, Tian Q, Zimmermann R (2014) Perception-guided multimodal aesthetics discovery for photo quality assessment. In Proc. ACM Multimedia 2014. pp. 237–246
29. Zhang L, Xia Y, Ji R, Li X (2015) Spatial-aware object-level saliency prediction by learning graphlet hierarchies. *IEEE Trans Ind Electron (T-IE)* 62(2):1301–1308 (IF: 5.165, JCR 1)
30. Zhang L, Gao Y, Xia Y, Dai Q, Li X (2015) A fine-grained image categorization system by celllet-encoded spatial pyramid modeling. *IEEE Trans Ind Electron (T-IE)* 62(1):564–571 (IF: 5.165, JCR 1)
31. Zhang L, Xia Y, Mao K, Shan Z (2015) An effective video summarization framework toward handheld devices. *IEEE Trans Ind Electron (T-IE)* 62(2):1309–1316 (IF: 5.165, JCR 1)
32. Zhang L, Gao Y, Hong R, Hu Y, Ji R, Dai Q (2015) Probabilistic skimlet fusion for summarizing multiple consumer landmark videos. *IEEE Trans Multimed (T-MM)* 71(1):40–49 (accepted, IF:1.754, CCF B, JCR 2)
33. Zhang J, Dai L, Sun S, Wang Z (2011) On the spectral efficiency of massive MIMO systems with low-resolution ADCs. *IEEE Commun Lett* 25(5):842–845
34. Zhang J, Xue X, Björnson E, Ai B, Jin S (2017) Spectral efficiency of multipair massive MIMO two-way relaying with hardware impairments. *IEEE Wireless Communications Letters*
35. Zhang J, Dai L, He Z, Jin S, Li X (2017) Performance analysis of mixed-ADC massive MIMO systems over rician fading channels. *IEEE J Sel Areas Commun* 35(6):1327–1338

Hu Zhen-tao, born in 1979. He received his Ph.D degrees in Control Science and Engineering from Northwestern Polytechnical University in 2010. He also received his B.S. and M.S. degrees from Henan University in 2003 and 2006 respectively. Now, he is an assistant professor of college of computer and information engineering, Henan University. His research interests include complex system modeling and estimation, target tracking and nonlinear filter, etc.

Zhen Wang received his bachelor's degree in Hefei University of Technology, China in 2017. And he is currently studying for a master's degree at Hefei University of Technology.

Peng Shu is a researcher in State Grid Zhejiang Electric Power Research Institute.

Xinyu Xiang is a researcher in State Grid Hangzhou Power Supply Company.