Foreword and Editorial

International Journal of Security Technology for Smart Device

We are very happy to publish this issue of an International Journal of Security Technology for Smart Device by Global Vision School Publication.

This issue contains 4 articles. Achieving such a high quality of papers would have been impossible without the huge work that was undertaken by the Editorial Board members and External Reviewers. We take this opportunity to thank them for their great support and cooperation.

In the paper “Technical Study of Remote Backup Center using Public Virtual Private Network”, due to the rapid development of information technology worldwide, the spread of information technology has made the use of information systems prominent throughout the industry. In particular, the citizens are using various public services provided by the Electronic Government all the time, as a result, the amount of information data has increased sharply. As the reliance on such information systems continues to increase, the demand for ensuring service continuity against various kinds of disasters that can affect the services is also increasing. Therefore, a safety management system that prevents the loss of credibility and financial loss caused by system damage is becoming a necessity, not an option. The safest and most reliable method to ensure continuity of information systems against disasters is to backup the data to remote locations. However, backing up data to a remote location requires large budget such as technical and administrative considerations, network dedicated lines, and construction of a physical remote center. Therefore, for small and medium enterprises, it is a burdensome reality to build as such, but looking at the existing research related, empirical researches that can suggest a remote backup center model for small and medium agencies and companies are very insufficient. Thus, this study is going to propose the composition of remote backup center model using public virtual private network and de-duplication backup technology for low-cost and high efficiency remote backup center model that can utilize small and medium sized agencies.

In the paper “Priority and Delay Aware packet transmission MAC Protocol for Wireless Sensor Networks”, researcher present a priority and delay aware packet transmission MAC Protocol which we call PDAP-MAC for some applications such as field monitoring in which an abnormal data and normal data may be generated. In this kind of WSNs applications, sensor nodes may send an abnormal data and normal data. Abnormal data packet may be generated when there is an event such as exceeding threshold value. These events are generally critical, so the abnormal data should be transmitted in limited time faster than the normal data to their final destination node, sink node. Therefore, the priority packet transmission mechanism is necessary in this application. The PDAP-MAC protocol reduces the abnormal packet transmission delay and average node energy consumption in comparison to existing related MAC protocols.

The paper entitled “Delay Aware Data Gathering Mechanism in Wireless Sensor Networks”, data packets from sensor nodes are generally transferred to the sink node in a wireless sensor networks. So many data packets are gathered around the sink node, resulting in significant packet collision and delay. In this paper we proposed an energy efficient data transmission

mechanism. The basic idea of this mechanism is to reduce duplicated data packets prior to be transmitted. Proposed mechanism consists of two parts. One works between sink node and 1-hop nodes from sink. In this area, data packets are transmitted in predefined time slots to reduce collisions. The other part works between other nodes except sink node. In this area, duplicated packets from neighbor nodes can be detected and dropped. Data packet signal length and data packet direction will be used to separate duplicated data packets. Our numerical analysis and simulation results show that our mechanism outperforms other related protocols in terms of energy consumption and transmission delay.

In the paper “Intruder Detection System Using Face Recognition for Home Security IoT Applications: A Python Raspberry Pi 3 Case Study”, in the present era, security is a primary concern in all facets of life; therefore, there is a strong need of an efficient security system. There are many existing systems, which perform surveillance by way of motion detection only. The proposed intruder detection system is a security system that performs detection through motion as well as integrates a biometric identification technique (i.e. front face recognition for increased accuracy). The use of facial recognition when compared to motion detection is a more efficient method as it can be implemented for larger distances and there is no need for equipment to record or compare the results. In this system, a passive infrared (PIR) sensor is used to detect motion. Once detected, the sensor will send a signal to raspberry pi to activate the web camera, which will capture an image of the activity. The captured image will then be processed and if any facial feature is detected, then facial recognition and detection algorithms will be run in order to identify the face. If no message will be given indicating that activity was detected but no facial features were found and an email notification is also sent to the owner. Regardless of content, all images captured by the camera are stored on a local disk (i.e. raspberry pi) as well as on the cloud (i.e. Google drive).

October 2018

Editors of the October Issue on
International Journal of Security Technology for Smart Device