On Mobile Internet Architecture of Smart Campus and Its Security Precautions

Guoqiang Hu[a], Xiaoling Li[b]

Network &Education Technology center, Northwest A&F University, Yangling, Shaanxi 712100, China

[a]hgq@nwsuaf.edu.cn, [b]lxl@nwsuaf.edu.cn

Abstract

With the rapid development of mobile Internet and campus wireless networks, future educational informatization is more concerned about innovation and intelligence. Under the background of the national strategy of Internet Plus, the question of how Smart Campus can provide more innovative services for teaching and management has become a focus for the information construction of many universities in the next period. Under such a context, this paper proposes and designs a mobile Internet architecture for campuses by combining specific campus applications, and raises several precautions against the security problems brought by this new architecture.

Keywords

mobile Internet architecture，security precautions，campus wireless networks.

1. Introduction

In order to earnestly implement the tenets of the National People's Congress and the Chinese People's Political Consultative Conference in 2015, National Development and Reform Commission is taking the lead in organizing and drawing up an action plan for Internet Plus. Interment Plus has showed its powerful influence on traditional industries, constantly promoting the upgrading of the latter. The role that the Internet plays in the educational revolution is also very obvious when Internet Plus encounters education. Precisely, Smart Campus is the most typical application of Internet Plus in the area of education, which refers to an "open education environment and convenient and comfortable surroundings, with the idea of providing personalized services for teachers and students, to comprehensively perceive the physical environment, identify learners' individual characteristics and learning contexts, provide seamless and interconnected network communication and effectively support the analyses, evaluations and smart decision-making during the course of education." [2]. Smart Campus is not only an "advanced form" into which the Internet develops in the area of education, but the perfect goal of the information construction of school education. In recent years, Chinese universities have made great achievements in information construction, yet fallen flat in realizing the goal of Smart Campus in terms of support for educational innovation and smart education. This paper designs a campus mobile interment architecture based on application scenarios and elaborates the security problems of Smart Campus and the precautions against them.

2. Campus mobile Internet architecture

2.1 General design of the campus mobile Internet architecture

With the expansion of the coverage of campus wireless networks and the increasing number of teachers and students using campus wireless networks, universities pay more attention to the quality of wireless networks, shifting from solving the matter of communication by simply building networks to focusing on upper applications, from traditional campus portals to mobile ones, providing convenience for teachers and students' study and life. In the meantime, it has become a direction for all the universities to concentrate on and discuss about how to bring greater convenience to teachers and students by making use of the characteristics of "mobility and interconnection" of campus

wireless networks. Scenario-based wireless coverage has become a focus in the construction of mobile campus portals, especially in auditoriums, dining halls and outdoor areas.

The campus mobile Internet architecture based on scenarios can be divided into four layers from bottom to up: Client, Scenario, Administration and Application, as are shown in Figure 1.

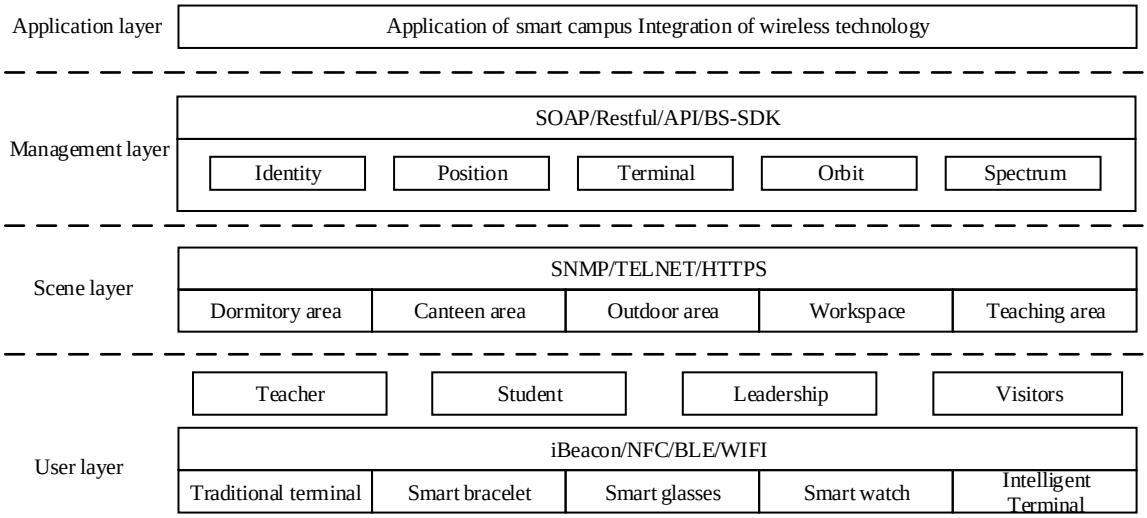

Fig. 1 On Mobile Internet Architecture of Smart Campus

2.2 Functions realized in each layer

(1) Client: it is categorized into Teacher, Student, School leader, and Visitor. The terminals that Client uses are both smart and traditional ones based on iBeacon [3], NFC (Near Field Communication) [4], Bluetooth Low Energy (BLE) [5] and WIFI [6].

(2) Scenario: as data are forwarded centrally from ACs (Analogue Controller) to APs (Access point), the layer Scenario is the ones in which wireless APs are deployed, such as dormitories, dining halls, outdoor areas, office areas, teaching areas and school buses and so on. ForCES (Forwarding and Control Element Separation) should be adopted in dormitories, with the APs installed in the equipment room while mini APs in the dormitories. With such design the construction will be easier, maintenance simpler and management finer. Wireless APs of high density should be adopted in the teaching areas and lecture halls because the characteristic of high concurrency of such APs can solve the problems of wireless coverage in a scenario that is of high density. APs of Internet of Things that support ZigBee, Bluetooth and RFID can be choices of the scenarios of dining halls and school buses to realize the combination of wired networks, wireless networks and Internet of Things.

(3)Administration: all management systems in universities, such as campus-card systems, uniform identity authentication platforms and positioning systems and so on.

(4)Application: all Smart Campus applications that adopt wireless technology.

3. Security problems brought by mobile Internet architecture

There are potential security problems in every technical network architecture. Mobile Internet architectures are based on wireless APs that are applied in different scenarios and these wireless APs are under the centralized control of ACs, as is show in Figure 2. As all kinds of businesses of smart applications are placed on wireless Aps, security problems become highly frequent due to the openness and uncontrollable wireless networks constructed by APs.

3.1 Security problems brought by the mobility of smart terminals

That smart terminals of wireless networks have mobility not only refers to the mobility of smart terminals under campus wireless networks, but that between the wireless networks of Telecom, Unicom and mobile operators. In this way, wireless APs are vulnerable to attacks due to lack of protection, leading to the potential of information transmitted by APs being stolen, destroyed or even

tampered. Some attackers may even attack the wireless networks through some devices at arbitrary places.

3.2 There are security problems that lie in hosts and devices of mobile Internet architectures

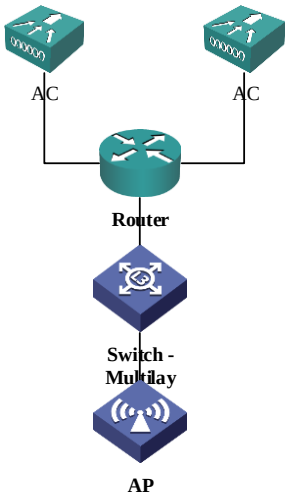

Fig. 2 Centralized forwarding

In the wireless networks blended with all kinds of smart applications, hackers' attacks on hosts are mostly in the form of Trojans. As mobile Internet architectures connect multiple hosts and devices through WIFI, ZigBee, Bluetooth, RFID and WSN[6], attacking hosts and devices with Trojans may pose a great threat to campus networks. Wireless Trojan viruses come with smart terminals, specially attacking the latter through wireless networks.

3.3 Security problems between different business flows

All the business flows of smart Internet architectures are uploaded to ACs from APs. Thus, with all business flows blended together, there exist potential security problems to certain extent.

4. Precautions to security problems

4.1 To forbid SSID broadcast function, and enable the function of hiding SSID on ACs.

4.2 To filter wireless MAC addresses so as to restrict access of smart terminals

Restrict access of illegal clients through APs' capabilities of filtering MAC addresses. Limit access to terminals with different levels of permissions for different clients.

4.3 To adopt encryption techniques so as to control access effectively

It is an effective measure to avoid illegal access by implementing effective supervision and control over all physical terminals accessing the wireless networks. When implementing it, Client can adopt encryption techniques to set up a strict mechanism for verifying password security. Only those who pass password verification can access the networks, which fundamentally helps avoid problems like illegal access.

4.4 To secure data and information safety through the technique of identifier matching in the service zones

During the data transmission of wireless networks, the technique of identifier matching in the service zones can be used to bring the independence of the authorized users with the devices in the wireless networks, in which way not only the security of wireless networks can be enhanced but leakage of personal information avoided, thus promoting the wireless networks to play its positive role.

4.5 To separate different business flows with firewalls to ensure the safety of each business

5. Conclusion

In this paper, a mobile Internet architecture of Smart Campus is designed and the solutions to potential security problems brought by it are proposed. Campus mobile Internet architecture based on

the wireless networks, combining big data and other kinds of systems can provide personalized and smart services for teachers and students.

References

[1] NING Jia jun. "Internet Plus " Implementation of the action plan background, connotation and the main content [J].E-Government,2015,06:32-38.
[2] Wu Min yu, Liu Huan, Ren You qun ."Internet Plus Campus": A New Phase of "Smart Campus" Construction of Colleges[J]. Journal of Distance Education,2015,04:8-13.
[3] Conte G, De Marchi M, Nacci A A, et al. BlueSentinel: a first approach using iBeacon for an energy efficient occupancy detection system[C]// Proceedings of the 1st ACM Conference on Embedded Systems for Energy-Efficient Buildings. ACM, 2015.
[4] Madlmayr G, Langer J, Kantner C, et al. NFC Devices: Security and Privacy[C]// Availability, Reliability and Security, 2008. ARES 08. Third International Conference on. IEEE, 2008:642-647.
[5] Tei R, Yamazawa H, Shimizu T. BLE power consumption estimation and its applications to smart manufacturing[C]// Society of Instrument and Control Engineers of Japan (SICE), 2015 54th Annual Conference of the. IEEE, 2015.
[6] William Lehr, Lee W McKnight. Wireless Internet access: 3G vs. WiFi?[J]. Telecommunications Policy, 2003, 27(03):351-370.
[7] Pottie G J, Kaiser W J. Embedding the Internet: wireless integrated network sensors[J]. Communications of the Acm, 2000, 43.
[8] SUN shi feng, The key technology of wireless network security[J].Network Security Technology & Application,2015,09:78+80.