IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received October 9, 2019, accepted October 31, 2019, date of publication November 5, 2019, date of current version November 15, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2951576

A LCX-Based Intrusion-Detection Sensor Using a Broadband Noise Signal

HANG XU, RUIXIN XIE, HONG HAN, ZHAOXIA ZHANG, JIANGUO ZHANG, LI LIU, BINGJIE WANG, AND LIQIANG LI

Key Laboratory of Advanced Transducers and Intelligent Control System, Ministry of Education and Shanxi Province, Taiyuan University of Technology, Taiyuan 030024, China

College of Physics and Optoelectronics, Taiyuan University of Technology, Taiyuan 030024, China

Corresponding author: Hang Xu (xuhang@tyut.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61601319, in part by the China Scholarship Council under Grant 201706935037, in part by the Key Research and Development (R&D) Projects of Shanxi Province under Grant 201703D321036 and Grant 201803D31037, in part by the Natural Science Foundation of Shanxi Province under Grant 201701D221114, Grant 201701D121009, and Grant 201801D121145, in part by the Shanxi Scholarship Council of China under Grant 2017-031, and in part by the Scientific and Technological Innovation Programs of Higher Education Institutions in Shanxi under Grant 2017136.

ABSTRACT An intrusion detection sensor system based on a broadband noise signal and two leaky coaxial cables (LCXs) is proposed and experimentally demonstrated. In the proposed sensor, the broadband noise signal is generated by our designed white noise generator used as the detection signal. The detection signal is transmitted and received by two parallel LCXs, forming an invisible electromagnetic monitoring field around the protected area. The intrusion distance along the LCXs can be accurately extracted by the correlation method and the difference between pre- and post-intrusion correlation curves. Experimental results demonstrate the proposed sensor can monitor the intrusion process and locate multiple intruders. The range resolution of 30 cm and the dynamic range of 30 dB can be achieved. Furthermore, the proposed sensor has the strong anti-radio frequency interference (anti-RFI) capability, which makes it very suitable in the complex RF environment.

INDEX TERMS Intrusion detection sensor, noise signal, leaky coaxial cable (LCX).

I. INTRODUCTION

Intrusion detection technologies have been widely used in safety protection of critical infrastructures such as banks, airports, nuclear power plants, military bases and other sensitive sites which require a very high level of security. Common intrusion detection technologies include laser scanners [1], [2], infrared sensors [3], [4], video mobile detectors (VMDs) [5], [6] and electronic fences [7], [8]. However, these technologies have the following defects: (1) Detection equipments such as electronic fences are usually exposed to the outside and vulnerable to intentional evasion and malicious destruction, so they have poor concealments. (2) The adaptabilities of detection equipments to weather change and terrain environment are also weak. For example, changes in environment temperature and visibility caused by wind, rain, snow, fog, hail and day/night can seriously interfere with the detection effects of laser scanners, infrared sensors and VMDs. In addition, the monitoring areas of laser scanners and infrared sensors are usually linear, so they can not adapt to the complex terrain environment.

Intrusion detection sensor based on leaky coaxial cables (LCXs) [9]–[11] can solve the aforementioned problems well. It uses a pair of LCXs to transmit and receive electromagnetic waves. An electromagnetic field for monitoring intruders is formed between two parallel LCXs with a certain spacing. By analyzing the change of echo signal, the LCX-based sensor can realize the purpose of intrusion alarm. Compared with common intrusion detection technologies, the LCX-based sensor has the following inherent advantages [12]: (1) The LCXs are buried in the shallow underground layer and the monitoring electromagnetic field is invisible, which makes the sensor more concealed. (2) The monitoring electromagnetic field between two LCXs is not affected by temperature, visibility and weather variations. (3) The LCXs have good flexibilities and can be laid around the protected area according to the terrain characteristics without blind area.

The associate editor coordinating the review of this manuscript and approving it for publication was Mohamed Kheir.

Variety microwave signals such as single-frequency continuous-wave (CW) [13], [14], radio frequency (RF) pulse [15]–[18] and carrier modulated Golay codes [19]–[21] have been used as the detection signals of LCX-based sensors. In previous studies, a single-frequency CW was transmitted by the LCX-based sensor into the electromagnetic surveillance space. The sensor can judge whether there exists an intruder by comparing the echo waveforms before and after intrusion, but it cannot give an accurate intrusion distance [22]. By transmitting a RF pulse such as a 1/2 sine pulse [15], a single-frequency pulse [16], a linear frequency modulation (LFM) pulse [17], and a chirp signal [18], the LCX-based sensor can locate the intruder with the location accuracy less than 1 m. It is realized by calculating the delay time of echo pulse after the pulse accumulation and the synchronous subtraction. However, its range resolution can only reach several meters, such as 6.64-m range resolution given by [17] and 3.32-m range resolution reported in [18]. To increase the signal-to-noise ratio (SNR), the complementary Golay codes with carrier modulation are used as the monitoring signal [21]. The characteristic of this sensor is that it can monitor two pairs of LCXs simultaneously using one processor [19]. Although the location accuracy and range resolution of this sensor can reach 1 m and 24 m by using the quarter rate translation and the high-speed correlation process [21], there is no significant improvement compared with the LCX-based sensor using the RF pulse. So far, the range resolution of the existing LCX-based sensors can only reach several meters, so it is difficult to distinguish and locate multiple intruders with a small spacing. Moreover, multiple LCX-based sensors need to work together to expand protected areas in practice, leading mutual interferences between the detection signals which mean radio frequency interferences (RFIs). Unfortunately, the detection signals of the existing LCX-based sensors are vulnerable to RFIs.

Noise has natural random features, wide and flat frequency spectrum and nearly perfect autocorrelation properties. As the detection signal, noise has been applied in time domain reflectometry [23], through-wall imaging radar [24], and remote ranging radar [25]. In 2005, Lo and Furse proposed a noise-domain reflectometry for locating wiring faults with 3-inches location accuracy [23]. In 2008, the ultrawideband (UWB) noise waveforms were used in the through-wall imaging radar by Narayanan, which made the system achieve a range resolution of 30 cm [24]. Grodensky *et al.* proposed a microwave-photonic UWB noise ranging radar in 2012, which improved the range resolution to 10 cm [25]. The above-mentioned researches indicate that the noise as the ranging signal can realize centimeter-scale location accuracy and range resolution.

In this paper, a LCX-based intrusion-detection sensor using a broadband noise signal is proposed and experimentally demonstrated. The noise signal is transmitted and received by a couple of LCXs, thus forming an invisible electromagnetic surveillance space. The intruders can be accurately located and tracked by correlating the noise echo signal with its reference signal and comparing pre- and post-intrusion correlation curves. The experiments demonstrate that the proposed sensor can realize the range resolution of centimeter level as well as the anti-radio frequency interference (anti-RFI) detection benefiting from the broadband and autocorrelation characteristics of the noise signal. While maintaining the inherent advantages of the existing LCX-based sensors, our sensor makes up for their defects of low range resolution and weak anti-RFI ability very well.

II. EXPERIMENTAL SETUP

The experimental setup of the LCX-based sensor utilizing a broadband noise signal is shown in Fig.1. The broadband noise signal generated by a white noise generator (WNG) is amplified by a broadband microwave amplifier (BMA). The amplified noise signal is split into the reference signal $r(t)$ and the detection signal $d(t)$ by a directional coupler with 15-dB coupling ratio. The reference signal $r(t)$ with 3 % power is collected directly by an oscilloscope (OSC), while the detection signal $d(t)$ with 97 % power is radiated into the monitoring space through the transmit LCX. The echo signal $e(t)$ containing the direct waves and the reflected wave from the intruder is received by the receive LCX. The transmit and receive LCXs are parallelly placed along the perimeter of the protected area. Matched terminations (MTs) are mounted at the ends of the LCXs to absorb signals and eliminate terminal reflection. An electromagnetic monitoring space is formed between these two LCXs. A low noise amplifier (LNA) is used to amplify the echo signal. Then, the amplified echo signal $e(t)$ is collected by the OSC with $r(t)$. Finally, both data handling and result displaying are realized on a personal computer (PC). Table 1 presents the main device parameters of our sensor.

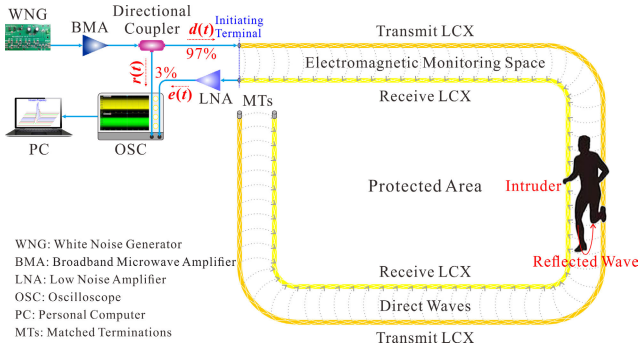


FIGURE 1. Experimental setup of the LCX-based sensor utilizing a broadband noise signal.

III. GENERATION AND CHARACTERISTICS OF NOISE SIGNAL

The broadband noise signal is generated by our designed WNG. Its circuit diagram is shown in Fig. 2(a). D is a Zener diode operating in a voltage reverse bias state. When the electric field in PN junction is large enough to the breakdown voltage, the carriers are accelerated to collide more electron-hole pairs from the lattice. Consequently, the avalanche

TABLE 1. The main device parameters of our sensor.

Devices	Frequency Band /Bandwidth	Other Parameters
BMA	75 Hz-10 GHz	Max Gain: 25dB
Directional Coupler	1 MHz-1 GHz	Coupling Ratio: 15 dB
LNA	9 kHz-1 GHz	Max Gain: 32 dB
OSC	2 GHz	Sampling Rate: 20 GSa/s
LCXs	≤450 MHz	

multiplication effect occurs, which leads to the avalanche breakdown of diodes. It is a noisy process, and the power spectral density of the noise is usually white. Therefore, the Zener diode is usually used to produce the white noise. In addition, C is a DC-isolating capacitor to filter out the DC component from the noise frequency spectrum. R is a current limiting resistor to prevent thermal breakdown due to excessive current flowing through the Zener diode. In order to realize the large-amplitude noise signal output, three cascaded amplifiers are used in this noise generator. The frequency range of the amplifier is from DC to 2 GHz, and its typical gain is 17.6 dB@1 GHz. The prototype board of WNG is shown in Fig. 2(b) with a size of 6 cm×3.5 cm and a +12-V driving voltage. It has the advantages of small size, simple structure, low cost and stable noise output with large amplitude.

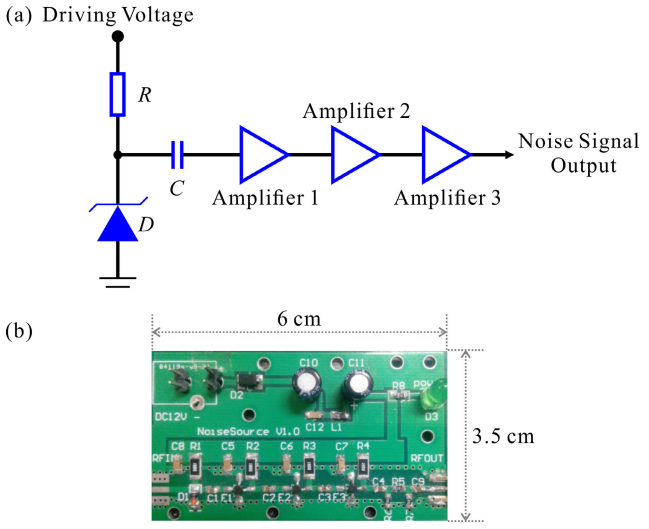


FIGURE 2. (a) Circuit diagram and (b) prototype board of the white noise generator.

Figure 3 shows the characteristics of the noise signal used in our LCX-based sensor. The noise waveforms exhibit natural random variations over time without any regularity, as depicted in Fig.3(a). Figure 3(b) shows that it has a wide and flat frequency spectrum with a 3-dB bandwidth of 1.4 GHz. Additionally, the noise signal has a delta-profile autocorrelation curve with a sharp correlation peak, showing an almost perfect "thumbtack" shape, as plotted in Fig. 3(c).

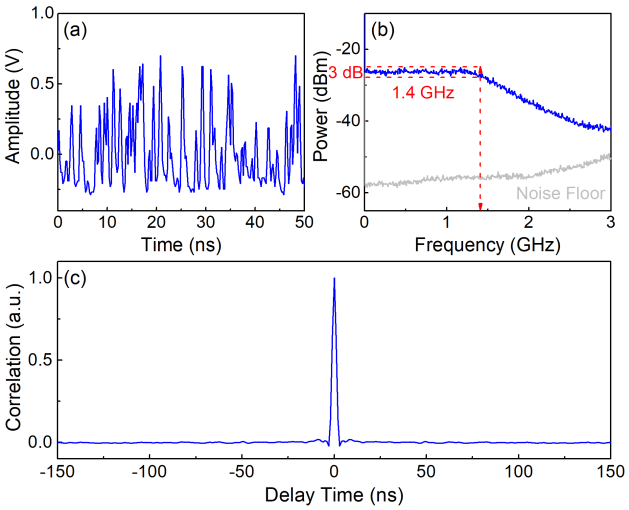


FIGURE 3. (a) Time sequence, (b) frequency spectrum and (c) autocorrelation curve of the noise signal.

The transmission power of noise signal measured by a power meter is 14.5 dBm.

IV. MEASURE PRINCIPLE

Two sparsely braided LCXs of MSLYFVZ-50-9 model are used to transmit and receive the noise signal in the proposed sensor. Their outer conductors are composed of diamond-shaped apertures woven with metal wires, which present a sparse network structure. The detection signal can be radiated or absorbed by these apertures, forming a stable electromagnetic field for monitoring intruders between two LCXs [26]. Unlike the radiation LCX commonly used in existing LCX-based sensors, the sparsely braided LCX is a typical coupled LCX, which possesses a wider working bandwidth. So it is selected for transmitting and receiving the broadband noise signal in our sensor. Table 2 gives the structural parameters and performance indicators of the LCXs used in our sensor.

TABLE 2. The structural parameters and performance indicators of the LCXs used in our sensor.

Parameter Name	Parameter Value
Inner Conductor of Round Copper Wire	3.5 mm@Diameter
Physically Foamed Polyethylene Insulation	8.8 mm@Diameter
Braided Outer Conductor	10 mm@Diameter
Flame Retardant Polyvinyl Chloride Jacket	12.6 mm@Diameter
Characteristic Impedance	50±3 Ω
Attenuation Constant	≤10 dB/100 m@450 MHz
Voltage Standing Wave Ratio	≤1.3
Coupling Loss	75±10 dB@450 MHz

The measure principle of our sensor is shown in Fig.4. When there exists no intruder in the monitoring space before the intrusion occurs, the receive LCX will receive the echo signal, which is composed of the direct waves from the transmit LCX. Assuming that the receive LCX contains m apertures and j denotes any of these apertures, the pre-intrusion

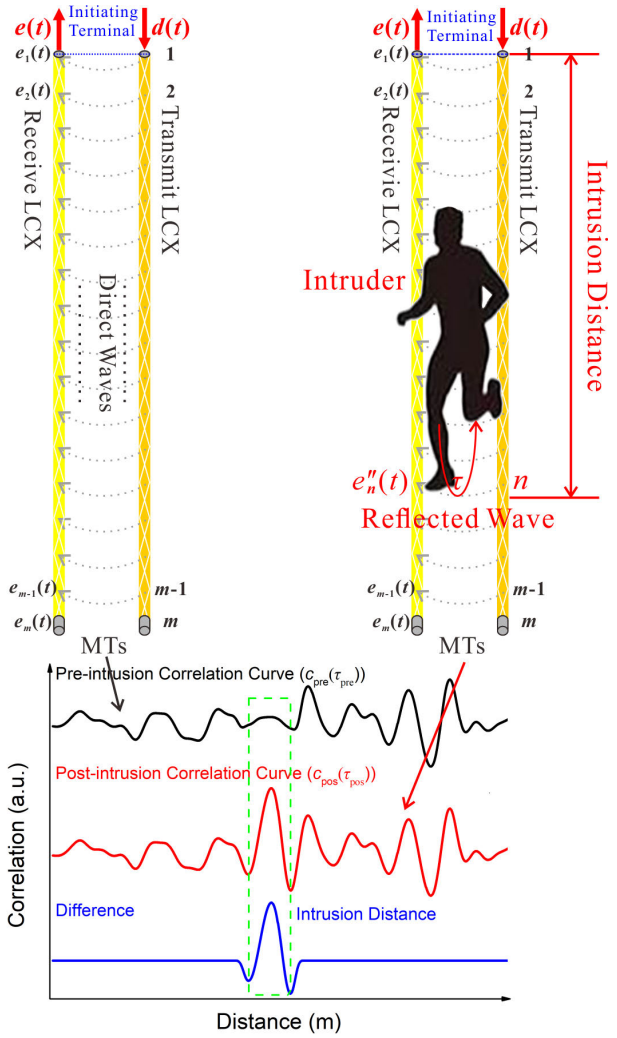


FIGURE 4. Measure principle of the LCX-based sensor utilizing a broadband noise signal.

echo signal $e_{\mathrm{pre}}(t)$ can be given by:

$$e_{\mathrm{pre}}(t) = \sum_{j=1}^{m} e_j(t) \tag{1}$$

where $e_j(t)$ denotes the direct waves received by the jth aperture of the receive LCX. A pre-intrusion correlation curve $c_{\mathrm{pre}}(\tau_{\mathrm{pre}})$ represented by the black curve in Fig.4 is obtained by correlating $e_{\mathrm{pre}}(t)$ and the reference signal $r(t)$ before the intrusion occurs. $c_{\mathrm{pre}}(\tau_{\mathrm{pre}})$ is used for pre-intrusion calibration, which is expressed as:

$$c_{\mathrm{pre}}\left(\tau_{\mathrm{pre}}\right) = e_{\mathrm{pre}}(t) \otimes r(t) = \sum_{j=1}^{m} \left[e_j(t) \otimes r(t)\right] \tag{2}$$

where τ_{pre} means the delay time of $e_{\mathrm{pre}}(t)$ relative to $r(t)$, and $\otimes$ represents the correlation calculation. Each direct wave received by the receive LCX is delay correlated with $r(t)$, so Eq.(2) indicates that $c_{\mathrm{pre}}(\tau_{\mathrm{pre}})$ is the superposition of the correlation curves from all direct waves. Note that $c_{\mathrm{pre}}(\tau_{\mathrm{pre}})$ needs to be scaled zero by subtracting the inherent delay time of signal propagation in the sensor.

Once an intruder crosses the electromagnetic monitoring space between two LCXs, the reflected wave caused by the intruder will be formed and mainly received by the nth aperture of the receive LCX with the direct waves. The post-intrusion echo signal $e_{\mathrm{pos}}(t)$ is written as:

$$\begin{aligned} e_{\mathrm{pos}}(t) &= \sum_{j=1}^{n-1} e_j(t) + \sum_{j=n+1}^{m} e_j(t) + e_n'(t) + e_n''(t) \\ &= e_{\mathrm{pre}}(t) + e_n''(t) \end{aligned} \tag{3}$$

where $e_n'(t)$ is the direct waves received by the nth aperture of the receive LCX, and $e_n''(t)$ is the reflected wave caused by the intruder and received by the nth aperture of the receive LCX. Through the correlation operation between $e_{\mathrm{pos}}(t)$ and $r(t)$ after the intrusion occurs, a post-intrusion correlation curve $c_{\mathrm{pos}}(\tau_{\mathrm{pos}})$ represented by the red curve in Fig.4 is obtained as:

$$c_{\mathrm{pos}}\left(\tau_{\mathrm{pos}}\right) = e_{\mathrm{pos}}(t) \otimes r(t) = c_{\mathrm{pre}}\left(\tau_{\mathrm{pre}}\right) + e_n''(t) \otimes r(t) \tag{4}$$

where τ_{pos} is the delay time of $e_{\mathrm{pos}}(t)$ relative to $r(t)$. Eq.(4) shows that $c_{\mathrm{pos}}(\tau_{\mathrm{pos}})$ is the superposition of the correlation curves from the direct waves and the reflected wave. In addition, $c_{\mathrm{pos}}(\tau_{\mathrm{pos}})$ also needs to be scaled zero.

The intrusion detection result $c(\tau)$ represented by the blue curve in Fig.4 is obtained by calculating the difference between $c_{\mathrm{pos}}(\tau_{\mathrm{pos}})$ and $c_{\mathrm{pre}}(\tau_{\mathrm{pre}})$, as expressed below:

$$c(\tau) = c_{\mathrm{pos}}\left(\tau_{\mathrm{pos}}\right) - c_{\mathrm{pre}}\left(\tau_{\mathrm{pre}}\right) = e_n''(t) \otimes r(t) = \delta(t-\tau) \tag{5}$$

where τ is the delay time of $e_n''(t)$ relative to $r(t)$, that is, the roundtrip time between the sensor and the intruder along the LCXs. As indicated by Eq.(5), $c(\tau)$ is the correlation curve from the reflected wave. The roundtrip time τ is determined by the correlation peak position, so the intrusion distance along the LCXs can be obtained by calculating $\upsilon\tau/2$, where υ means the propagation velocity of electromagnetic wave in the LCX.

V. EXPERIMENTAL RESULTS

A. SINGLE INTRUSION DETECTION

The experimental scenario of single intrusion detection is shown in Fig.5(a), where an intruder crosses the LCXs into the protected area. The transmit and receive LCXs are laid on the ground around a rectangular protected area, parallel to each other and spaced at a distance of 0.4 m. A tapeline is placed parallel to the LCXs to reveal the actual intrusion distance. Figure 5(b) shows the pre- and post-intrusion correlation curves. By comparing them, one can find that an obvious correlation peak appears at the intrusion distance while these two curves basically coincide at other distances. By calculating the difference between pre- and post-intrusion correlation curves, an obvious correlation peak at 4.0 m is

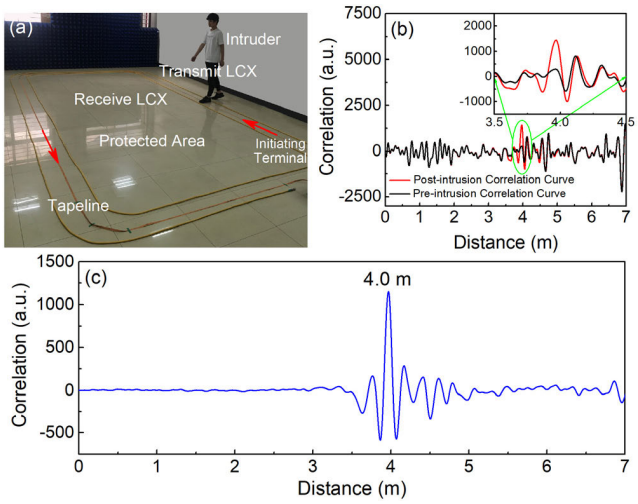


FIGURE 5. (a) Experimental scenario of single intrusion detection. (b) Comparison between pre- and post-intrusion correlation curves. (c) Intrusion location result at 4.0 m.

obtained as shown in Fig.5(c), whose peak position indicates the intrusion distance from the initiating terminal along the LCXs. Note that the correlation is calculated with a length of 500000 sampling points after comprehensive consideration of the detection effect and the signal processing speed.

Our LCX-based sensor can also be used to monitor the intrusion process of a single intruder by observing the position and height changes of correlation peak in this process. The illustration in Fig. 6 shows the complete process of an intruder passing through the rectangular protected area. The intruder first crosses the LCXs on one side, and enters the protected area, then crosses the LCXs on the other side to leave. The detection results in Fig. 6 show that the intruder enters the protected area at 3.7 m from the initiating terminal along the LCXs, and then leaves at 11.8 m after about 5 s. When the intruder enters or leaves the protected area, the correlation peak height always increases firstly, then reaches the maximum, and finally decreases. This changing trend corresponds to the process of intruder approaching firstly,

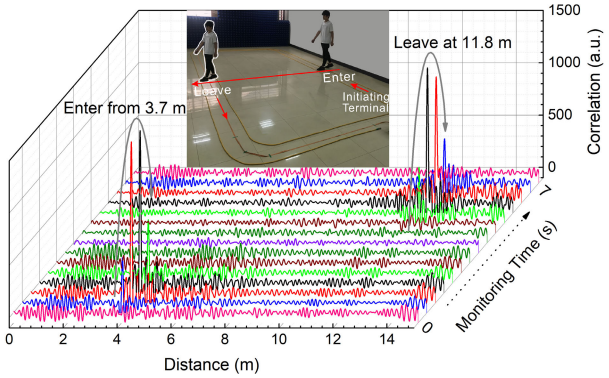


FIGURE 6. Monitoring results of a single intrusion process.

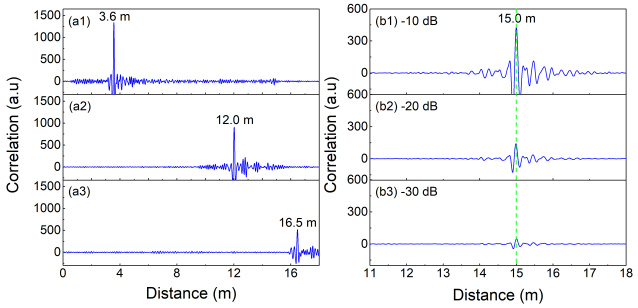


FIGURE 7. (a) Detection results of different intrusion distances. (b) Measurement results of the dynamic range.

crossing subsequently and finally leaving LCXs, respectively. It is because that the closer the intruder approaches the LCXs, the stronger the reflected signal produced by him, and the higher the correlation peak can be generated. During the process of intrusion monitoring, the OSC's working mode is set to the continuous acquisition mode, i.e. it continuously and automatically captures and stores a set of data including reference signal and echo signal at about 0.5 s interval. The data is then sent to the PC for processing and displaying in a few seconds.

The detection results of different intrusion distances are depicted in Figs.7(a1)-(a3). The correlation peaks clearly show that the intrusion distances are 3.6 m, 12.0 m and 16.5 m, respectively. With the increase of intrusion distance, the intruder's reflected signal becomes weaker, which leads to the decrease of correlation peak height. Limited by the size of the experimental site, it is difficult to directly measure the maximal detection range of our sensor in experiment. But the dynamic range can be further measured for estimating the maximal detection range. The intrusion detection result at 15.0 m is analyzed, when the transmission power decreases by 10 dB, 20 dB and 30 dB respectively. As expected, Figures 7(b1)-(b3) show that the correlation peak height drops with the reduction of the transmission power. If the transmission power drops more than 30 dB, the correlation peak representing intrusion distance will be submerged in the background noise, indicating that the intruder is no longer detectable. Therefore, the 30-dB dynamic range of our sensor can be inferred. According to the transmission loss of the LCXs measured by the power meter is 8.8 dB/100 m for the broadband noise signal, the maximal detection range of our sensor is estimated to be 185 m ($30/8.8\times100/2+15.0$ m$\approx$185 m) under the 14.5-dBm noise transmission power.

The accuracy of intrusion location is assessed by the relative error δ which is defined as:

$$\delta = |D_m - D_a|/D_a \times 100\% \tag{6}$$

where D_m is the measured intrusion distance given by our sensor, D_a is the actual intrusion distance provided by the tapeline. The relationship between the relative error δ and the intrusion distance D_a is depicted in Fig.8. Benefiting from the broadband characteristic of the noise signal, a low

location error $|D_m - D_a|$ of 10 cm can be obtained, which is similar to that of the recent reported LCX-based sensors [18] under the same intrusion distance. In addition, the dispersion of sparsely braided LCXs for the broadband signal is relatively weak, which results in a low and relatively stable location error within a certain intrusion distance. Therefore, it can be expected that δ reduces with the increase of D_a, as shown by the experimental data and fitted trajectory in Fig.8.

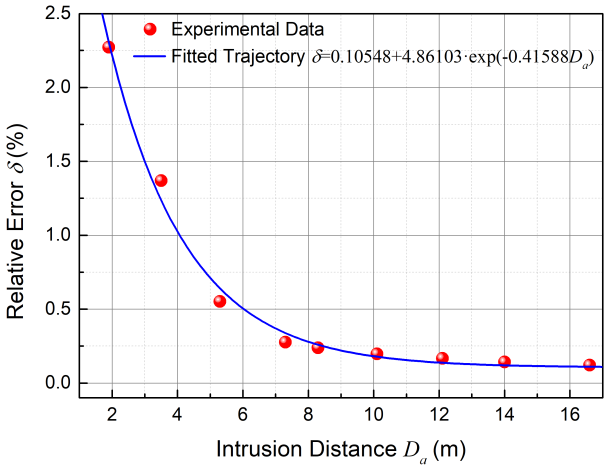


FIGURE 8. Relative error δ as a function of intrusion distance D_a.

B. MULTIPLE INTRUSIONS DETECTION

The detection results of multiple intrusions under the noise transmission power of 14.5 dBm is given in this subsection. When multiple intrusions occur simultaneously at different distances, the detection results are shown in Fig. 9. Fig. 9(a) gives the location results of two intruders at 3.4 m and 9.1 m, respectively. The detection results of three intruders located at 3.0 m, 7.9 m and 13.0 m are shown in Fig. 9(b). Four intruders crossing the LCXs simultaneously at 3.0 m, 8.2 m, 13.0 m and 16.1 m can also be located in Fig. 9(c). The results indicate that our sensor has the function of locating multiple intruders simultaneously.

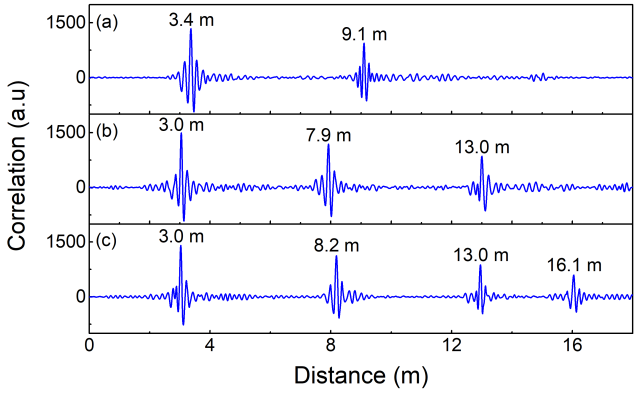


FIGURE 9. Detection results of (a) two intruders, (b) three intruders and (c) four intruders crossing the LCXs simultaneously.

Our LCX-based sensor can also monitor the intrusion process that two intruders step into the protected area with a short time interval. The corresponding results given in Fig. 10 show that one intruder firstly enters the monitoring area at 2.6 m from the initiating terminal along the LCXs, and about 1.5 s later another intruder enters at 4.3 m. The intrusion process can be seen from the height variation of correlation peak, which is consistent with the variation rule in Fig. 6. As the results prove, our sensor can monitor the intrusion process of multiple intruders, whether they intrude at the same time or not.

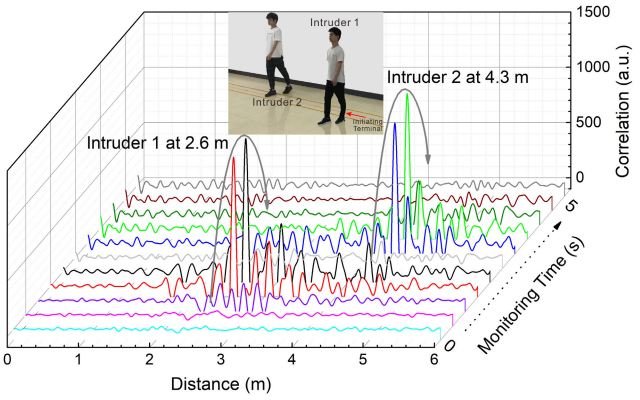


FIGURE 10. Monitoring results of two intrusion process occurring at different times.

In order to investigate the range resolution, our sensor locates two intruders with different spacings crossing the LCXs at the same time. The detection results are given in Fig. 11, where one intruder's distance is fixed at 3.8 m, and the spacing between the other intruder and the one is set as 90 cm, 60 cm and 30 cm, respectively. As depicted in Fig. 11, two intruders with 30-cm spacing can be clearly distinguished by two correlation peaks. In theory, the range resolution is determined by $\upsilon/2B$ [27], where $\upsilon = c_0/\sqrt{\mu_r \varepsilon_r} = 0.83c_0$, c_0 represents the speed of light, and B denotes the bandwidth of detection signal. The 1.4-GHz bandwidth of the noise signal

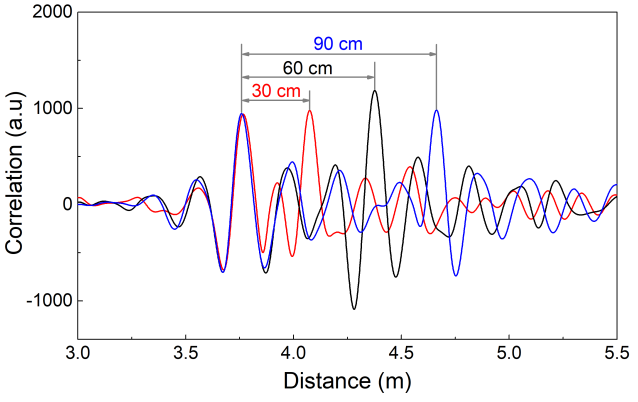


FIGURE 11. Detection results of two intruders with 30-cm, 60-cm and 90-cm spacing, respectively.

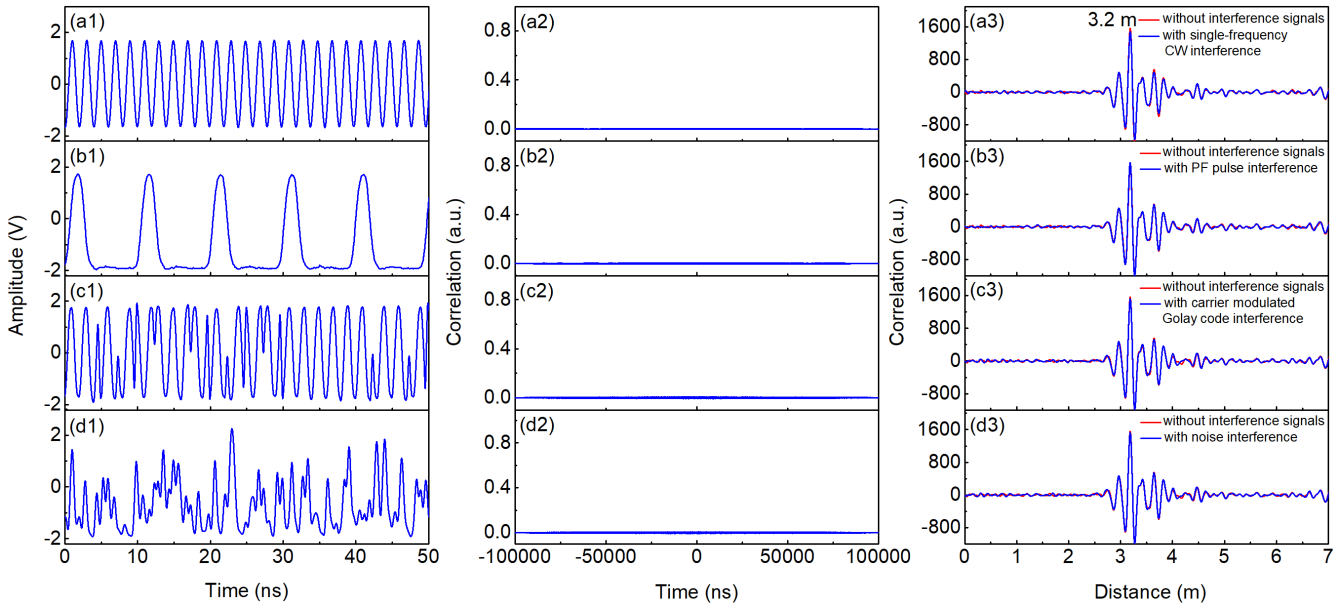


FIGURE 12. Time sequences of (a1) single-frequency CW, (b1) RF pulse, (c1) carrier modulated Golay codes and (d1) interference noise. (a2)-(d2) Crosscorrelation curves of different interference signals and the noise reference signal $r(t)$. (a3)-(d3) Comparison results of intrusion detection with and without interference signals.

in Fig.3(b) can realize 9-cm range resolution. Here, restricted by the 450-MHz working bandwidth of LCXs, the theoretical resolution is 28 cm, which is consistent with the experimental resolution of 30 cm. In addition, the bandwidths of other devices in our sensor are all greater than 450 MHz, as shown in Table 1. Finally, the centimeter-scale range resolution of our sensor is demonstrated.

C. ANTI-RFI DETECTION

The noise signal as the natural random signal shows strong anti-RFI ability to external RFIs due to its almost perfect autocorrelation property. The external RFIs usually come from the detection signals of other LCX-based sensors, when multiple sensors of the same type and different types work together to expand the protected area. The anti-RFI ability of our sensor is demonstrated experimentally in this subsection. The third LCX placed parallel to the transmit/receive LCXs is used to transmit interference signals into the monitoring space to form a complex RF environment, resulting in the noise echo signal and interference signals being received into our sensor together. The time sequences of interference signals including single-frequency CW, RF pulse, carrier modulated Golay codes and noise are plotted in Figs. 12(a1)-(d1), respectively. The transmission power of interference signals is the same as that of the noise detection signal, which is 14.5 dBm. The bandwidth/frequency of interference signals is selected as 500 MHz, because it is within the working bandwidth of LCXs used in the experiment. Crosscorrelation curves of different interference signals and the noise reference signal $r(t)$ in Figs. 12(a2)-(d2) reveal that the noise reference signal is uncorrelated with any interference signal as there is no peak in correlation curves. Figures 12(a3)-(d3) give the comparison results of intrusion detection with (blue curves) and without (red curves) interference signals. It can be seen from the almost overlapping detection results with and without interference signals, the correlation peak position as well as the correlation peak height are not changed by interference signals. As the results indicate that the LCX-based sensor using the noise as the detection signal has good immunity against external RFIs, which makes it very suitable in the complex RF environment.

VI. DISCUSSION

In practice, small animals sometimes break into the protected area and cause false alarm and misjudgement. Therefore, intrusion detection sensors are expected to distinguish human targets and small animals. The experiments indicate that our sensor can also distinguish human targets and small animals based on the correlation peak height. The basic principle is the larger the intruder's size bringing in the stronger reflected signal, which generates a higher correlation peak. Figures 13(a)-(b) show the detection results of a human target and a cat under the same intrusion distance and detection environment. The comparison results show that when the intruder is a human target, the correlation peak

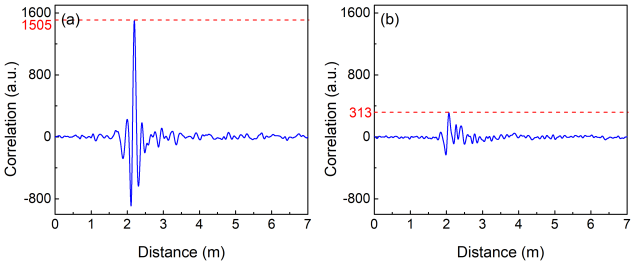


FIGURE 13. Detection results of (a) a human target and (b) a cat.

TABLE 3. Comparison of range resolution between our LCX-based sensor and the recent reported LCX-based sensors.

Parameter Name	Range Resolution
Our LCX-Based Sensor with Noise Signal	30 cm
LCX-Based Sensor with Golay Codes in Ref. [21] Reported in 2007	24 m
LCX-Based Sensor with LFM Pulse in Ref. [17] Reported in 2018	6.64 m
LCX-Based Sensor with Chirp Signal in Ref. [18] Reported in 2018	3.32 m

height, i.e. correlation coefficient, is 1505, while that of the cat is only 313. From these results, it is believable that setting appropriate correlation peak thresholds within different range segment, human targets and small animals can be properly distinguished.

VII. CONCLUSION

In summary, a LCX-based sensor using the broadband noise signal has been proposed for intrusion detection. The proof-of-concept experiments demonstrate the proposed sensor can locate and track multiple intruders. It can achieve a range resolution of 30 cm and a dynamic range of 30 dB. Additionally, the proposed sensor exhibits the excellent anti-interference capability to external RFIs. It also has the potential to distinguish human targets and small animals. Compared with the existing LCX-based sensors, the advantages of our sensor are as follows: (1) Broadband noise signal is easily generated with simple structure and low cost. (2) The range resolution can reach centimeter level due to the broadband characteristic of noise signal, which is superior to the recent reported LCX-based sensors's range resolution of meter level, as shown in Table 3. (3) It can be well used in the complex RF environment benefitting from the anti-RFI ability of noise signal. It is reasonable to believe that the proposed sensor provides a promising solution for perimeter safety protection of important/confidential places.

REFERENCES

[1] P. Hosmer, "Use of laser scanning technology for perimeter protection," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 19, no. 8, p. 13–17, Aug. 2004.

[2] K. Sahba, K. E. Alameh, and C. L. Smith, "A proposed motionless laser scanning architecture for perimeter security," in *Proc. 40th Annu. Int. Carnahan Conf. Secur. Technol.*, Lexington, KY, USA, Oct. 2006, pp. 9–16.

[3] M. Moghavvemi and L. C. Seng, "Pyroelectric infrared sensor for intruder detection," in *Proc. IEEE Region 10 Conf. TENCON*, Chiang Mai, Thailand, Nov. 2004, pp. 656–659.

[4] S. A. Aldalahmeh, A. M. Hamdan, M. Ghogho, and D. McLernon, "Enhanced-range intrusion detection using pyroelectric infrared sensors," in *Proc. SSPD*, Edinburgh, U.K., Sep. 2016, pp. 1–5.

[5] K. Sage and S. Young, "Security applications of computer vision," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 14, no. 4, pp. 19–29, Apr. 1999.

[6] F. Ortega-Zamorano, M. A. Molina-Cabello, E. López-Rubio, and E. J. Palomo, "Smart motion detection sensor based on video processing using self-organizing maps," *Expert Syst. Appl.*, vol. 64, pp. 476–489, Dec. 2016.

[7] A. Yousefi, A. A. Dibazar, and T. W. Berger, "Intelligent fence intrusion detection system: Detection of intentional fence breaching and recognition of fence climbing," in *Proc. IEEE Conf. Technol. Homeland Secur.*, Waltham, MA, USA, May 2008, pp. 620–625.

[8] S. Yang and F. L. Bu, "Design of frequency adjustable pulse in intelligent electronic fence system," in *Proc. ICTCE*, Beijing, China, Nov. 2018, pp. 344–347.

[9] J. L. Poirier, "Leaky coaxial cable resource protection sensor performance analysis," *IEEE Trans. Aerosp. Electron. Syst.*, vol. AES-18, no. 3, pp. 275–285, May 1982.

[10] J. Cheal, S. O'Brien, and M. Tutor, "Buried cable sensor with intruder location," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 20, no. 7, pp. 11–15, Jul. 2005.

[11] W. Tsujita, K. Inomata, and T. Hirai, "Development of dual leaky coaxial cable for intruder detection sensor," in *Proc. IEEE Int. Conf. Technol. Homeland Secur. (HST)*, Waltham, MA, USA, Nov. 2013, pp. 126–129.

[12] Q. Guan, H. Lu, K. Wang, and C. Chen, "A novel approach for intruder localization based on leaky coaxial cable sensor with IQ demodulation and synchronous subtraction," *Appl. Comput. Electromagn. Soc. J.*, vol. 33, no. 12, pp. 1483–1488, Dec. 2018.

[13] R. K. Harman and J. E. Siedlarz, "Advancements in leaky cable technology for intrusion detection," in *Proc. Carnahan Conf. Secur. Technol.*, Lexington, KY, USA, May 1982, pp. 115–121.

[14] D. Lindseth and R. W. Hansen, "Leaky cable intrusion detection sensors," in *Proc. Carnahan Conf. Secur. Technol.*, Lexington, KY, USA, May 1986, pp. 57–63.

[15] R. K. Harman, "Intrepid: A new outdoor perimeter sensor technology," in *Proc. IEEE Int. Carnahan Conf. Secur. Technol.*, Albuquerque, NM, USA, Oct. 1994, pp. 137–143.

[16] Q. Guan, H. Lu, C. Chen, and K. Wang, "Research on human intruder detection and localization based on LCX sensor," *Int. J. RF Microw. Comput. Aided Eng.*, vol. 29, no. 1, p. e21484, Jan. 2019.

[17] Q. Guan, C. Chen, and C. He, "A novel sensor using VHF zigzag-slotted leaky coaxial cable for intruder localization," *Microw. Opt. Technol. Lett.*, vol. 60, no. 3, pp. 634–639, Mar. 2018.

[18] Q. Guan, H. Lu, C. Chen, and C. He, "Multiple human targets detection and localization using leaky coaxial cable sensing technique," *Appl. Comput. Electromagn. Soc. J.*, vol. 33, no. 9, pp. 973–978, Sep. 2018.

[19] K. Harman and B. Hodgins, "The next generation of Guidar technology," in *Proc. 38th Annu. Int. Carnahan Conf. Secur. Technol.*, Albuquerque, NM, USA, Oct. 2004, pp. 169–176.

[20] K. Harman and B. Hodgins, "Next generation of GUIDAR technology," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 20, no. 5, pp. 16–26, May 2005.

[21] K. Harman, B. Hodgins, and J. Patchell, "Experience with ranging buried cable sensing," in *Proc. 41st Annu. IEEE Int. Carnahan Conf. Secur. Technol.*, Ottawa, ON, Canada, Oct. 2007, pp. 193–200.

[22] R. K. Harman, "Intrepid MicroTrack leaky cable sensor," in *Proc. 36th Annu. Int. Carnahan Conf. Secur. Technol.*, Atlantic, NJ, USA, Oct. 2002, pp. 191–197.

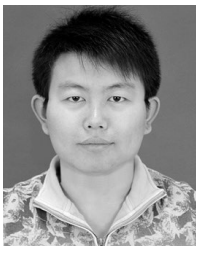
[23] C. Lo and C. Furse, "Noise-domain reflectometry for locating wiring faults," *IEEE Trans. Electromagn. Compat.*, vol. 47, no. 1, pp. 97–104, Feb. 2005.

[24] R. M. Narayanan, "Through-wall radar imaging using UWB noise waveforms," *J. Franklin Inst.*, vol. 345, no. 6, pp. 659–678, Sep. 2008.

[25] D. Grodensky, D. Kravitz, and A. Zadok, "Ultra-wideband microwave-photonic noise radar based on optical waveform generation," *IEEE Photon. Technol. Lett.*, vol. 24, no. 10, pp. 839–841, May 15, 2012.

[26] B. Colak, O. Cerezci, Z. Demir, M. Yazici, B. Turetken, and I. Araz, "Calculation of leakage through apertures on coaxial cable braided screens," in *Proc. MMET*, Kiev, Ukraine, Sep. 2002, pp. 473–475.

[27] H. Xu, B. J. Wang, J. G. Zhang, L. Liu, Y. Li, Y. C. Wang, and A. B. Wang, "Chaos through-wall imaging radar," *Sens. Imag.*, vol. 18, no. 1, p. 6, Jan. 2017.



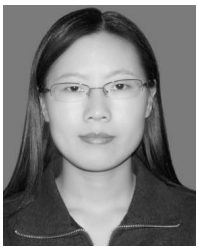
HANG XU received the Ph.D. degree in physical electronics from the Taiyuan University of Technology, China, in 2015. He is currently a Lecturer with the Key Laboratory of Advanced Transducers and Intelligent Control System, Ministry of Education and Shanxi Province, Taiyuan University of Technology. His research interests include through-wall imaging radar, life-detection radar, and intrusion detection sensor.

RUIXIN XIE received the B.Eng. degree from the Hunan University of Science and Technology, China, in 2017. He is currently pursuing the M.Eng. degree with the Taiyuan University of Technology. His research interest includes leaky coaxial cable sensor for perimeter intrusion detection.

HONG HAN received the Ph.D. degree in optics from the Harbin Institute of Technology, China, in 2014. She is currently an Associate Professor with the Key Laboratory of Advanced Transducers and Intelligent Control System, Ministry of Education and Shanxi Province, Taiyuan University of Technology. Her research interests include the dynamic features of chaotic lasers and chaotic security communication.

ZHAOXIA ZHANG received the Ph.D. degree in circuit and system from the Taiyuan University of Technology, China, in 2010. She is currently a Professor with the College of Physics and Optoelectronics, Taiyuan University of Technology. Her research interests include through-wall imaging radar, life-detection radar, and cognitive radar.

JIANGUO ZHANG received the Ph.D. degree in circuit and system from the Taiyuan University of Technology, China, in 2013. He is currently an Associate Professor with the Key Laboratory of Advanced Transducers and Intelligent Control System, Ministry of Education and Shanxi Province, Taiyuan University of Technology. His research interest includes microwave photon radar.



LI LIU received the Ph.D. degree in physical electronics from Beihang University, China, in 2011. She currently is an Associate Professor with the Key Laboratory of Advanced Transducers and Intelligent Control System, Ministry of Education and Shanxi Province, Taiyuan University of Technology. Her research interests include through-wall imaging radar, life-detection radar, and ground penetrating radar.

BINGJIE WANG received the Ph.D. degree in circuit and system from the Taiyuan University of Technology, China, in 2012. She is currently an Associate Professor with the Key Laboratory of Advanced Transducers and Intelligent Control System, Ministry of Education and Shanxi Province, Taiyuan University of Technology. Her research interests include laser radar and time-domain reflectometry.

LIQIANG LI received the B.Eng. degree from Hubei Engineering University, China, in 2017. He is currently pursuing the M.Eng. degree with the Taiyuan University of Technology. His research interest includes chaos through-wall imaging radar.