Nowadays wireless communication has become a widely used technology with the endless of applications. The security concerns of wireless communication are rapidly increasing together with the growth of wireless applications in order to provide a large number of secure services to wireless users. Especially, some information is so valuable and private that needs to be transmitted securely to its intended recipient without interception. Security protocols and encryption methods are commonly proposed to protect sensitive data in wireless communication. However, there are some probabilities that attackers can decrypt the signal and obtain the confidential information. To improve security for wireless communication, optical wireless communication (OWC) can be applied as an alternative communication system. Since optical signal cannot penetrate through walls or other opaque barriers, the coverage of OWC systems is limited to the boundaries of the room in which the system is installed. Furthermore, optical wireless transmission offers several potential advantages over radio frequency (RF), including large unregulated bandwidth, immunity to interference caused by other RF wireless devices, possibility of frequency reuse, and the use of inexpensive optoelectronic devices which are small and consume little power.

The goal of this research is to propose the schemes to attain secure data transmission in physical layer of indoor OWC. This dissertation proposes two schemes which are a position-based diversity transmission scheme and a hybrid RFID - OWC with an adaptive priority transmission scheme. The system models, implementations, and analytical results of both schemes are addressed.

In chapter 1, the background of OWC is briefly introduced. The OWC technologies can be classified in terms of whether they are used for indoor or outdoor environment. The characteristics and challenges of both indoor and outdoor OWC are described. Since there has been increased interest in the use of OWC systems, recent developments and applications of OWC systems are provided. This chapter also presents the contributions and organization of the dissertation.

In chapter 2, the overview of indoor optical wireless communication is provided. This chapter focuses on indoor OWC since this dissertation aims at proposing the schemes to achieve secure data transmission in physical layer of indoor OWC. At first, the comparison between optical wireless communication and radio media is illustrated. The characteristics of radio and indoor OWC links are discussed. Subsequently, optoelectronic components for optical wireless transmission, transmitter and receiver, are presented. Regarding the channel model, for OWC links, the most practical modulation is intensity modulation with direct detection (IM/DD). The modeling of OWC channels with IM/DD is illustrated, and the baseband channel model for indoor optical wireless communication is provided. The noise in OWC is also discussed in this chapter. Then, eye and skin safety for OWC, including the safety standard and interpretation of safety classification for optical sources are listed. Finally, modulation of OWC, both binary modulation and multi level modulation, is presented.

In chapter 3, a position-based diversity transmission scheme employing OWC is proposed to improve the security at the physical layer of optical wireless transmission. Although the interception of optical wireless systems is far more difficult than RF communication systems, data interception is possible. For example, if the intruders stay in the room where optical transmitters are placed, they can still intercept the signal, leaving the system vulnerable.

In this scheme, the I (in-phase) and Q (quadrature) signal of QPSK (quaternary phase-shift keying) modulation are transmitted separately to obtain a secure position-based transmission. Consequently, the information cannot be demodulated by intercepting only the I or the Q signal. Secure data transmission is achieved by establishing a demodulation area in which signal can be demodulated accurately, so intruders outside this area cannot get a correct signal. The transmitted time of the I and Q transmitter is adjusted by applying delay to handle synchronization problems. In the proposed model, single or multiple demodulation area (s) can be attained. To obtain different multiple demodulation area (s), TDMA (time-division multiple access) with adaptive transmitted power for each time slot is applied. The power in each time slot is changed according to the position of demodulation area. Users can move inside the area where they stay or move to other areas if mentioned areas are not occupied by users of other groups.

This scheme is not complex and easy to implement. Moreover, it can be applied together with the main security methods such as data encryption, strengthening the
security of the systems. For example, when applying this scheme with the encryption method, intruders not only have to decrypt the signal, but also have to stay in a specific position to demodulate the signal accurately. Although intruders who stay outside the area where information can be demodulated correctly have ability to decrypt the signal, they could not get the accurate information. From the analytical results, the probability that the intruders can get the correct signal in the proposed scheme is decreased, compared to conventional QPSK. Therefore, the secure data transmission in position-based diversity transmission scheme is achieved.

In Chapter 4, a hybrid RFID - OWC with an adaptive priority transmission scheme is presented. Recently, radio frequency identification (RFID) has attracted extensive interest because RFID technology has many benefits including, non line of sight, contactless, simultaneous collection of data, and high accuracy. However, RFID have some implications for security and privacy concerns. RFID tags are subject to clandestine interception, allowing leakage of sensitive personal information. Since OWC provides high security, secure data transmission of the proposed system is achieved by applying OWC to transmit confidential information in RFID system. The energy harvesting of RFID is employed for CCR (corner cube retroreflector) to modulate optical signal which propagates back to the reader. By applying energy harvesting and CCR, the RFID tag consumes low energy and can then be a passive tag that does not need any other power sources.

The adaptive priority transmission (APT) method is proposed to transmit information depending on the level of confidentiality and significance of that information, and also to ensure that the BER is lower than the specific value. The more confidential information is transmitted by OWC with adaptive data rate, and the rest of the information (if there is any) is transmitted by RFID. BER is analyzed regarding the half-power angle of the transmitter, the optical transmitted power, the data rate, and the angle between tag and reader. The proposed system can be implemented together with other security methods, such as data encryption in the higher layer, to improve security particularly in applications that require tag to transmit sensitive or significant personal information. The analytical results verify the feasibility of OWC transmission in the proposed scheme.

In Chapter 5, conclusions of the dissertation are presented. The possible future research works are discussed to further improve the security in indoor OWC and RFID applications.