Regular Paper

Radio Propagation Characteristics-based Spoofing Attack Prevention on Wireless Connected Devices

Mihiro Sonoyama[1,a)] Takatsugu Ono[2,b)] Haruichi Kanaya[2,c)]
Osamu Muta[3,d)] Smruti R. Sarangi[4,e)] Koji Inoue[2,f)]

Received: July 25, 2018, Accepted: November 27, 2018

Abstract: A spoofing attack is a critical issue in wireless communication in which a malicious transmitter outside a system attempts to be genuine. As a countermeasure against this, we propose a device-authentication method based on position identification using radio-propagation characteristics (RPCs). Not depending on information processing such as encryption technology, this method can be applied to sensing devices etc. which commonly have many resource restrictions. We call the space from which attacks achieve success as the "attack space." In order to confine the attack space inside of the target system to prevent spoofing attacks from the outside, formulation of the relationship between combinations of transceivers and the attack space is necessary. In this research, we consider two RPCs, the received signal strength ratio (RSSR) and the time difference of arrival (TDoA), and construct the attack-space model which uses these RPCs simultaneously. We take a tire pressure monitoring system (TPMS) as a case study of this method and execute a security evaluation based on radio-wave-propagation simulation. The simulation results assuming multiple noise environments all indicate that it is possible to eliminate the attack possibility from a distant location.

Keywords: wireless communication, device authentication, spoofing attack, radio propagation characteristics

1. Introduction

Wireless sensing devices have been becoming more popular because these improve design flexibility by means of eliminating wiring cost [1], [2]. Since there is no physical constraint in transmitting and receiving the radio wave, however, system designers face a critical security issue called a *spoofing attack* [3]. A spoofing attack is a threat in which an attacker causes the system to behave erroneously by pretending to be genuine and by transmitting fake signals remotely. It has the potential to become the first step for achieving the other attacks, including sniffing, man-in-the-middle and energy exhausting [4], [5].

To prevent spoofing attacks, authentication methods based on common or public key encryption are applied [6], [7]. However, these methods have problems such as a risk of key information leakage and an enormous calculation cost for encrypting and decrypting data [8], [9]. Since the devices used in the embedded systems or sensor networks generally need to operate in a constrained resource environment, a device-authentication method in which key-information management is not needed is required.

To solve the aforementioned problems, we propose a spoofing-attack detection and prevention method on radio-wave communications. For systems in which the range of wireless communication is fixed and closed like in cars, it is entirely reasonable to assume that there is no trial of spoofing attacks from inside. Therefore, a receiver (RX) should reject signals transmitted from outside the system. Our purpose is to define a spatial boundary, inside of which is called an *attack space* where spoofing attacks achieve success, to make the RX has the ability for boundary checking. If the signal comes from inside the attack space, the RX regards it as an authorized communication. Otherwise, the RX rejects the signal as a spoofing attack. If we can confine the attack space to within the system, remote spoofing attacks can be completely prevented.

The questions that need to be addressed are: *how can the attack space be defined?*, and *how can designers confine the attack space to within the system?* For the first question, we exploit the radio-propagation characteristics (RPCs), e.g., the received signal strength. Since RPCs depend only on physical phenomena, i.e., the operation environment in the system, it is impossible to tamper with them remotely. To answer the second question, we construct the attack-space model using two RPCs for determining the positions of the TX and RX because the size and shape of the attack space depend on this positional relationship. Based on the analysis of the model, system designers can position the TX and RX appropriately for confining the attack space inside the system.

[1] Graduate School of Information Science and Electronic Engineering, Kyushu University, Fukuoka 819–0395, Japan
[2] Faculty of Information Science and Electrical Engineering, Kyushu University, Fukuoka 819–0395, Japan
[3] Center for Japan-Egypt Cooperation in Science and Technology, Kyushu University, Fukuoka 819–0395, Japan
[4] Department of Computer Science and Engineering, Indian Institute of Technology Delhi, New Delhi 110016, India
[a)] mihiro.sonoyama@cpc.ait.kyushu-u.ac.jp
[b)] takatsugu.ono@cpc.ait.kyushu-u.ac.jp
[c)] kanaya@ed.kyushu-u.ac.jp
[d)] muta@ait.kyushu-u.ac.jp
[e)] srsarangi@cse.iitd.ac.in
[f)] inoue@ait.kyushu-u.ac.jp

The contributions of this paper are as follows [*1].

- In Section 3, we construct the attack-space models based on the received signal strength ratio (RSSR) and the time difference of arrival (TDoA) as the RPCs to define the space boundary. Moreover, we also propose a combination model of RSSR and TDoA to compensate for the disadvantages of the two models and efficiently confine the attack space to the system.
- In Section 4, we introduce the probability distribution which indicates the noise occurring on the RSSR value of attacking signals in order to make it possible to evaluate the system security. Comparing the probabilistically-generated value and the theoretical value, we qualitatively study the impact of the noise of attacking signals on the proposed method.
- In Section 5, we quantitatively evaluate the security of the combined model by using the radio-propagation simulation. We set the multiple simulation environments and attack scenarios taking TPMS as a case study of our method. The results show that it is impossible for the attackers far away from the genuine TX to complete an attack. Furthermore, we show that the proposed method potentially extends the TX lifetime by about 1.5 times through the cost evaluation while comparing with a lightweight MAC-based authentication method.

2. Background

2.1 Threat Model and Target Systems

The systems which our proposal can be applied to satisfy the following conditions: 1) make use of wireless communication, and 2) a legitimate physical communication range can be determined at the system design stage. We focus on the spoofing attacks from the outside of the communication range determined in 2) that attempt to cause the system to behave erroneously. In this paper, we assume that the inside of a system is safe, i.e., the threats come only from outside the system. We believe this assumption is reasonable because mounting a malicious TX inside the system is impractical.

The greatest feature of our method is that it does not depend on information processing such as key management and encryption processing at all. Therefore, for example, the implementation of the devices which have the requirement of low power operation or miniaturization is particularly effective. The following three are the specific examples of the systems and its spoofing problems.

Embedded Systems

Various sensors and actuators are mounted in embedded systems such as vehicles, appliances, and autonomous robots. Some of them cannot be connected to the control unit via wire, and in that case, the wireless communication will be employed. Direct TPMS in which a TX is attached to the corresponding tire is a typical example. For TPMS, the range of legitimate communication is inside the car body. Since most products do not support battery replacement and it is necessary to replace the device or the whole tire when the battery runs out, low-power operation is highly required for the TX. In fact, Rouf et al. and Xu et al. each explored commercially available TPMSs and both revealed that no authentication is executed in the RX connected to the control unit on the car body [11], [12]. In this paper, we employ a TPMS as a case study and validate the proposed method.

Smart Home Devices

Smart home whereby users monitor and manage their house using Internet-connected devices is a typical example of the IoT systems. Devices that construct the system are appliances, lights, remote controllers, locks, and plugs etc. Many of them are connected to smart home gateways, such as Amazon Echo and Google Home, via radio channels and are operated. The legitimate communication range of smart home systems is inside the home. Ling et al. explored a commercially available smart plug that can be monitored and operated from the application on the smartphone [13]. As a result, they reported that the system does not have the authentication function of the plug and the spoofing actually succeeds. Li et al. prepared a second channel of infrared, ultrasound and modulated visible light in addition to the radio wave channel, and proposed a challenge-response authentication mechanism using these hybrids [14]. Since each second channel wave is blocked by a wall, only the devices inside the home can be authenticated. The meaning is different, however, its basic concept is the same to our proposal.

Implantable Medical Devices (IMDs)

IMDs responsible for monitoring the physical condition and maintaining the health of the user continue to progress and spread. These devices need to be wirelessly connected to devices outside the body, and some of them can be operated by the owner using a remote controller. The communication range needs to be confined to its close proximity and inside the trusted medical facility. In addition, since the replacement of the battery or the device itself induces a heavy physical burden, risks, and costs to the patient, the requirement for saving power consumption is more severe than in the above two systems. Burleson et al. reported that it is possible to spoof transmission packets of the glucose sensor used in combination with an insulin pump and manipulate the dosage of insulin from a distant location [15]. The paper by Rasmussen et al. introduced in Ref. [15] proposed an authentication method which utilizes ultrasonic wave to decide the distance boundary of communications [16]. This suggests the applicability of our method in the field of IMDs.

2.2 Related Work

To detect spoofing attacks, it is necessary to carry out device authentication of the transmission source from the received signals. A general method for device authentication is to carry out encryption processing, such as a message authentication code (MAC), for each round of communication [6]. Since key infor-

[*1] We have introduced the fundamental concept of the attack space at the 15th IEEE International Conference on Dependable, Autonomic and Secure Computing 2017 [10]. In Ref. [10], the verification assuming a specific application is not done. Moreover, the statistical methods are not applied to the modeling and evaluation and many challenging remains to be realized. In this paper, we introduce a simulation environment in which the impact of noise on observed values is represented by the probability distribution, and present a case study of a TPMS as an example.

mation is necessary for MAC calculation, a device without key information cannot create the correct code. As a result, the RX can accurately determine the authenticity of the signal.

In the context of wireless sensing devices, due to constraints arising from the lack of battery power, and real-time requirements, the overhead of encryption in some cases may be prohibitive [9]. Furthermore, in a system where a large number of nodes cooperatively operate such as the wireless sensor networks (WSNs), preparing the common keys for each of communication party makes secure key management even more difficult. To solve these problems, the methods for lightweight key generation and key management for IoT devices such as WSNs are studied [5], [17].

However, once the attacker obtains the key information, the RX can no longer execute normal device authentication, and secure communication is not guaranteed. For example, in 2014, an attacker obtained a large amount of information including secret keys due to a bug in the encryption software called Heartbeat, which is an extension function of OpenSSL [8]. In this way, the leakage of key information is a real problem. Although the information-theoretically secure one-time key generation schemes based on natural phenomena have been proposed in the literature [18], [19], the applicability remains challenging because the additional resources such as dedicated antennas are required.

Recently, research on device authentication on the physical layer in wireless communication has been actively conducted. The basic philosophy of these methods is to eliminate the need for the encryption processing and secret information management by using physical information for the authentication as a substitute for the key information. There are two approaches, one is using individual differences of devices caused by manufacturing variation [20], [21], and the other is based on the RPCs [4], [9], [22], [23], [24], [25], [26], which includes our proposal. The difference between our proposal and Refs. [4], [9], [22], [23], [24] is whether the target space is modelable and controllable. In particular, Refs. [23], [24] are not suitable for space definition because they use the spatial randomness of the frequency response. Refences [25], [26] are related studies that attempt to define the space for secure wireless communication by using the received signal strength (RSS) and the RSSR. Reference [25] simply uses RSS as the target RPCs, on the other hand, it requires the complicated calculation in association with a rich estimation algorithm such as the comparison with the previous state. Our approach does not memorize a state etc. and performs the localization only with a target signal. Reference [26] covers only the case in which a genuine RX and multiple fake TXs are aligned on a straight line, whereas our attack-space models are much more general due to three-dimensional analysis.

Physical layer authentication using RPCs is basically based on the mapping technique from the observed RPCs to the device location. In estimates the distances or angles to the target device through the RSS, time of arrival (ToA), angle of arrival (AoA), etc., and combines a plurality of them to specify the position of the target device [27], [28], [29], [30], [31]. Since monitoring RPCs can be fundamentally achieved without adding any dedicated hardware or signals, a power-hungry cost-inefficient computing environment is also not needed.

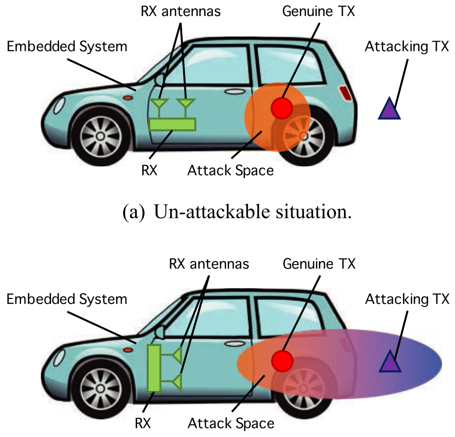
Although our method stands on the localization technique on wireless communications, when we consider methods to prevent spoofing attacks in embedded systems, there are fundamental differences from conventional localization techniques. First, the interest is in detecting whether the source of received signals comes from inside a system, so it is not necessary to estimate the precise position of the TX, e.g., using the graph theory or Bayesian model estimation [32], [33], [34]. Second, we attempt to define and control the physical space (attack space) where the RX trusts received signals by exploiting the RPCs to detect spoofing attacks. To achieve this purpose, we introduce geometric models of the attack space. Traditional localization studies are aimed at improving the estimation accuracy, whereas our final goal is to theoretically clarify the possibility of spoofing attacks and prevent them at the system-design stage.

3. Radio Propagation Characteristics Based Spoofing-attack Prevention

3.1 Overview

Figure 1 depicts the concept of our proposed method. Although we refer to the RSS as an example of an RPC in this section, it can be applied to other RPCs such as ToA. We consider a vehicular system including the TPMS as an example. The physical distance between the genuine TX and RX is decided at the design stage. That is, if the transmission power is constant, the received power is also always constant. A straightforward approach to prevent spoofing attacks using this property is to cancel received signals that have inappropriate RSS values, e.g., a fake signal transmitted from outside the system tends to be with too weak an RSS as compared to a genuine one. However, such a simple implementation has a critical vulnerability. If the attacker can estimate the physical distance between the fake TX and RX, amplifying the transmission power appropriately enables spoofing attacks.

It is possible to solve this issue by using two RX antennas and exploiting the RSSR for spoofing-attack detection because the RSSR does not depend on the transmission power. In this case,



(a) Un-attackable situation.

(b) Attackable situation.

Fig. 1 Conceptual diagram of attack space.

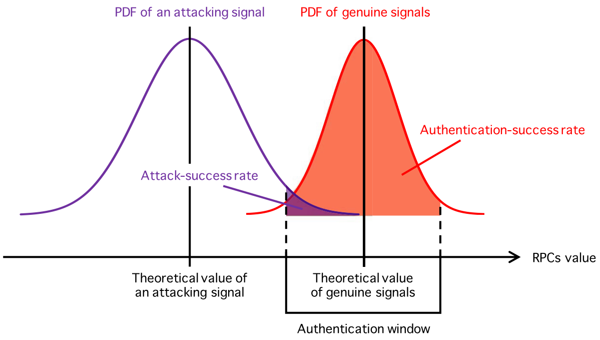


Fig. 2 Two types of noise to be considered.

the space where TX has the possibility to provide an appropriate RSSR is defined as the attack space. The shape of the attack space also depends on the positional relationship of TX and RX antennas similar to the RSSR itself. The location of the TX is inevitably decided based on the application and sensing target (the wheel in the TPMS case), system designers can control the attack space by carefully placing RX antennas. If the designers can confine the attack space to inside the system (vehicle body in our example), it is possible to prevent spoofing attacks, as illustrated in Fig. 1 (a). Otherwise, the system is exposed to the threat, as shown in Fig. 1 (b).

While we focus on the RSSR and TDoA as RPCs in this paper, in the actual environment, the observed RPCs values fluctuate due to the noise occurring in the propagation process of radio waves and the hardware manufacturing variation. Thus, we have to consider the following two types of noise separately as shown in **Fig. 2**.

Noise on the Genuine Signals

The probability density function (PDF) drawn by the red line in Fig. 2 indicates the fluctuation of the RPCs value of the genuine signals. Considering this fluctuation, the actual authentication is executed based on a determination as to whether the observed RPCs value falls within a certain range, called the *authentication window*. it becomes possible to obtain the theoretical RPCs value of the genuine signals by constructing the attack-space models. Moreover, since system designers can probe the genuine communication channel in detail, we can assume that the probability distribution of RPCs values are given. In the case of TPMS, the impact of the presence of chassis and tire wheels etc. on RPCs can be modeled in advance. We do not mention its detail in this paper, but please refer to Refs. [35], [36] etc. That is, the designers can appropriately decide the authentication window to meet required authentication-success rate.

Noise on Attacking Signals

Like the genuine signals, the theoretical RPCs value of signals from an attacker can be obtained through the attack-space modeling. However, since the communication environment of attackers cannot be probed in advance, the designers cannot obtain the probability distribution such as the purple line in Fig. 2. In the case of TPMS, the impact of the environment outside the vehicle on the attacking signals from the roadside is unknown. That is, we have to assume a specific distribution in order to estimate the attack-success rate filled in purple in Fig. 2.

From the above, to discuss the validity of the proposed method, the following steps need to be carried out: 1) establish the deriving method of the theoretical RPCs values, i.e., the attack-space model, 2) analyze the attack space based on the authentication window determined by a channel probing, and 3) evaluate the security of the system assuming the probability distribution which derives the fluctuation of attacking signals. The purpose of this section, which corresponds to 1) and 2) above, is to construct attack-space models to allow system designers to decide the position of RX antennas and control the attack space. The discussion about 3) is given in Section 4 and Section 5.

3.2 RSSR-based Attack-space Model

Hereafter, we assume that one TX and two RX antennas are mounted in the system, and refer to the RX antenna close to the TX as RA1 and the other one as RA2. The attenuation of radio waves in free space, in which radio waves propagate spherically without noise, is generally expressed by the Friis transmission equation, as shown in Eq. (1).

$$P_{rn} = P_t G_t(\theta_{tn}, \phi_{tn}) G_{rn}(\theta_{rn}, \phi_{rn}) \left(\frac{\lambda}{4\pi D_{trn}} \right)^2 \quad (1)$$

where P_{rn} is the received power at RAn, P_t is the transmitted power, G_t/G_{rn} is the gain of TX/RAn, λ is the wavelength, and D_{trn} is the distance between the TX and RAn. In addition, θ_{tn} and ϕ_{tn} indicate the elevation angle and azimuth angle from the TX towards RAn, and θ_{rn} and ϕ_{rn} indicate the elevation angle and azimuth angle from RAn toward the TX, respectively. The RSSR of RA1 and RA2 is given by Eq. (2).

$$RSSR = \frac{P_{r1}}{P_{r2}} \quad (2)$$

A set of points where the value of Eq. (2) matches the genuine value is defined as the attack space and is shown in Fig. 1. TXs existing in this space are authenticated as genuine. Substituting Eq. (1) for P_{r1} and P_{r2} in Eq. (2) yields Eq. (3).

$$RSSR = \frac{G_t(\theta_{t1}, \phi_{t1}) G_{r1}(\theta_{r1}, \phi_{r1}) D_{tr2}^2}{G_t(\theta_{t2}, \phi_{t2}) G_{r2}(\theta_{r2}, \phi_{r2}) D_{tr1}^2} \quad (3)$$

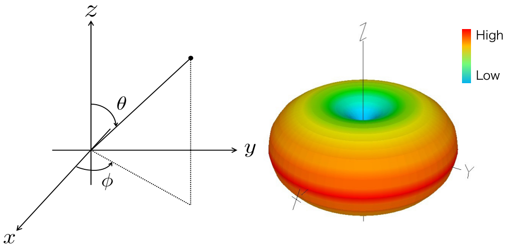
That is, the RSSR is determined by the antenna gain of TX/RX and the distance between them.

The gain of the antenna is an index showing how many times the radiation-power intensity of the target antenna is that of the reference antenna, and is expressed by the product of the square of the directivity function $Dir(\theta, \phi)$ and the constant k as shown in Eq. (4).

$$G(\theta, \phi) = kDir(\theta, \phi)^2 \quad (4)$$

Note that the directivity is a strength characteristic that depends on the antenna type and the direction of propagation of radio waves. Substituting Eq. (4) into Eq. (3), $RSSR$ can be represented as

$$RSSR = \frac{Dir_t(\theta_{t1}, \phi_{t1})^2 Dir_{r1}(\theta_{r1}, \phi_{r1})^2 D_{tr2}^2}{Dir_t(\theta_{t2}, \phi_{t2})^2 Dir_{r2}(\theta_{r2}, \phi_{r2})^2 D_{tr1}^2}. \quad (5)$$



(a) Correspondence between coordinate systems. (b) Directivity of half-wave dipole antenna.

Fig. 3 Directivity on rectangular coordinate system.

Because we assume that the configuration of the genuine TX and RA1/RA2 is decided and fixed at the design stage of the system, the right-hand side of Eq. (5) can be regarded as constants. Thus, the RSSR value of genuine signals is also constant. On the other hand when we consider attacking signals, In addition to the change of θ_{rn}, ϕ_{rn}, and D_{trn} along with the change of TX's position, the value of $Dir_{tn}(\theta_{tn}, \phi_{tn})$ depends on the installation angle and antenna type of TX. The shape of the attack space consequently changes.

In this paper, we assume that the genuine TX, RA1/RA2 and the attacking TX are all half-wave dipole antennas, which are commonly used as a standard antennas. The directivity function of a half-wave dipole antenna is given in Eq. (6).

$$Dir_d(\theta, \phi) = Dir_d(\theta) = \frac{\cos\left(\frac{\pi}{2}\cos\theta\right)}{\sin\theta} \qquad (6)$$

The correspondence between the rectangular coordinate system and the spherical coordinate system in this situation is shown in **Fig. 3** (a). Moreover, the directivity when the antenna is arranged parallel to the z-axis on the rectangular coordinate system is shown in Fig. 3 (b). Equation (6) and Fig. 3 (b) indicate that a half-wave dipole antenna radiates radio waves equally in all directions on the ϕ plane but not on the θ plane.

As mention above, the value of $Dir_t(\theta_{tn}, \phi_{tn})$ changes by changing the directivity function or the arguments representing the installation angle. In this paper, we apply multiple values to $Dir_t(\theta_{tn}, \phi_{tn})$ by applying multiple installation angles while the antenna type of attacking TX is fixed to a half-wave dipole antenna. Since Dir_d is a function of only the elevation angle, it is only necessary to derive Θ that is the elevation angle after antenna rotation.

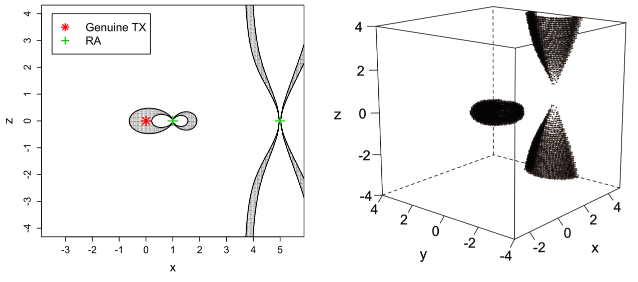
The transformation from the spherical coordinate system to the rectangular coordinate system is given by Eq. (7).

$$\begin{cases} x = r\sin\theta\cos\phi \\ y = r\sin\theta\sin\phi \\ z = r\cos\theta \end{cases} \qquad (7)$$

The transformation from (x, y, z) to (X, Y, Z), which rotate α [rad] in the θ direction and β [rad] in the ϕ direction, is given by the following rotation matrix.

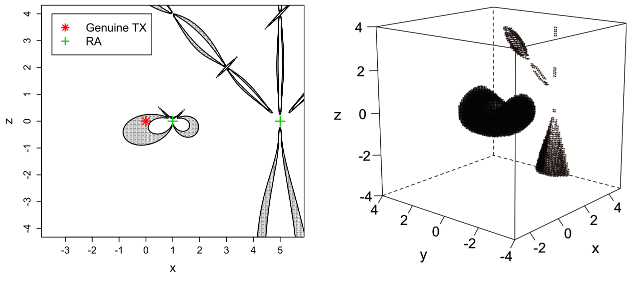
$$\begin{bmatrix} X \\ Y \\ Z \end{bmatrix} = \begin{bmatrix} \cos\alpha & 0 & \sin\alpha \\ 0 & 1 & 0 \\ -\sin\alpha & 0 & \cos\alpha \end{bmatrix} \begin{bmatrix} \cos\beta & -\sin\beta & 0 \\ \sin\beta & \cos\beta & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} \qquad (8)$$

Equations (7) and (8) yield Eq. (9).



(a) Two dimensions. (b) Three dimensions.

Fig. 4 RSSR attack-space ($\alpha = 0, \beta = 0$).



(a) Two dimensions. (b) Three dimensions.

Fig. 5 RSSR attack-space ($\alpha = \frac{\pi}{4}, \beta = 0$).

$$\begin{bmatrix} X \\ Y \\ Z \end{bmatrix} = r \begin{bmatrix} \sin\theta\cos\alpha\cos(\phi+\beta) + \cos\theta\sin\alpha \\ \sin\theta\sin(\phi+\beta) \\ -\sin\theta\sin\alpha\cos(\phi+\beta) + \cos\theta\cos\alpha \end{bmatrix} \qquad (9)$$

Therefore, the elevation angle Θ after these rotations is given by Eq. (10).

$$\begin{aligned} \Theta(\theta, \phi) &= \mathrm{Cos}^{-1}\left(\frac{Z}{r}\right) \\ &= \mathrm{Cos}^{-1}(-\sin\theta\sin\alpha\cos(\phi+\beta) + \cos\theta\cos\alpha) \end{aligned} \qquad (10)$$

We denote $\Theta(\theta_{t1}, \phi_{t1})$ as Θ_{t1}, $\Theta(\theta_{t2}, \phi_{t2})$ as Θ_{t2}.

Substituting Dir_d in Dir_t and Dir_{rn} in Eq. (5) yields Eq. (11).

$$RSSR = \frac{Dir_d(\Theta_{t1})^2 Dir_d(\theta_{r1})^2 D_{tr2}^2}{Dir_d(\Theta_{t2})^2 Dir_d(\theta_{r2})^2 D_{tr1}^2}. \qquad (11)$$

By applying Eq. (6) to Eq. (11), the model formula of the attack space is constructed.

$$RSSR = \frac{\cos^2\left(\frac{\pi}{2}\cos\Theta_1\right)\cos^2\left(\frac{\pi}{2}\cos\theta_1\right)\sin^2\Theta_2\sin^2\theta_2 D_{tr2}^2}{\cos^2\left(\frac{\pi}{2}\cos\Theta_2\right)\cos^2\left(\frac{\pi}{2}\cos\theta_2\right)\sin^2\Theta_1\sin^2\theta_1 D_{tr1}^2} \qquad (12)$$

By deriving Eq. (12) above, the step 1) in Section 3.1 is achieved. Subsequently, we perform the analysis of the attack space, which means to complete the step 2) in Section 3.1. **Figures 4** and **5** show the attack space for different α and β where the genuine TX and RA1/RA2 are installed at $(0, 0, 0)$, $(1, 0, 0)$, $(5, 0, 0)$ respectively, and the authentication window is 12.0 to 37.0. This range is set considering the rotational motion of the TXs along the diameter of the tire, as we describe in Fig. 12, Section 5.1 in detail. We use this window also in the following discussion for simplicity. The filled areas in Fig. 4 (a)/Fig. 5 (a) and the black areas in Fig. 4 (b)/Fig. 5 (b) illustrate the attack space.

Figures 4 (a) and 5 (a) are planes of $y = 0$ in (b) of each figure. Note that the genuine TX and RA1/RA2 plotted in the sectional view (a) are not plotted in the three-dimensional view (b). These results show the two critical problems. First, the shape of the attack space greatly changes by adjusting the directivity of the attacking TX. In this way and in the case in which the possibility of attacks is caused by a variation in the attacking TX, it is not possible to define the attack space. Second, the attack space cannot be limited to a finite space uniquely. When there is a possibility of an attack from an infinite distance, the attacking TX can enter the attack space no matter where the system designer places the communication devices. If the above problems cannot be solved, we cannot prevent spoofing attacks.

3.3 TDoA-based Attack-space Model

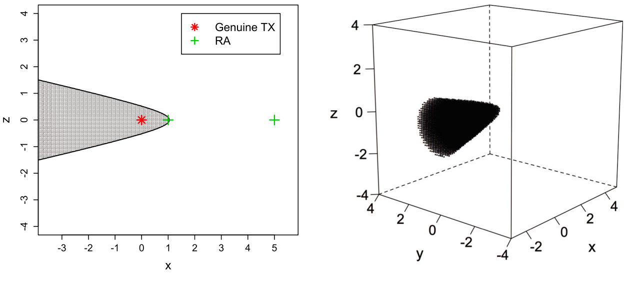
There is a method of estimating the distance between the TX/RX using the transmission-time information added to the signal. With this method, the RX calculates the difference between the arrival time of the signal and the transmission time of the signal. With regard to spoofing attacks, the attacking TX can tamper with transmission-time information, and the RX cannot make a true/false judgment of the received transmission-time information. Therefore, it is impossible to estimate the correct distance for false signals and we cannot take this approach.

It is possible to estimate the position of the TX without the information of transmission time by using the difference in signal arrival time at two RX antennas, that is TDoA. In this paper, we assume that signals always propagate at the speed of light c. Based on this assumption, the TDoA of RA1 and RA2 is given by Eq. (13).

$$TDoA = \frac{D_{tr2} - D_{tr1}}{c} \tag{13}$$

That is, the TDoA is determined only by the distance between TX and RA1/RA2. As in the case of RSSR, a set of points where the value of Eq. (13) falls within the authentication window is defined as the attack space. **Figure 6** shows the attack space with the same arrangement of TX and RA1/RA2 as Fig. 4, and the authentication window is $\frac{3.9}{c}$ to $\frac{4}{c}$. In this figure, the filled areas in (a) and black areas in (b) are the attack spaces akin to Fig. 4. (a) is a plane of $y = 0$ in (b). Since in three-dimensional space, one sheet of the hyperboloid is equidistant from two points, the attack space becomes the inside of it.

Regarding the TX and RA1/RA2 arrangement of Fig. 6, the maximum TDoA value is $\frac{4}{c}$ and the minimum TDoA value is 0. Where 1 unit of each axis is 0.3 [m], the maximum value is 4×10^{-9} [s] = 4 [ns]. When taking a digital circuit or a software approach as an example of an implementation for measuring TDoA, the time resolution depends on the sampling frequency of the A/D converter that converts the received analog signal into the digital signal. To observe 4 [ns] as TDoA, 250 [MHz] or more sampling frequency, which is the reciprocal of 4 [ns], is necessary. Besides, the sampling frequency for detecting $\frac{3.9}{c}$ as TDoA is approximately 256 [MHz], which is the required sampling-frequency to obtain the attack space of Fig. 6.



(a) Two dimensions. (b) Three dimensions.

Fig. 6 TDoA attack-space.

Unlike the RSSR model, it is not necessary to consider anything else other than the position information of the attacking TX in the TDoA-based model since the propagation speed of the signal does not depend on the antenna's directivity. Therefore, there is no possibility of attack caused by adjustment of the attacking TX, similar to what is shown in Figs. 4 and 5. Furthermore, we do not have to consider the fluctuation of TDoA value because the change in the propagation speed of radio waves due to the noise is negligibly small compared with the above-mentioned time resolution 4 [ns]. However, the possibility of attack from an infinite distance still exists. From the above, like the RSSR, even with TDoA, spoofing attacks cannot be prevented in the model using two RX antennas.

3.4 Attack-space Model Combining RSSR and TDoA

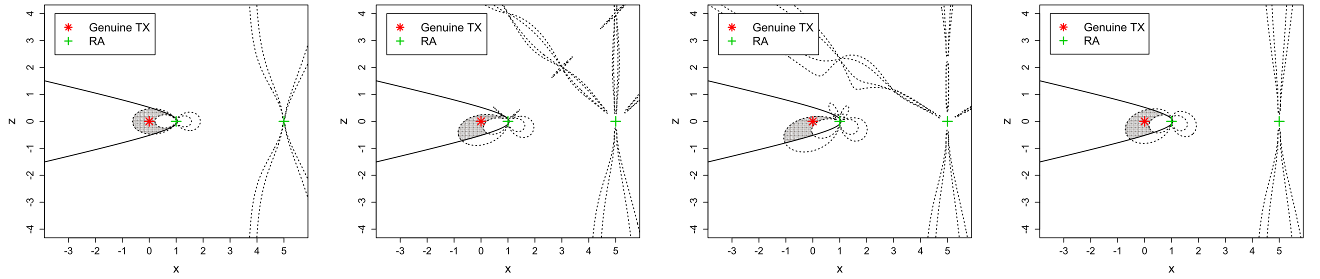
The condition to prevent spoofing attacks that we clarify by constructing the RSSR- and TDoA-based attack-space models is that *the attack space can be limited to a finite space regardless of the directivity of the attacking TX*. In addition, we confirm that neither model is potent enough to satisfy this condition just by itself. However, as explained in Section 3.3, the TDoA-based model can restrict the direction of the attack space. In contrast, we can exploit RSSR to confine the attack space in terms of distance. In this way, it is possible to construct a model satisfying the above condition by using the two models complementarily, i.e., measuring both RSSR and TDoA for each signal.

Figure 7 draws the boundary of the RSSR attack-space for multiple installation angles of the attacking TX by dotted lines and the boundary of the TDoA attack-space by solid lines. Moreover, the filled areas show the intersection of the RSSR and TDoA attack spaces, that is, the set of points in which we can satisfy both of the authentication conditions. We define it as the attack space of the combination model. In all figures in Fig. 7, since the attack spaces are confined to a finite space, we can confirm that the combined model has the availability for these installation angles of the attacking TX. Note that we discuss the comprehensive verification for arbitrary installation angles in Section 5.

4. Consideration of Noise

4.1 Multipath Fading

In this paper, we regard multipath fading, which is the noise occurring in the propagation process of radio waves, as the main cause of observation error on the RSSR of attacking signals. In this section, as the preparation for achieving the step 3) in Section 3.1, we introduce its probability distribution and give the qualitative study to the impact of the noise of attacking signals on



(a) $\alpha = 0, \beta = 0$. (b) $\alpha = \frac{\pi}{4}, \beta = 0$. (c) $\alpha = \frac{\pi}{3}, \beta = 0$. (d) $\alpha = \frac{\pi}{3}, \beta = \frac{\pi}{4}$.

Fig. 7 Attack space of combination model.

the proposed authentication method. Note that the noise model to be described below represents the impact of the environment outside the system on attacker signals, and does not represent the impact of components inside the system. The reason why we do not consider the impact of the components inside the system on RPCs is that we assume it can be modeled or estimated at the design stage of the system and will not affect the accuracy of the authentication.

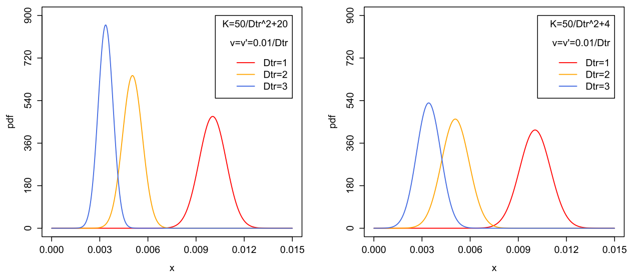
The signal radiated into space arrives at the RX antenna as not only the direct wave but also scattered waves due to reflection, diffraction, etc., and the wave obtained by combining these waves is the received signal. The fluctuation of the RSS caused by the phase relationship of signals propagating on different paths is called multipath fading. When we represent the RSS in a multipath fading environment via probability distributions, there are several variations depending on the communication environment. Yao et al. conducted the experiments regarding Vehicular Ad Hoc Networks (VANETs) using real vehicles with antennas for transmitting and receiving on the roof [37]. As a result of observing and analyzing its RSS value, they reported that for communication within 100 [m], the noise can be represented by a normal distribution in all three environments, campus, rural area, and urban area. This suggests that in most cases, the modeling of the fluctuation of the RSS on road environments can be achieved via a simple probability distribution, not complicated propagation models. In this paper, we apply the Rice distribution $Rician(v, \sigma)$ to the model, which is suitable to represent multipath fading where there is a direct wave in the line-of-sight (LOS) [38]. The PDF of $Rician(v, \sigma)$ is given by Eq. (14).

$$f(x)|_{v,\sigma} = \frac{x}{\sigma^2} \exp\left(-\frac{x^2 + v^2}{2\sigma^2}\right) I_0\left(\frac{xv}{\sigma^2}\right) \qquad (14)$$
$$(x > 0,\ \sigma > 0,\ v > 0)$$

Where x is the received amplitude, I_0 is the modified Bessel function of the first kind with order zero. Parameter v is the amplitude of the direct wave through LOS, and σ^2 is the received power of the scattered wave.

To derive the value of σ on each point, we introduce the Rice coefficient K which represents the S/N ratio of the received signal. Letting v' be the received amplitude without consideration of the directional gain, the relationship between σ and K is given by Eq. (15).

$$K = \frac{v'^2}{2\sigma^2} \qquad (15)$$



(a) $(C_1, C_2) = (50, 20)$. (b) $(C_1, C_2) = (50, 4)$.

Fig. 8 Probability density function of Rice distribution.

In this work we assume that K value monotonously decreases as the communication distance increases, and converges to a certain constant value. Based on this assumpsion, we project the K value at each point by the function of D_{tr}, the distance between TX and RX antenna, shown in Eq. (16).

$$K = \frac{C_1}{D_{tr}^2} + C_2 \qquad (16)$$

The positive constants C_1 and C_2 indicate the sensitivity of the function and the minium value respectively. First, we find v' substituting P, the received power obtained from the Friis transmission formula with $G_t = G_{rn} = 1$, into Eq. (17).

$$v' = \sqrt{2P} \qquad (17)$$

Calculating K from Eq. (16) and substituting v' and K into Eq. (15), we derive the unique value of σ for each point.

Figure 8 shows the PDF of $Rician(v, \sigma)$. In both Figs. 8 (a) and 8 (b), the transmission power is set so that $v' = 0.01$ when $D_{tr} = 1$ and v is equal to v'. Hereafter, the unit of D_{tr} in Eq. (16) is unified to [m]. Figure 8 (a) shows the distributions with $(C_1, C_2) = (50, 20)$ while Fig. 8 (b) shows the distributions with $(C_1, C_2) = (50, 4)$. We can find the following insights through these figures. 1) As the value of v increases with decreasing D_{tr}, the standard deviation increases but the coefficient of variation decreases. That is, the level of relative variation of RSS to the expected value v decreases as the TX approaches the RX antenna. 2) When the value of C_2 decreases, for example from Fig. 8 (a) to Fig. 8 (b), the standard deviation increases in the same point, above all, the change in a distant location is remarkable.

4.2 Derivation of RSSR in a Noisy Environment

We consider the situation where RA1/RA2 are installed 1.2 [m] away from each other, and signals are transmitted from the TX on

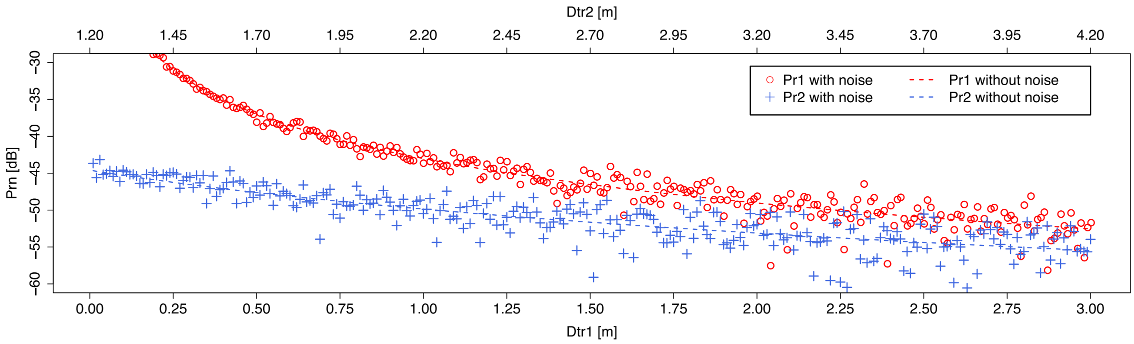


Fig. 9 Distance characteristics of P_{rn}.

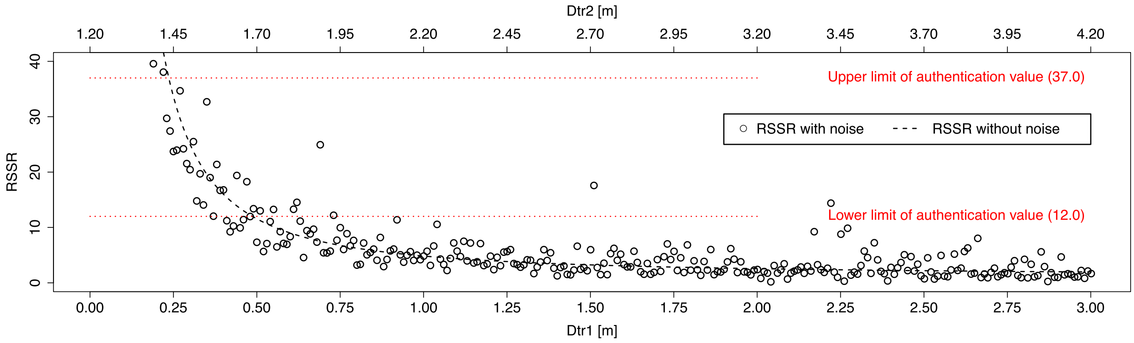


Fig. 10 Distance characteristics of $RSSR$.

the same straight line, which means $D_{tr2} - D_{tr1} = 1.2$ [m] is always established. As in Fig. 8 (b), $(C_1, C_2) = (50, 4)$, $v = v'$ and the transmission power is set so that $v' = 0.01$ when $D_{tr} = 1$. **Figure 9** shows the distance characteristics of the received power at RA1/RA2, P_{r1} (red) and P_{r2} (blue), under the above conditions. The dashed lines indicate the values without noise and the circles and crosses indicate the values with noise.

Figure 10 shows the distance characteristics of the RSSR calculated from the received power sequence in Fig. 9. The dashed line shows the value without noise and the points show the value with noise as in Fig. 9. For reference, the upper and lower limits of the authentication window are written with dotted red lines. Although the theoretical success/failure boundary of the authentication is about $D_{tr1} = 0.48$, we can find both the cases of failure at points closer than it and success at points further than it. Each of these facts means that the genuine TX fails the authentication and the attacking TX outside succeeds the spoofing.

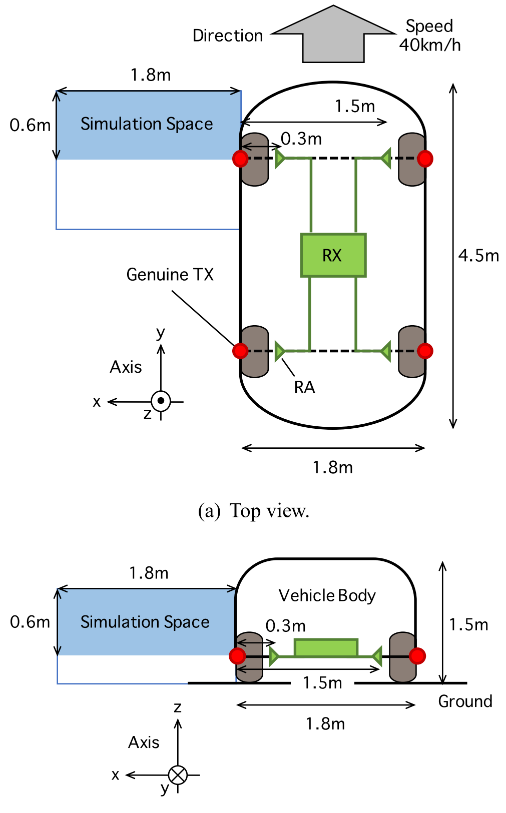
To improve the authentication-success rate of the genuine signals, we have to make the authentication window wider. However, it simultaneously increases the attack-success rate from a distant location and compromises the security of the system. Unfortunately, as long as RSSR is a physical phenomenon which can be modeled using probability distribution, it is hard to completely eliminate the attack possibility from a distant location as shown in Fig. 10. Therefore, to improve the security of the system, the devices on the authentication procedure side is also important, such as decreasing the required authentication-success rate and increasing the tolerance of attack-success rate.

5. Evaluation of the Possibility of Attacks

5.1 Evaluation Setups

As shown in Fig. 7, we have verified that the combined model works well for some particular α and β values. However, it is practically necessary to have resistance against attacking TXs with arbitrary directivities after considering the fluctuation of the attacking signals introduced in Section 4. For this reason, in this section, we calculate the attack-success rate at each point supposing these factors and perform the quantitative evaluation on the security of the proposed method. It corresponds to the completion of the step 3) in Section 3.1.

Figure 11 shows the configuration of the assumed vehicle and the simulation space. We employ the type of TPMS in which one RX, connected to or included in the control unit, has four antennas. Such kind of implementation is already commercially available. Two front antennas receive the signals from two front TXs, and the rear side is the same too. We assume RSSR and TDoA are calculated in the central RX based on the observed value on each antenna. The inside of the blue frame is a space where we evaluate the possibility of attacks, and the blue area is simulated. The reason for it is that the symmetry of the positional relationship and directivity of TX/RXs cause the symmetry of the simulation results. Regarding the size of the evaluation space, we set the width of the x-axis (the width of roadside) as the width of the vehicle, and the y- and z-axes width to a value that is equal to the corresponding dimension of the TDoA attack space. **Figure 12** shows the antenna installation of TX and RX. The red and green marks represent the directivity of a half-wave dipole antenna shown in Fig. 3 (b) on a plane. We assume TXs, which are packaged with the pressure sensor, are attached to the edge of the wheel and rotate with the rotation of the tires. All RX anten-



(a) Top view.

(b) Rear view.

Fig. 11 Vehicle configuration and simulation space.

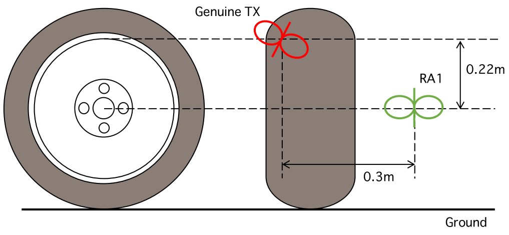


Fig. 12 Antenna installation of TX and RX.

nas are installed in the vertical direction while the TX antennas are installed so that its directivity is always maximized in the direction to RA1, i.e., the nearest RX antenna to each. This aims to keep the genuine RSSR as large as possible. In general, as the transmission point becomes farther, the ratio of the distances and the difference of the directions to the two receiving antennas become smaller, and the RSSR also becomes smaller. Therefore, the greater the genuine RSSR, the harder it is to attack from a distant location.

In this paper, we evaluate the two attack-success rates, q_{ave} and q_{max}, at each point through the following equations.

$$q_{ave}(x,y,z)|_{C_1,C_2} = \frac{1}{|\alpha||\beta|}\sum_{\alpha,\beta} q_{attack}(x,y,z,\alpha,\beta)|_{C_1,C_2} \quad (18)$$

$$q_{max}(x,y,z)|_{C_1,C_2} = \max_{\alpha,\beta}\, q_{attack}(x,y,z,\alpha,\beta)|_{C_1,C_2} \quad (19)$$

Where α and β are respectively the installation angles in the θ direction and the ϕ direction, which take a value from 0 to π. $|a|$ is not the absolute value of a but the total number of values that a will take. $q_{attack}(x,y,z,\alpha,\beta)|_{C_1,C_2}$ is the probability the attacking signal takes a value in the authentication window from a point (x,y,z) with an installation angle (α,β) under an environment where the coefficients of Eq. (16) are (C_1,C_2). Equation (18) derives the average rate, q_{ave}, when all installation angles are tried at each point, which assumes the situation that the attacker does not know which (α,β) combination leads to the higher attack-success rate. On the other hand, Eq. (19) derives the maximum rate at each point, q_{max}, which assumes the situation that the attacker knows which (α,β) combination leads to the higher attack-success rate. Because it is hard to analytically obtain q_{attack} using a probability distribution, we implemented the computer simulation tool based on the radio wave-propagation model to numerically calculate it.

The assumed conditions for the simulations are as follows.

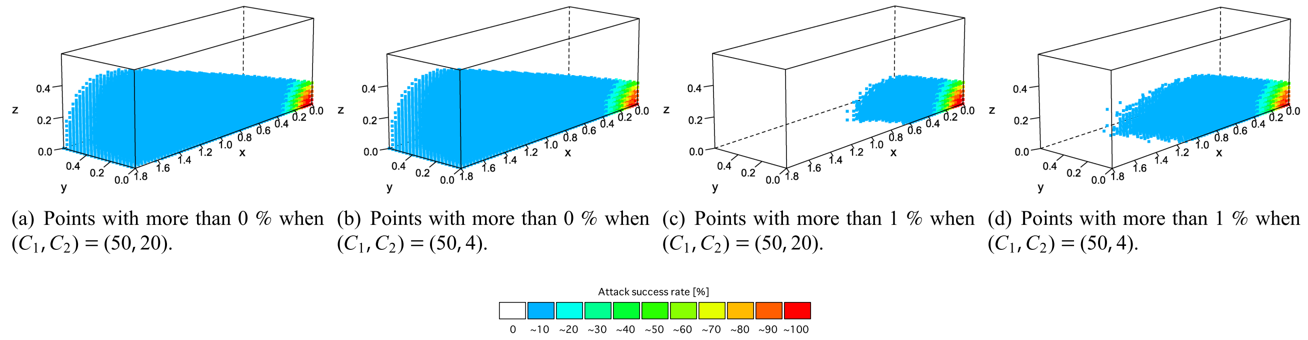
- The authentication window is set from 12.0 to 37.0 so that the authentication will succeed no matter where on the circumference the genuine TX is.
- Transmission points are set in the whole of the simulation space at 3 [cm] intervals on each axis.
- Both θ and ϕ directions are divided in steps of $\frac{\pi}{18}$, in other words α and β respectively have 19 options, totaling $|\alpha||\beta| = 361$.
- (C_1, C_2) is set to $(50, 20)$ and $(50, 4)$. Note that these noise parameters, introduced in Section 4, are not determined considering the shape and material etc. of the vehicle system of Fig. 11.

5.2 Simulation Results

Figure 13 shows q_{ave} at each point. In all figures, these rates are rounded to integer and indicated with color-coding. That is, the area with the rates of 0.5 [%] or less is regarded as without the attack possibility and is not drawn. Each of Figs. 13 (a) and (b) draws all the points with q_{ave} greater than 0 [%] when $(C_1, C_2) = (50, 20)$ and $(50, 4)$ respectively. These indicate that the attack possibility from a distant location cannot be excluded completely. However, Figs. 13 (c) and (d) simultaneously show that q_{ave} is smaller as going away from the genuine TX. These draw only the points with q_{ave} greater than 1 [%]. Besides, these figures revealed that the convergence of the attack space is gradual as the noise is larger when we change the threshold of q_{ave} to be drawn. This means that the situation with a greater noise is more advantageous to attackers who do not know the effective installation angle (α,β).

Figure 14 shows q_{max} at each point using the same color-coding in Fig. 13. Each of Figs. 14 (a) and (b) draws all the points with q_{max} greater than 0 [%] when $(C_1, C_2) = (50, 20)$ and $(50, 4)$ respectively. These indicate the attack possibility from a distant location same as q_{ave}, but the success rate is higher than q_{ave}. Figures 14 (c) and (d) show that q_{max} decreases as going far away, and this property is also common with q_{ave}. The different property of q_{max} from q_{ave} is that the convergence of the attack space is gradual as the noise is smaller. This means that the situation with less noise is more advantageous to attackers who know the effective installation angle (α,β), contrary to the unknown situation.

Anyway, no matter whether attackers know an effective installation angle or not, it is not desirable for the method that the secu-



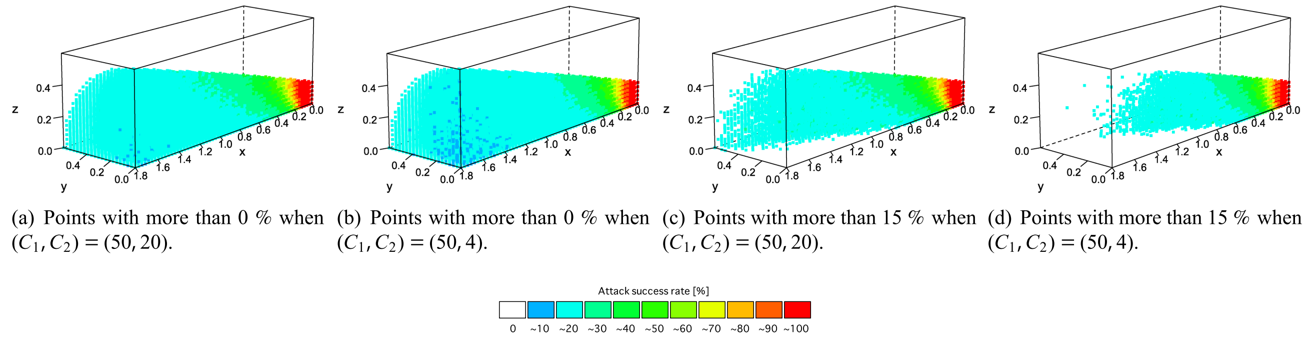
(a) Points with more than 0 % when $(C_1, C_2) = (50, 20)$.

(b) Points with more than 0 % when $(C_1, C_2) = (50, 4)$.

(c) Points with more than 1 % when $(C_1, C_2) = (50, 20)$.

(d) Points with more than 1 % when $(C_1, C_2) = (50, 4)$.

Fig. 13 q_{ave} at each point.



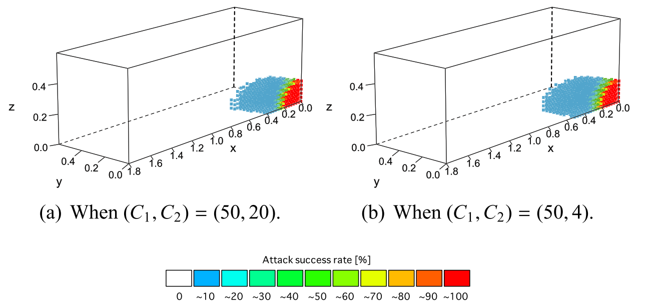
(a) Points with more than 0 % when $(C_1, C_2) = (50, 20)$.

(b) Points with more than 0 % when $(C_1, C_2) = (50, 4)$.

(c) Points with more than 15 % when $(C_1, C_2) = (50, 20)$.

(d) Points with more than 15 % when $(C_1, C_2) = (50, 4)$.

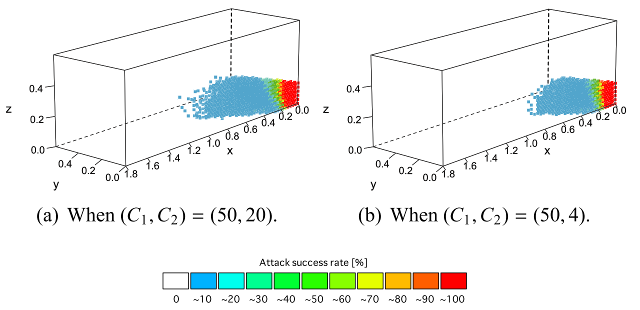
Fig. 14 q_{max} at each point.



(a) When $(C_1, C_2) = (50, 20)$.

(b) When $(C_1, C_2) = (50, 4)$.

Fig. 15 Points in which attack succeeds more than 3 out of 9 times in case of assuming q_{ave}.



(a) When $(C_1, C_2) = (50, 20)$.

(b) When $(C_1, C_2) = (50, 4)$.

Fig. 16 Points in which attack succeeds more than 7 out of 9 times in case of assuming q_{max}.

rity level probabilistically fluctuates due to the noise. However, even in the situation shown in Figs. 13 and 14, as we mentioned in Section 4.2, we can avoid the attacks from a distant location by devising the authentication procedures and increasing the q_{ave} and q_{max} tolerance. In other words, it makes sure that the system does not fall into a critical state by a single spoofing signal. Actually, according to the article [11], a legitimate TX needs to transmit eight packets following the first packet reporting the low tire pressure. Since the TPMS investigated in Ref. [11] does not have the authentication function, it seems to be an implementation to prevent erroneous reports of measured values. Using these nine signals, we examine an authentication procedure to eliminate the attack-success rate from a distant location.

Figure 15 shows the probability that the signal spoofing will succeed more than 3 out of 9 trials at each point assuming q_{ave}, in other words the attackers who do not know the effective installation angle. Comparing with Fig. 13, the attack space is reduced to $x = 0.45$ [m] in Fig. 15 (a) and $x = 0.51$ [m] in Fig. 15 (b). That is, regardless of the noise parameters, it is possible to limit the attack space to about 0.5 [m] proximity. **Figure 16** shows the probability that the signal spoofing will succeed more than 7 out of 9 trials at each point assuming q_{max}, in other words the attackers who know the effective installation angle. Comparing with Fig. 14, the attack space is reduced to $x = 0.90$ [m] in Fig. 16 (a) and $x = 0.60$ [m] in Fig. 16 (b). That is, regardless of the noise parameters, it is possible to limit the attack space to a proximity within 1.0 [m]. **Figure 17** shows changes in the spread of the attack space on the x-axis when changing the number of success required by the authentication procedure. The red circles are the results when $(C_1, C_2) = (50, 20)$ and the blue crosses are the re-

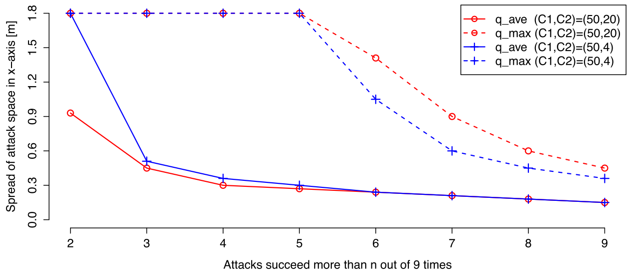


Fig. 17 Changes of spread of attack space on x-axis.

sults when $(C_1, C_2) = (50, 4)$. The solid lines correspond to q_{ave} and the dashed lines correspond to q_{max}. When we have some estimation of the noise level of the environment in which the system will be used, we can draw the graph as in Fig. 17. Then, finding a point below the size of the desired attack space, the authentication procedure will be determined.

Since TPMS is enabled only when the vehicle is driven, to achieve spoofing undergoing the above procedure, the attacker has to keep staying the close range of the genuine TX as drawn in Figs. 15 and 16. Especially for Fig. 16, in addition, attackers have to keep the relative installation angle of the TX. We conclude that it is impossible and the proposed method realistically guarantees the security in the TPMS case study.

5.3 Cost Evaluation

In the end, we investigate the validity of our proposed method from the viewpoint of cost in TX. Xu at el. implemented a MAC-based authentication on a TPMS and evaluated the overheads of energy consumption and transmission delay [12]. We refer the article and compare the assuming implementation of our method. Since the TX in our proposed method does not perform any information processing for the authentication, the costs before the implementation of the MAC-based authentication in Ref. [12] can be regarded as the costs in our method. They adopt `Katan32`, a lightweight hardware block cipher, for the way of encryption and MAC generation. However, the data cited in this paper is only the part related to MAC generation, not including the cost required for encryption and key generation.

Energy Consumption

According to Ref. [12], the transmission of a sensing packet without MAC consumes the energy of 9.826 [mJ], and the transmission of one with MAC consumes 15.231 [mJ]. This means approximately a 1.5 times increase in energy consumption, in other words, our method can extend the lifetime of TPMS sensors by 1.5 times while keeping its spoofing attack resistance. We should note that about two-thirds of 15.231 [mJ] is dependant on the signal transmission, not the MAC generation. Therefore, increasing the number of signal transmissions from sensors for the authentication procedure may lead to a more energy-exhausted scheme than the MAC-based method. That is, when we use n signal transmissions for one authentication ($n > 2$), the lifetime of sensors will be $\frac{1.5}{n}$ times of the MAC-based method.

Transmission Delay

According to Ref. [12], the transmission of a sensing packet without MAC takes 23.5 [ms], and the transmission of one with MAC takes 36.6 [ms]. That is, the difference of 13.1 [ms] is consumed for the MAC generation and the transmission of the increased part in the packet. While, according to another paper [11], which explores TPMS security in detail using an off-the-shelf, the system works well if the TX sends a packet once during the detection window of 240 [ms]. These make us aware that the time required for MAC adaptation is sufficiently smaller than the time constraint of TPMS. Therefore, in this case study, both our method and the one for comparison satisfy the real-time requirements and there is no superiority or inferiority from this point of view.

6. Conclusions

For improving the security of wireless communication of sensing devices, we proposed a device-authentication method based on RPCs to prevent spoofing attacks and modeled the attack space. The analysis of the RSSR- and TDoA-based attack space led to a consideration of the following possible attack scenarios: 1) the possibility of an attack from an infinite distance in both RSSR- and TDoA-based models, and 2) the possibility of an attack caused by the adjustment of the attacking TX in the RSSR-based model. We also proposed the combination model that complementarily ensures security in the aforementioned scenarios and carried out detailed simulations assuming the effect of noise on the RSSR of attacking signals. The results indicate that the increase in noise leads to the ease of attack success from a distance. However, we confirmed that the system designers can avoid this problem by devising on the aspect of the authentication procedure and the proposed method can become an effective countermeasure against spoofing attacks.

Our future work is to show an applying manner to the real system, such as estimating method of the noise parameter of attackers in the real environment and how to design the authentication procedure suitable for the proposed method. In addition, we have to investigate the manufacturing cost for the additional RX antenna installation. If it is cheaper or easier compared to the addition of hardware required for MAC generation, we can further enhance the validity of our proposal.

Acknowledgments This research was supported by Strategic International Research Cooperative Program, Japan Science and Technology Agency (JST) and JSPS KAKENHI Grant Number JP17K19984.

References

[1] Yick, J., Mukherjee, B. and Ghosal, D.: Wireless Sensor Network Survey, *Comput. Netw.*, Vol.52, No.12, pp.2292–2330 (2008).

[2] Tsai, H.-M., Tonguz, O.K., Saraydar, C., Talty, T., Ames, M. and Macdonald, A.: Zigbee-based intra-car wireless sensor networks: A case study, *IEEE Wireless Communications*, Vol.14, No.6, pp.67–77 (2007).

[3] Perrig, A., Stankovic, J. and Wagner, D.: Security in Wireless Sensor Networks, *Comm. ACM*, Vol.47, No.6, pp.53–57 (2004).

[4] Cheng, H.C., Ho, S.Y. and Yeh, P.C.: Collaborative non-cryptographic physical-layer authentication schemes in wireless networks, *URSI Radio Science Bulletin*, Vol.2014, No.349, pp.18–31 (2014).

[5] Azarmehr, M., Ahmadi, A. and Rashidzadeh, R.: Secure authentication and access mechanism for IoT wireless sensors, *Proc. IEEE International Symposium on Circuits and Systems* (*ISCAS*), pp.1–4 (2017).

[6] Bellare, M., Canetti, R. and Krawczyk, H.: Keying hash functions for message authentication, *Proc. 16th Annual International Cryptology Conference on Advances in Cryptology*, pp.1–15 (1996).

[7] Rivest, R.L., Shamir, A. and Adleman, L.: A Method for Obtaining Digital Signatures and Public-key Cryptosystems, *Comm. ACM*, Vol.26, No.1, pp.96–99 (1983).

[8] Gujrathi, S.: Heartbleed Bug: An OpenSSL Heartbeat Vulnerability, *International Journal of Computer Science and Engineering*, Vol.2, No.5, pp.61–64 (2014).

[9] Demirbas, M. and Song, Y.: An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks, *Proc. 2006 International Symposium on World of Wireless, Mobile and Multimedia Networks*, pp.564–570 (2006).

[10] Sonoyama, M., Ono, T., Kanaya, H., Muta, O. and Inoue, K.: Wireless Spoofing-Attack Prevention Using Radio-Propagation Characteristics, *Proc. IEEE 15th Int'l Conf. on Dependable, Autonomic and Secure*

Computing, pp.502–510 (2017).

[11] Rouf, I., Miller, R., Mustafa, H., Taylor, T., Oh, S., Xu, W., Gruteser, M., Trappe, W. and Seskar, I.: Security and Privacy Vulnerabilities of In-car Wireless Networks: A Tire Pressure Monitoring System Case Study, *Proc. 19th USENIX Conference on Security*, p.21 (2010).

[12] Xu, M., Xu, W., Walker, J. and Moore, B.: Lightweight Secure Communication Protocols for In-vehicle Sensor Networks, *Proc. 2013 ACM Workshop on Security, Privacy & Dependability for Cyber Vehicles*, *CyCAR '13*, pp.19–30 (2013).

[13] Ling, Z., Luo, J., Xu, Y., Gao, C., Wu, K. and Fu, X.: Security Vulnerabilities of Internet of Things: A Case Study of the Smart Plug System, *IEEE Internet of Things Journal*, Vol.4, No.6, pp.1899–1909 (2017).

[14] Li, C., Ji, X., Zhou, X. and Zheng, J.: HlcAuth: Key-free and Secure Communications via Home-Limited Channel, *Proc. 2018 on Asia Conference on Computer and Communications Security*, pp.29–35 (2018).

[15] Burleson, W., Clark, S.S., Ransford, B. and Fu, K.: Design challenges for secure implantable medical devices, *Proc. DAC Design Automation Conference 2012*, pp.12–17 (2012).

[16] Rasmussen, K.B., Castelluccia, C., Heydt-Benjamin, T.S. and Capkun, S.: Proximity-based Access Control for Implantable Medical Devices, *Proc. 16th ACM Conference on Computer and Communications Security*, *CCS '09*, pp.410–419 (2009).

[17] Porambage, P., Braeken, A., Schmitt, C., Gurtov, A., Ylianttila, M. and Stiller, B.: Group Key Establishment for Enabling Secure Multicast Communication in Wireless Sensor Networks Deployed for IoT Applications, *IEEE Access*, Vol.3, pp.1503–1511 (2015).

[18] Aono, T., Higuchi, K., Ohira, T., Komiyama, B. and Sasaoka, H.: Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels, *IEEE Trans. Antennas and Propagation*, Vol.53, No.11, pp.3776–3784 (2005).

[19] Ren, K., Su, H. and Wang, Q.: Secret key generation exploiting channel characteristics in wireless communications, *IEEE Wireless Communications*, Vol.18, No.4, pp.6–12 (2011).

[20] Wang, G., Qian, C., Cai, H., Han, J., Ding, H. and Zhao, J.: Replay-resilient Physical-layer Authentication for Battery-free IoT Devices, *Proc. 4th ACM Workshop on Hot Topics in Wireless*, *HotWireless '17*, pp.7–11 (2017).

[21] Danev, B., Luecken, H., Capkun, S. and El Defrawy, K.: Attacks on Physical-layer Identification, *Proc. 3rd ACM Conference on Wireless Network Security*, *WiSec '10*, pp.89–98 (2010).

[22] Cai, L., Zeng, K., Chen, H. and Mohapatra, P.: Good Neighbor: Secure Pairing of Nearby Wireless Devices by Multiple Antennas, *Proc. Network and Distributed System Security Symposium* (*NDSS*) (2011).

[23] Xiao, L., Greenstein, L., Mandayam, N. and Trappe, W.: Fingerprints in the Ether: Using the Physical Layer for Wireless Authentication, *Proc. IEEE International Conference on Communications 2007*, pp.4646–4651 (2007).

[24] Li, Z., Xu, W., Miller, R. and Trappe, W.: Securing Wireless Systems via Lower Layer Enforcements, *Proc. 5th ACM Workshop on Wireless Security*, *WiSe '06*, pp.33–42, ACM (2006).

[25] Bhargava, V. and Sichitiu, M.L.: Physical authentication through localization in wireless local area networks, *Proc. IEEE Global Telecommunications Conference*, Vol.5, pp.2658–2662 (2005).

[26] Marxen, J. and Orailoglu, A.: Ensuring System Security through Proximity Based Authentication, *Proc. 2017 Asia and South Pacific Design Automation Conference*, pp.330–335 (2017).

[27] Musicki, D., Kaune, R. and Koch, W.: Mobile Emitter Geolocation and Tracking Using TDOA and FDOA Measurements, *IEEE Trans. Signal Processing*, Vol.58, No.3, pp.1863–1874 (2010).

[28] Hara, S. and Anzai, D.: Experimental Performance Comparison of RSSI- and TDOA-Based Location Estimation Methods, *Proc. IEEE Vehicular Technology Conference*, pp.2651–2655 (2008).

[29] Niculescu, D. and Nath, B.: Ad hoc positioning system (APS) using AOA, *Proc. IEEE INFOCOM 2003, 22nd Annual Joint Conference of the IEEE Computer and Communications Societies* (*IEEE Cat. No.03CH37428*), Vol.3, pp.1734–1743 (2003).

[30] Gemayel, N.E., Koslowski, S., Jondral, F.K. and Tschan, J.: A low cost TDOA localization system: Setup, challenges and results, *Proc. 10th Workshop on Positioning, Navigation and Communication* (*WPNC*), pp.1–4 (2013).

[31] Prashar, D., Kumar, D. and Jyoti, K.: Performance Analysis of Secure Localization Techniques in Wireless Sensor Network, *Proc. 2nd International Conference on Information and Communication Technology for Competitive Strategies*, *ICTCS '16*, pp.48:1–48:7 (2016).

[32] Lin, Z., Han, T., Zheng, R. and Fu, M.: Distributed Localization for 2-D Sensor Networks With Bearing-Only Measurements Under Switching Topologies, *IEEE Trans. Signal Processing*, Vol.64, No.23, pp.6345–6359 (2016).

[33] Abouzar, P., Michelson, D.G. and Hamdi, M.: RSSI-Based Distributed Self-Localization for Wireless Sensor Networks Used in Precision Agriculture, *IEEE Trans. Wireless Communications*, Vol.15, No.10, pp.6638–6650 (2016).

[34] Schloemann, J. and Buehrer, R.M.: On the value of collaboration in anchorless robot self-localization, *MILCOM 2012–2012 IEEE Military Communications Conference*, pp.1–6 (2012).

[35] Zeng, H. and Hubing, T.H.: The Effect of the Vehicle Body on EM Propagation in Tire Pressure Monitoring Systems, *IEEE Trans. Antennas and Propagation*, Vol.60, No.8, pp.3941–3949 (2012).

[36] Leng, Y., Wenfeng, D., Peng, S., Ge, X., Nga, G.J. and Liu, S.: Study on Electromagnetic Wave Propagation Characteristics in Rotating Environments and Its Application in Tire Pressure Monitoring, *IEEE Trans. Instrumentation and Measurement*, Vol.61, No.6, pp.1765–1777 (2012).

[37] Yao, Y., Xiao, B., Wu, G., Liu, X., Yu, Z., Zhang, K. and Zhou, X.: Voiceprint: A Novel Sybil Attack Detection Method Based on RSSI for VANETs, *2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks* (*DSN*), pp.591–602 (2017).

[38] Abdi, A., Tepedelenlioglu, C., Kaveh, M. and Giannakis, G.: On the estimation of the K parameter for the Rice fading distribution, *IEEE Communications Letters*, Vol.5, No.3, pp.92–94 (2001).

Mihiro Sonoyama received his B.E. degree in School of Engineering from Kyushu University, Japan, in 2017. He is currently a master student in the Graduate School of Information Science and Electrical Engineering, Kyushu University. His research interests include the cyber physical secure computing. He is a member of the IEEE.

Takatsugu Ono received his Ph.D. degree from Kyushu University, Japan, in 2009. He was a researcher for Fujitsu Laboratories Ltd., Kawasaki, Japan, and engaged in developing a server for a data center. He is currently an associate professor in the Faculty of Information Science and Electrical Engineering at Kyushu University. His research interests include the area of memory architecture, secure architecture, and supercomputing. He is a member of the IEEE, IPSJ, and IEICE.

Haruichi Kanaya was born in Yamaguchi, Japan, in 1967. He received his B.S. (Physics) degree from Yamaguchi University in 1990, and his M.E. (Applied Physics) and D.E. degrees from Kyushu University in 1992 and 1994, respectively. In 1994, he became a Research Fellow (PD) of the Japan Society for the Promotion of Science. In 1998, he was a visiting scholar at the Massachusetts Institute of Technology (MIT), USA. He is currently engaged in the study and design of RF CMOS LSI System, energy harvesting device, and miniature, planar, flexible and array antenna. He is an Associate Professor in the Department of Electronics, Graduate School of Information Science and Electrical Engineering, and also System LSI Research center, Kyushu University. He is a senior member of the Institute of Electrical and Electronics Engineers (IEEE).

Osamu Muta graduated from Sasebo Institute of Technology, in 1994, and then received B.E. degree from Ehime University, in 1996, M.E. degree from Kyushu Institute of Technology, Japan, in 1998, and Ph.D. degree from Kyushu University in 2001. In 2001, he joined the Graduate School of Information Science and Electrical Engineering, Kyushu University as an assistant professor. Since 2010, he has been an associate professor in Center for Japan-Egypt Cooperation in Science and Technology, Kyushu University. His current research interests include signal processing techniques for wireless communications and powerline communications, MIMO, and nonlinear distortion compensation techniques for high-power amplifiers. He received the 2005 Active Research Award from IEICE technical committee of radio communication systems, the 2014 and the 2015 Chairman's Awards for excellent research from IEICE technical committee of communication systems, respectively. He is a member of IEEE and a senior member of IEICE.

Smruti R. Sarangi received his B.Tech. degree in Computer Science from IIT Kharagpur, India, in 2002, and his M.S. and Ph.D. degrees in Computer Science from the University of Illinois at Urbana-Champaign, Champaign, IL, USA, in 2007. He is currently an Associate Professor in the department of Computer Science and Engineering, IIT Delhi, and additionally holds a joint appointment in the department of Electrical Engineering. His research interests include computer architecture, parallel systems, and the internet of things. He is a member of IEEE and ACM.

Koji Inoue received his B.E. and M.E. degrees in computer science from Kyushu Institute of Technology, Japan in 1994 and 1996, respectively. He received the Ph.D. degree in Department of Computer Science and Communication Engineering, Graduate School of Information Science and Electrical Engineering, Kyushu University, Japan in 2001. In 1999, he joined Halo LSI Design & Technology, Inc., NY, as a circuit designer. He is currently a professor of the Department of I&E Visionaries, Kyushu University. His research interests include power-aware computing, high-performance computing, secure computer systems, 3D microprocessor architectures, multi/many-core architectures, nanophotonic computing and quantum computing.