

Management and Diagnosis Architecture for a Large-Scale Public WLAN

†Seongkwan Kim, ‡Se-kyu Park, †Sunghyun Choi, §Jaehwan Lee, and §§Hanwook Jung

†School of Electrical Engineering and INMC, Seoul National University

‡Applications Team, Cambridge Silicon Radio (CSR) Korea

§Department of Computer Science, University of Maryland

§§Convergence Project Team, Korea Telecom

skim@mwnl.snu.ac.kr, kevin.park@csr.com, schoi@snu.ac.kr, jhlee@cs.umd.edu, hanuk@kt.co.kr

Abstract

In Korea, a large-scale IEEE 802.11b-based public wireless LAN (WLAN) service, called NESPOT, has been in operation by Korea Telecom (KT) across the country during the last four years. Along with a fast growth of the service, however, the service quality problems have been encountered. In order to manage and overcome such problems properly, we have developed a diagnostic tool, which is composed of a database for wireless connection-related dissatisfaction, a log collector and analyzer, and a mechanism to report breakdown of access points (APs). To our best knowledge, this is the first attempt to address an integrated management and develop a diagnosis architecture for large-scale commercial WLANs.

1. Introduction

Korea Telecom (KT), the largest telecommunication and Internet Service Provider (ISP) in Korea, started a public wireless Internet service provisioning based on IEEE 802.11b Wireless LAN (WLAN) in early 2002 [3]. This WLAN service is called NESPOT [1]. As of late 2005, it serves over 500,000 subscribers with about 16,000 hotspots comprising over 280,000 access points (APs) in operation. However, as the number of subscribers and deployed APs increase, KT has been encountering a number of issues related to service quality and maintenance of the NESPOT system. Sometimes, NESPOT subscribers experience and complain problems such as lack of coverage, poor network performance, and intermittent connectivity, and hence KT has made efforts to overcome such obstacles.

In order to understand possible problems in NESPOT, we have modeled and developed (1) a centralized error log database, which collects user-side access error, that are cat-

egorized and are automatically reported using a specific client-side software, and (2) an error log collecting and analyzing tool. By using these diagnostic approaches, we found several causes, which degrade the NESPOT service quality, and we have proposed appropriate solutions to overcome some of the identified error causes. Moreover, to efficiently maintain malfunctioning APs, which are spread out over the country, we propose an automatic broken-down AP reporting scheme in this paper.

To our best knowledge, this is the first effort to diagnose and manage a large-scale commercial WLAN. We believe that our diagnosis architecture and the corresponding outputs are helpful for other WLAN users, researchers, and administrators of WLANs to better understand the networks and provide a better quality service.

The rest of the paper is organized as follows. Related work is presented in Section 2. Possible problems experienced by WLAN users during communications are described in Section 3. The error-log reporting system as well as log collector and analyzer are presented in Sections 5 and 6, respectively. Section 7 introduces a broken-down AP reporting mechanism, and finally, the paper concludes in Section 8.

2. Related Work

Many researchers have explored the wireless network installed and managed in their own campus site [16, 14, 17, 13]. Tang and Baker have analyzed a 12-week trace of a WLAN usage in their department [16]. Voluminous trace information from 74 wireless users has been collected using tcpdump, simple network management protocol (SNMP) traces, and authentication logs. Kotz and Essien have explored a significantly larger scale experiment covering a much longer duration in the Dartmouth campus [14]. Moreover, they have analyzed the wireless network again for sev-

enteen weeks over years 2003 and 2004. Based on the earlier work, Kotz *et al.* found dramatic increases in usage, and changes in applications and devices used in the same (but quantitatively enlarged with respect to WLAN devices and APs) network [13].

Most of the above research have mainly used SNMP traces to collect data and to analyze statistics. However, since our research objective is focused on the analysis of end user's distress, which is experienced especially in wireless part, we needed a new diagnostic mechanism for user-side (wireless-part) trouble. Such an objective is fundamentally different from the previous work in which researchers tried to analyze WLAN itself and users' traffic pattern. For this reason, a *users' error log database*, so called *NeSAS*, has been developed by KT. By exploiting and examining NeSAS error logs, we can get more benefits than a SNMP-based WLAN management model. The details of NeSAS is described in Section 5.

While all the empirical research described above have focused on analyzing traffic patterns and WLAN network itself, Adya *et al.* proposed a new diagnosis architecture for wide-scale deployment of WLAN network in Microsoft corporations [6]. Before their work, diagnosis tools for IEEE 802.11-based wireless networks have been supported only as vendor-specific solutions [7, 8, 9]. We here briefly summarize their technical features based on the introduction found in their company web pages. A vendor-independent management solution [9] supports new and legacy WLAN devices from different vendors and handles all communications among multi-vendor devices, allowing administrators to monitor and configure diverse WLANs from the visualized web console. Security threat is concerned as a management component [7, 8]. *Rogue AP*, i.e., "unauthorized AP," which has no authority to allow any associated station to access the network, must be a kind of intrusion into a WLAN system, so that it should be detected and removed. One of the proprietary solutions provides such a functionality, and hence this threat can be removed by detecting Rogue AP's location [8].

While such proprietary products have their own special functionalities for WLAN diagnosis, the features provided by these manufactures are more towards network-management purpose. In [6], however, the authors provide tools for detection, isolation, diagnosis, and correction of faults, which are complained by end users. One proposed technique, called *Client Conduit* protocol, enables the fault diagnosis of disconnected clients with aid of *Diagnostic Server* and *MultiNet* [10].

In spite of the novelty, their work has some limitations with respect to a public wireless Internet service provider (WISP) as follows: (1) A client-side modification is needed. That is, since a WISP cannot normally provide any diagnostic function in Operating System (OS) level, it is not easy to provide a special client-side function such as Client Conduit.

(2) Proposed diagnostic architecture in [6] is more appropriate for company-wide WLANs, not for county-wide commercial WLAN service. For example, for Client Conduit, an additional operation mode, MultiNet, is needed. However, in most cases, the commercial WISP does have a control over the types of WLAN adapter cards to be used in its network, and hence the WISP network should be able to provide a service to any type of WLAN adapter cards. Accordingly, in the paper, we present our distinctive (i.e., applicable to a country-wide WLAN, independent of the types of client devices and WLAN adapters, and easily-usable by any unspecialized user) features, which have been developed by exploiting and diagnosing the country-wide commercial WLAN.

3. Possible Faults in Public WLANs

In this section, we identify the most important faults that WLAN users and network administrators can encounter due to the characteristics of a large-size WLAN such as KT NESPOT.

3.1. Unreliable Connectivity

WLAN users can experience troubles due to unstable wireless connection or wireless connection-setup failure. In NESPOT, the connectivity problem is classified into the following two cases: (1) initial-access failure and (2) intermittent connectivity. While intermittent connectivity can be caused by time-varying wireless channel condition, user's mobility, and low signal quality, initial-access failure is due mainly to user's mistake and access attempt in a marginal area of the service coverage. In order to minimize the initial-access failure, KT has developed the NeSAS DB. Error-logs in NeSAS are collected from each individual NESPOT user via NESPOT Connection Manager (CM), and are analyzed by using the log collector and analyzer, which are also developed for NESPOT diagnosis, in comparison with AP logs. From the analysis, we have estimated and found possible causes, which lead an initial-access failure, and propose a possible solution to minimize such access failures in NESPOT.

For the intermittent connectivity problem, only a dense deployment of WLAN APs can be the ideal solution. Instead, we propose a practical solution, which is an automatic broken-down AP reporting mechanism and it is surely a useful solution for managing such a large-scale WLAN network.

3.2. Performance Degradation

In a WLAN, a user can experience degraded performance due to co-channel interference from adjacent Basic Ser-

vice Sets (BSSs)¹, which is caused by poorly planned network, time varying wireless channel condition, user's mobility, malfunctioning network components, and so on. For NESPOT, co-channel interference and time-varying channel effect should be carefully considered from the initial stage of deployment, and hence we do not take them into account in the paper. As the size of a WLAN increases, however, the number of malfunctioning components (especially, APs) might increase. Therefore, an efficient recovering mechanism for such malfunctioning APs is highly desirable.

3.3. Network Security Issue

User's authentication problem and existence of Rogue APs in a WLAN can be severe threats in the perspective of WLAN users as well as network administrator. Even though we consider a well-controlled commercial system, it is possible that there exist Rogue APs. In fact, all the NESPOT APs use the same Service Set Identifier (SSID), which is "NESPOT," and hence a malicious person can easily place a rogue AP, i.e., an AP with SSID set to NESPOT, but without a proper network configuration². Therefore, we estimate the possibility of the existence of rouge AP(s) by analysis of user error logs in NeSAS and APs' logs. For the user authentication, NESPOT employs IEEE 802.1x-based authentication mechanism as many large-scale WLAN systems do [4]. Since such a user-authentication procedure operates automatically by an authentication program, misuses by each WLAN user can lead to corresponding problems (e.g., sharing personal identification information, typing invalid ID/password, and so on).

4. Access Procedure in KT NESPOT

In this section, we describe the NESPOT initial-access procedure to better understand the proposed NESPOT diagnosis architecture. The initial-access procedure of NESPOT is composed of IEEE 802.11 association, IEEE 802.1x authentication, and dynamic host configuration protocol (DHCP)-based IP address assignment. An IEEE 802.11 association consists of scanning, authentication, and association, which occur in order [2]. Since an 802.11 association is often automatically conducted right after a WLAN adapter is turned on, it does not make any problematic issue. Therefore, we do not take it into account in the paper. As discussed in Section 3, many problems can be induced during the NESPOT initial-access procedure, so that we describe the procedure in the following.

¹A BSS is composed of an AP and users associated with the AP.

²Generally, a "Rogue AP" represents a hole in the corresponding WLAN, accessible by unauthorized users. On the other hand, the considered intrusion, i.e., a rogue AP with SSID of NESPOT, in this paper, might not give an access to the network so that legitimate NESPOT users can be very unhappy with the network access quality.

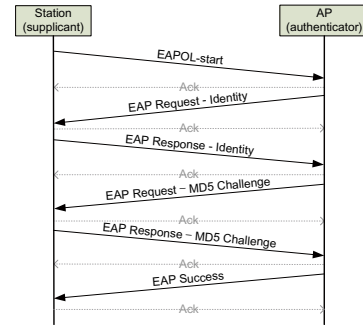


Figure 1. IEEE 802.1x authentication process

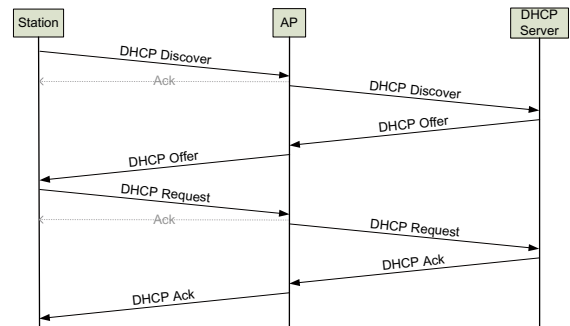


Figure 2. DHCP protocol

4.1. IEEE 802.1x Authentication Process

After associating with an AP successfully, the station³ starts the IEEE 802.1x authentication by transmitting an EAPOL (EAP over LAN)-start frame to the associated AP, and an exchange of 802.1x frames follows as shown in Fig. 1 [4]. Besides this figure, there is unillustrated 802.1x authentication entity, RADIUS (Remote Authentication Dial In User Service) server, which is called an authentication server in IEEE 802.1x terminology, while station and AP are called supplicant and authenticator, respectively [15].

As shown in Fig. 1, EAP-MD5 (Extensible Authentication Protocol-Message Digest 5) [5] is employed in NESPOT for 802.1x authentication, and user identification and password are used to authenticate a user. However, current Microsoft Windows OS's such as *Windows XP* do not support EAP-MD5. Therefore, a software, which takes care of EAP-MD5 authentication, is needed for NESPOT user authentication. For this reason, KT distributes NESPOT user-authentication software, called NESPOT CM (CM) to support various WLAN devices.

Any frame transmission failure during the six-way hand-

³We refer to a station as a WLAN client or user device.

shake of 802.1x authentication procedure is reported to NeSAS along with the corresponding error code. The detail about this error report is presented in the next section.

4.2. DHCP Process

While IEEE 802.1x authentication is initiated and conducted, Dynamic Host Configuration Protocol (DHCP) is also launched at the same time [12] so that the station can obtain an IP address dynamically. As illustrated in Fig. 2, DHCP protocol consists of a four-way handshake of broadcast frames (with the destination address set to the broadcast address, i.e., 0xFFFF). Note that the 802.11 provides only unreliable broadcast, and it implies that broadcast frames are not acknowledged. However, in Fig. 2, since any uplink data frame in IEEE 802.11 infrastructure mode is always transmitted in a unicast manner (even if its final destination address is the broadcast address), a station should receive an Ack frame from the associated AP. If there is no 802.11 Ack for an uplink frame transmission, the frame can be retransmitted according to the 802.11 Medium Access Control (MAC) operation. This makes the transmission of DHCP Discover and DHCP Request more reliable compared with the other two, i.e., DHCP Offer and DHCP Ack.

5. NeSAS: User Error Log Database

In order to efficiently analyze all possible errors during initial-access procedure, we have classified the errors, and enumerated them as corresponding error codes from 000 and 008. When an access failure occurs, the related information along with the corresponding error code is stored at a depository of a station, and then it is reported to the NeSAS server when the station accesses NESPOT successfully in a later time. For this process, a specific client-side software is needed. Fortunately, as NESPOT already utilizes a user-side software for NESPOT user authentication (i.e., NESPOT CM), the problem can be easily solved by implementing the error report process into the existing NESPOT CM. It is an advantage of such a software-based authentication approach, which KT has employed. If a web-based authentication method is utilized as many other commercial WLAN-based WISPs, such a functionality is difficult to be incorporated.

All errors during NESPOT initial-access procedure are reported to the NeSAS server by NESPOT CM using the HTTP protocol along with the corresponding log and error code. The log information includes error event time, user ID, BSSID (i.e., the MAC address of the AP), and RSSI (i.e., the received signal strength measured when the access failure occurred). Fig. 3 illustrates different types of error codes and the corresponding meanings. Note that other than the illustrated error cases, the main authentication procedure is

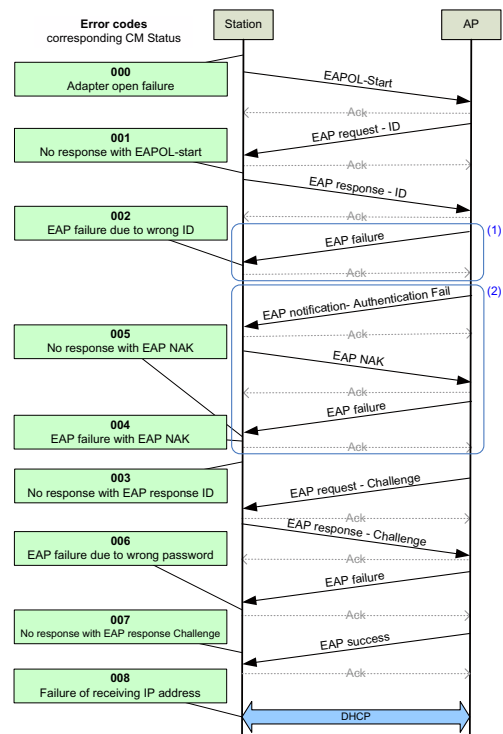


Figure 3. Error codes reported from CM to NeSAS server

identical to what is shown in Fig. 1. For error codes 000, 002, and 004, which are not self-explanatory in Fig. 3, the detailed meanings are described as follows:

- **000 Adapter open failure:** Before sending the first 802.1x frame, EAPOL-start, a station should be associated with an AP. When the association process fails or a user attempts to access NESPOT network without turning on a WLAN adapter, error code 000 occurs and will be reported.
- **002 & 004 EAP failure due to wrong ID / EAP NAK:** When a NESPOT user enters her/his ID incorrectly, two possible errors can occur such as (1) and (2) in Fig. 3. In the second case, AP can inform a specific reason of authentication failure using *EAP notification-authentication failure* message. This is possible only for new versions of CM, while some old versions of CM cannot understand the message, and hence code 002 is used instead. Even though a specific cause of authentication failure can be informed by using error code 004, all the notified causes are only invalid ID and duplicated log-in cases during our log analysis.

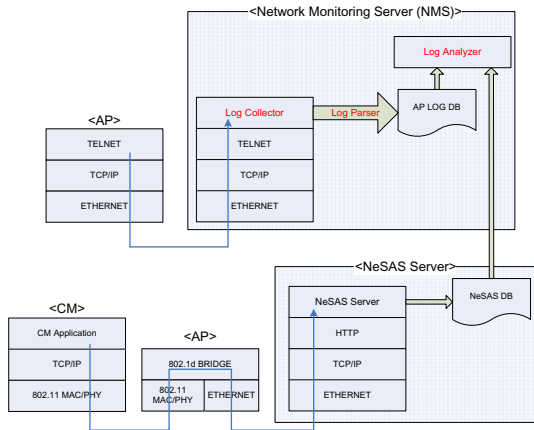


Figure 4. Log-collector and analyzer in NESPOT NMS

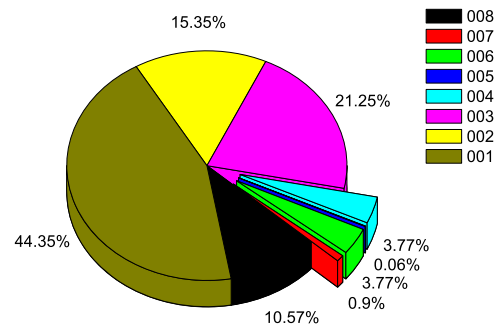


Figure 5. Statistical analysis of NeSAS DB

6. NESPOT Log Collector and Analyzer

As presented in the previous section, the user log information gives some hint about what the user experiences over the air. In our diagnosis architecture, we utilize the system logs at the APs along with the user logs reported to the NeSAS server. AP's system log identifies whether a connection failure is due to the wired part in AP or the wireless part of station. For example, when 001 error occurs, with the corresponding AP-side system log information, we can identify whether it is due to transmission error in wireless link, due to AP failure, or due to an attempt to access a rogue AP. KT already developed NESPOT management protocol, called *Dr. NESPOT*, which has been in operation. *Dr. NESPOT* was developed as a unified utility to handle erroneous situations and maintenance of NESPOT APs, so that it provides common interfaces of APs from different vendors, which have their own proprietary contexts [11]. While *Dr. NESPOT* defines a protocol to fetch each AP's log, the syntax of the system logs into a formatted data structure is not defined yet. Therefore, a program, called *log-collector*, to periodically fetch and store AP's system logs is developed.

A *log-analyzer* program finds any anomalies in log data by cross-checking AP system log DB and NeSAS DB so that we can identify the cause of an error log. The schematic of log-collector and analyzer is illustrated in Fig. 4.

Through a systematic analysis of NeSAS DB and AP system log DB, we find a consistent trend of reported error logs. We draw the statistical trend as illustrated in Fig. 5. The result in Fig. 5 is extracted from the samples (approximately, over 4,474,000 samples) in NeSAS DB from Aug. 10 to Aug. 19, 2004. As shown in Fig. 5, error codes 001, 002,

and 003 are the major ones. Moreover, we estimate possible causes, which lead the corresponding errors in the figure, as shown in Table 1. We also find that one of the major error causes is "access attempt at marginal link area" with many packet transmission errors due to bad link quality. Considering the large portion of 001 and 003 errors, we conclude that this cause could be one of the major factors affecting the NESPOT initial access performance. Hence, we recollect samples with the Receive Signal Strength Indication (RSSI) value of below -80 dBm, which implies that a user attempted to access NESPOT at marginal link (low signal strength) area. The filtered samples and their distribution are plotted in Fig. 6.

Table 1. Error codes and estimated causes

Codes	Causes
001	Disassociated during authentication 802.1X protocol failure due to an AP bug Associated with a rogue AP Retrial from previously authenticated station Access attempt at marginal link area
002	Non-existing ID Duplicated log-in
003	Error in wireline part Access attempt at marginal link area
004	Non-existing ID Duplicated log-in
005	Disassociated during authentication Access attempt at marginal link area
006	Wrong password
007	Disassociated during authentication Access attempt at marginal link area
008	Disassociated during authentication Receiving valid IP, but not allowed by CM Access attempt at marginal link area

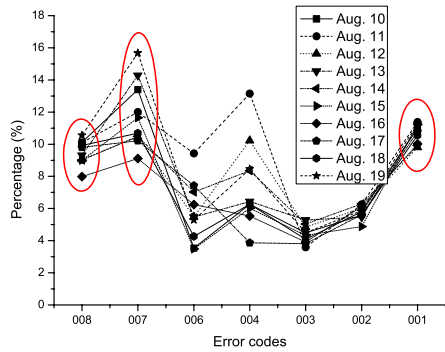


Figure 6. Error ratio below -80 dBm RSSI

As shown in Fig. 6, more than 10 % of reported errors (in average) is due to access attempt at marginal link area in cases of 001, 005, 007, and 008 errors. For the cases of 004 and 006 errors, the average value is below 10 % and the actual portions plotted in Fig. 5 are not enough to consider in detail, so that we have only focused on 001, 005, 007⁴, and 008 errors as well as the major cause of them, i.e., access attempt at marginal link area.

We have worked on the issue of access attempt at marginal link area, and proposed the *fragmented unicast* transmission of DHCP packets, as solutions for the problem. Due to the lack of space, we here briefly discuss how much gain is expected from the approach without presenting its exact details. Fig. 7 shows the validity of our solution. The solid line and the triangle points illustrate the access error probability of the original 4-way handshake DHCP process by simulation and mathematical analysis, respectively. As illustrated as the dashed line and the square points, if the relatively large-size DHCP packets⁵ are fragmented and each fragment is transmitted in a unicast manner, the transmission range is extended. For instance, by applying our fragmentation and unicast transmission approach, a station can get an IP address at the location of 83-meter distance from its AP with about 70 % success probability, while a station with the original DHCP process has above 60 % success probability when a station is located 80 meters away from its AP. The extended distance in Fig. 7 is roughly 3 meters, but the actual amount of enlarged coverage in 2 dimensional area is approximately over 1500 square meters.

⁴In fact, error portions of 005 and 007 errors in Fig. 5 are comparatively small. Moreover, the daily distribution of 005 error with the RSSI value of below -80 dBm is quiet unstable due to its small amount of error samples, so that its error ratio is not shown in Fig. 6.

⁵The average MPDU (MAC Protocol Data Unit) size of DHCP packets is 374 bytes, while the average MPDU sizes of 802.11 association and 802.1x authentication frames are 40 and 54.5 bytes, respectively.

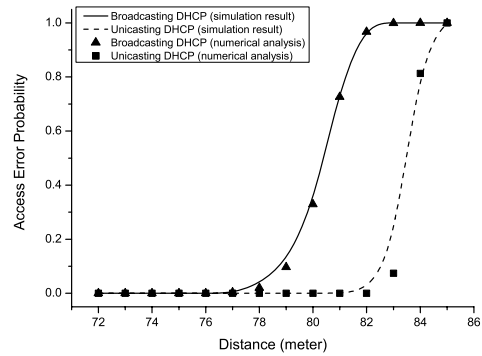


Figure 7. Access probability at marginal area

Considering the scale of the wide-area commercial WLAN, the above contribution in each BSS is considerable. Therefore, by applying a simple and efficient approach, i.e., fragmentation and unicast transmission of DHCP packets, we can reduce the problem with the access attempt at marginal link (signal-strength) area. Accordingly, we expect that the numbers of 001, 007, and 008 errors can be decreased. The evaluation of our proposal has been done by only simulation and mathematical analysis so far. In the future, we plan to evaluate the proposed approach in the KT NESPOT practically.

7. Reporting AP Breakdown

As of early 2005, KT operates about 16,000 hotspots and over 280,000 APs. Considering such a huge size, it is very important to manage and locate broken-down APs automatically. Moreover, broken-down APs are known as one of main reasons causing user dissatisfaction. Therefore, we propose a method of reporting AP's breakdown autonomously. An automatic reporting scenario of AP's breakdown is as follows. An AP self-diagnoses its breakdown due to the unreachability of its RADIUS server. Then, it changes its Service Set Identifier (SSID) into *NESPOT_STU001* automatically, and conveys the modified SSID in the beacon frames. The normal SSID used by NESPOT APs is the same as the name of the service, i.e., NESPOT, and STU001 means Service is Temporarily Unavailable due to unreachable RADIUS server. Once a station receives a beacon frame with such a modified SSID, it stores the SSID and AP's BSSID (Basic Service Set Identification, which is the AP's MAC address). When the station accesses NESPOT successfully at a later time, CM reports stored error-logs as well as the SSID information to the NeSAS server. Therefore, a network administrator of NESPOT can be easily informed,

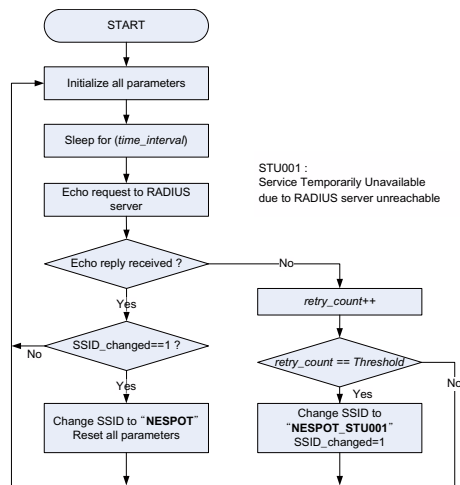


Figure 8. Breakdown detection and reporting procedure in AP

which AP operates abnormally and why or how (using the SSID).

The detailed procedure for a NESPOT AP to check its connectivity to the RADIUS server, and changes its SSID upon the detection of a unreachability is illustrated in Fig. 8. An AP sends an Echo request packet to the NESPOT RADIUS server periodically with the period of *time_interval*. If the AP does not receive a corresponding Echo reply packet from the RADIUS server within a given *time_out* duration, it increases *retry_count* and resends another Echo request packet after the *time_interval* duration. If the AP does not receive an Echo reply packet and the *retry_count* has been increased up to the *Threshold*, it changes its SSID into NESPOT_STU001, which will be conveyed in beacon frames. Sometimes, an AP cannot receive an Echo reply due to some temporary errors (e.g., network congestion in wired network, rebooting RADIUS server, and so on). The changed SSID should be restored after the temporarily unreachable problem is resolved, and hence we reflect this possibility in the reporting process.

Even if we have exemplified the RADIUS server unreachability above, the proposed broken-down AP reporting scheme can be used for different types of errors or status report purposes as well, e.g., DHCP server failure. We will extend our reporting method in consideration of various causes of breakdown in the future.

8. Conclusion

As the scale of WLAN increases in terms of the numbers of deployed APs, hotspots as well as subscribers, the need

for the network management and diagnosis architecture has emerged. In this paper, we propose a diagnosis architecture for a public (commercial) WLAN, called KT NESPOT. The proposed architecture consists of the following components: (1) user error-log reporting and gathering system, (2) log collector and analyzer, and (3) broken-down AP reporting system. By exploiting our diagnosis architecture, NESPOT administrator can easily maintain and recover the system, and users can experience a more fault-tolerant WLAN. We believe that our research work can be a good reference for relevant WLAN users and network administrators to utilize and manage the large-scale commercial WLAN systems more efficiently.

References

- [1] KT NESPOT. [online] <http://www.kt.co.kr/index.jsp/>.
- [2] IEEE 802.11, *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications*, 1999.
- [3] IEEE 802.11b, *Supplement to Part 11: Higher-speed Physical Layer Extension in the 2.4 GHz Band*, 1999.
- [4] IEEE 802.1X, *Standards for Local and Metropolitan Area Networks: Port-Based Network Access Control*, 2001.
- [5] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowitz. Extensible Authentication Protocol (EAP). IETF RFC 3748, June 2004.
- [6] A. Adya, P. Bahl, R. Chandra, and L. Qiu. Architecture and Techniques for Diagnosing Faults in IEEE 802.11 Infrastructure Networks. In *Proc. ACM MobiCom*, Sept. 2004.
- [7] AirDefense. Self-Managing Wireless Intrusion Protection. [online] <http://airdefense.net/>.
- [8] AirMagnet. Enterprise Wireless Intrusion Detection and Protection Solution. [online] <http://airmagnet.com/>.
- [9] AirWave. AirWave Wireless Management Suite. [online] <http://airwave.com/>.
- [10] R. Chandra, P. Bahl, and P. Bahl. Multinet: Connecting to Multiple IEEE 802.11 Networks Using a Single Wireless Card. In *Proc. IEEE INFOCOM*, Hong Kong, Mar. 2004.
- [11] Y. Choi, S. Park, S. Choi, G. W. Lee, J. H. Lee, and H. Jung. Enhancement of a WLAN-Based Internet Service. *ACM Mobile Networks and Applications*, 10(3), June 2005.
- [12] R. Droms. Dynamic Host Configuration Protocol (DHCP). IETF RFC 1531, June 1993.
- [13] T. Henderson, D. Kotz, and I. Abyzov. The Changing Usage of a Mature Campus-wide Wireless Network. In *Proc. ACM MobiCom*, Sept. 2004.
- [14] D. Kotz and K. Essien. Analysis of a Campus-wide Wireless Network. In *Proc. ACM MobiCom*, Sept. 2002.
- [15] C. Rigney, S. Willens, A. Rubens, and W. Simpson. Remote Authentication Dial In User Service (RADIUS). IETF RFC 2865, June 2000.
- [16] D. Tang and M. Baker. Analysis of a Local-Area Wireless Network. In *Proc. ACM MobiCom*, Aug. 2000.
- [17] J. Yeo, S. Banerjee, and A. Agrawala. Measuring Traffic on the Wireless Medium: Experience and Pitfalls. Technical report, Univ. of Maryland, Dec. 2002.