Method for Remotely Diagnosing Failures in Wireless LAN Systems

● Hiroshi Fujita ● Yun Wen ● Kazuyuki Ozaki ● Chikara Kojima

Many offices and work sites have been migrating LAN and machine-to-machine (M2M) systems they use for local device access to wireless LANs, which are easily accessible and are a cost-effective means of providing access. However, wireless LANs are susceptible to interference from other devices, and their communication ranges are limited. These environmental factors affect data communication quality and thus destabilize their performance. To maintain stable performance, it is important to establish an operation system capable of quickly detecting failures in a wireless network and promptly reestablishing communication. It is also important to keep the cost low. We identified two requirements for achieving wireless LAN management at low cost: additional device functionality is not required, and the system manager is able to identify the causes of problems and/or the affected sections of the network without having to be on-site. We have developed a network-driven remote failure diagnostic method that meets these requirements and have evaluated its effectiveness using computer simulation. This paper describes the operating principle of this method and the results of the evaluation.

1. Introduction

Many office LAN systems and machine-to-machine (M2M) systems for local device access are now being migrated to wireless networks. This migration is providing users with more opportunities to use a wireless LAN conforming to the IEEE 802.11 standard[1)] as a communications system. The frequency bands allocated to wireless LANs (2.4 GHz, 5 GHz) are unlicensed, which means that anyone can easily construct a network on those bands, and the fact that they require no communication fees has been driving the adoption of wireless LAN. The result is a virtuous cycle in which many products are now being equipped with a wireless LAN function and a drop in prices is making it easier for users to acquire such products.

However, the quality of communications with a wireless LAN depends on the environment and can therefore fluctuate. This means that a LAN's level of quality may be less than that envisioned during construction. For example, the use of an unlicensed frequency band opens up the possibility of radio-frequency interference from other devices using the same band. In addition, the very weak transmission power of devices using these frequency bands means that they have short transmission distances and are susceptible to the effects of blocking by buildings, walls, and other structures. Under such conditions, an operation and management system that can quickly detect and resolve issues in the wireless network is essential to maintaining stable performance.

Wireless network outsourcing is an attractive means of meeting the needs of wireless LAN operation and management.[2)] A service provider designs the wireless network and then operates and manages it. This enables even users with no specialized knowledge of radio communications to make use of a wireless network. There is still room for improvement however in the way that operation and management services respond to failures in a wireless network. For example, a service provider with a limited number of personnel and providing services to several customers has to manage multiple wireless networks in an efficient manner, and it is unrealistic to install an operation monitoring function in existing user wireless terminals. It is therefore important that the occurrence of a failure and the range of its impact be determined remotely to prevent

as much as possible the need to visit the affected site. However, with existing failure diagnostic methods, it is necessary to either add a new function to wireless terminals or visit the site to install dedicated monitoring equipment. Needless to say, this can drive up the cost of network operation and management.

Fujitsu Laboratories has been researching ways to achieve stable performance in wireless systems.[3] In particular, we have been developing a diagnostic and control technology that will enable simple and efficient operation and management of a wireless LAN system that connects to the core system of an enterprise.

We, the authors, have identified two requirements with respect to the operation and management of wireless LANs. First, there must be no need to add new functions to user wireless terminals; second, the system manager must be able to identify the location and cause of a problem from the network side without having to visit the site itself. We have developed a network-driven remote failure diagnostic method that satisfies these requirements and have evaluated its effectiveness by computer simulation. In this paper, we explain the operating principle of this method and present the results of our evaluation.

2. Failures in wireless LANs

The causes of failures in wireless LANs can be broadly divided into interference from other devices using the same frequency band, a drop in receive power due to blocking along the radio signal path, and failure of the wireless device itself.[4]

Devices that can interfere with a wireless LAN include wireless LAN devices using the same frequency band (2.4 GHz, 5 GHz), Bluetooth and ZigBee communication devices sharing the industrial, scientific, and medical (ISM) radio bands, and non-communication devices such as microwave ovens and microwave therapeutic equipment. In addition, radio signals from meteorological radar and marine radar in the 5 GHz band can also interfere with wireless LANs. Since radio signals from all sorts of devices are constantly being transmitted, the frequency band (channel) allocated to each access point (AP) during the system design stage should be chosen so as to minimize interference among the APs. However, if APs are subsequently added due to an increase in traffic volume or expansion of the coverage area, interference may occur between an existing AP and a new AP using the same channel. Data transmitted from those APs may overlap when they arrive on the receive side and thereby prevent their separation. One way to handle this failure in data transmission and reception is to resend the data. Doing this, however, incurs a delay and lowers throughput. This means that the time taken to download content or respond to an entered command can deteriorate remarkably, which can make wireless LANs unsuitable for a core system.

In addition, receive power can drop if the radio signal path is blocked by walls, shelves, or other obstacles. If it drops substantially, radio signals may never arrive on the receive side, preventing the terminal from connecting to the network. Accordingly, signal propagation must be measured when installing an AP to determine where exactly it should be installed to secure sufficient receive power in terminals. However, a change in room layout can involve a change in the positions of partitions, shelves, and other physical objects, resulting in subsequent blocking of signals. Additionally, while the AP equipment may have been operating normally at the time of installation, equipment malfunctions due to accidents during use or deterioration over time cannot be prevented.

The quality of communications provided by a wireless LAN can therefore change frequently after operation commences, so there is a need for operation and management that can maintain performance in an ongoing manner.

3. Issues in operation and management of wireless LAN

Two issues must be addressed to enable a system manager to operate and manage a wireless LAN so as to maintain stable performance.

1) Remote monitoring

The conventional approach to dealing with a reported failure in a wireless network is to analyze logs and measure signal propagation on-site, as illustrated in **Figure 1 (a)**. The need for the system manager to analyze logs and/or perform signal-propagation measurements can create a considerable workload. Furthermore, for a rare event, much time may be needed to reproduce it. In short, uncovering the source of a failure and resolving the problem has tended to be a lengthy process, which has greatly inconvenienced users and magnified the manager's workload. The

need therefore arose for a method that could automatically monitor network quality and detect failures.

2) Identifying the cause and location of a failure

Since the countermeasure to a wireless failure depends on its cause and location, the cause and location must be accurately determined. In addition, the ability to automatically determine the cause and location of a wireless failure would improve the manager's work efficiency. One countermeasure against interference is to change the channel. However, if a certain AP is experiencing interference and its channel is changed, the channels of all other APs may have to be changed as well because the new channel may otherwise interfere with surrounding APs. On the other hand, if a terminal is experiencing interference, its connection can be switched to another AP that is using a channel without interference, thereby eliminating the problem for that terminal.[5)]

One method that has been proposed for remotely monitoring a network for failures and identifying the cause and location of a failure is to introduce failure-monitoring equipment in all user terminals and APs, as shown in **Figure 1 (b)**.[6)] This, however, is not a realistic approach since upgrading all user terminals would be a difficult and expensive task. Consequently, to monitor the network for wireless failures without creating a major burden for both the system manager and users, such a function should be implemented on the network side without adding it to user terminals, as shown in **Figure 1 (c)**.

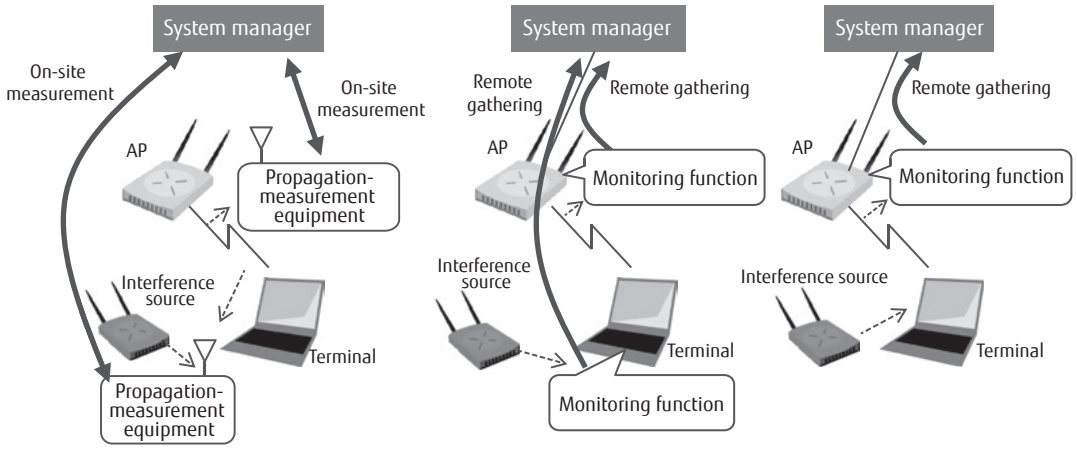
4. Remote failure diagnostic method

4.1 Operating principle

Fujitsu Laboratories has developed a remote failure diagnostic method for wireless LANs that is capable of remote operation from the network side with no need for upgrading user terminals.[7)] This method supports remote failure diagnostics and failure location detection.

1) Remote failure diagnostics using ACK response

The media access method normally used in wireless LANs is carrier sense multiple access with collision avoidance (CSMA/CA). We use the retransmission operating principle of this method to detect the occurrence of a failure caused by interference, an equipment malfunction, blocking, etc. (**Figure 2**). An AP transmitting in accordance with CSMA/CA waits a randomly set time before retransmitting signals to avoid collisions with other packets transmitted by other terminals. If the AP does not detect packet transmission by another terminal during this waiting time, it transmits its packet to the target terminal. If it does detect packet transmission by another terminal, it waits for that transmission to complete and then waits some more for a randomly set time. A terminal transmits an acknowledgement (ACK) signal on successfully receiving a packet from an AP. The time from when a packet is generated at the AP to when an ACK is received at the AP from the



(a) Arrangement of dedicated monitoring equipment

(b) All terminals and APs have a monitoring function

(c) Only APs have a monitoring function

Figure 1
Different approaches to network monitoring.

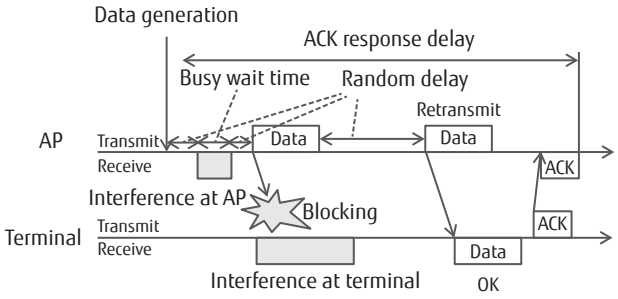


Figure 2
CSMA/CA resend operating principle.

terminal in response to that packet is defined as the ACK response delay. Measuring the ACK response delay for the terminal on the AP side enables the occurrence of a failure to be detected and the type of failure to be diagnosed.

As shown in Figure 2, if interference occurs on the AP side before the AP transmits its packet, CSMA/CA dictates that transmission be suspended (busy wait) until the interference disappears. This increases transmission wait time and thus delays packet reception at the terminal and ACK reception at the AP. The ACK response delay is thus larger compared to the case of no interference. Additionally, if interference occurs on the terminal side with respect to an incoming data packet, a data-packet receive error will occur, and the AP will retransmit the data packet. This also delays return of the ACK to the AP, thereby increasing the ACK response delay. The occurrence of data-packet interference can thus be detected by watching for an increase in ACK response delay.

If blocking occurs between the AP and terminal, or if equipment (AP or terminal) malfunctions, no data packet will arrive at the terminal, and no ACK will be returned to the AP that transmitted the packet. Any blocking that changes over time (fading) due to, for example, human movement is not considered to be a failure since the system can quickly recover from such instantaneous signal blocking as long as the people keep moving.

In short, the cause of wireless failures can be determined by detecting interference on the basis of an increase in the ACK response delay and by detecting blocking on the basis of a failed ACK response.

2) Determining failure location using spatial distribution of affected terminals

The location of a failure is determined from the distribution of ACK response delays of terminals. If interference is occurring on the AP side, the ACK response delay of all terminals increases, and if interference is occurring on the terminal side, the delay of only some terminals increases. Accordingly, failure location can be determined to be on the AP side or terminal side by examining ACK response delay over the entire system. If the cause of the failure is blocking and the obstacle in question is blocking the AP, all wireless communication links will be blocked, and ACK responses from all terminals will be missing. If the cause of the failure is an AP malfunction, packet transmission itself will be nonexistent, which means, of course, no response at all from any terminal. In short, the absence of any response from any terminal means that AP is either blocked or malfunctioning.

In short, the failure location can be narrowed down to the AP side or terminal side on the basis of whether the ACK responses are delayed or are missing for all terminals.

4.2 Evaluation results

With the proposed failure diagnostic method, diagnostic packets are periodically transmitted to all terminals, and the delay or lack of ACK responses to those packets is observed. A lack of responses means that there is blocking. A delay means there is interference. However, a response is delayed only if a diagnostic packet and an interfering packet collide, so detection may not be possible if interfering traffic is generated infrequently. We therefore used a wireless-LAN system-level simulator to evaluate the accuracy with which interference could be detected and to determine the interference location for interfering traffic generated at different frequencies.

The simulation conditions are listed in **Table 1**. One AP and 20 terminals were first arranged in prescribed areas. Next, one interfering AP and one interfering terminal were positioned as sources of interference in accordance with two scenarios: 1) interference affecting AP side; 2) interference affecting some terminals.

For both scenarios, our aim was to determine whether the presence of interference and the terminals affected by interference could be correctly diagnosed. For the AP-side interference scenario, we placed the AP

within the communication range of the interference source and randomly positioned the terminals outside that range, as shown in **Figure 3 (a)**. For the terminal-side interference scenario, we randomly positioned some of the terminals within the communication range of the interference source and placed the AP outside that range, as shown in **Figure 3 (b)**.

In both scenarios, the AP transmits a diagnostic packet to the terminals at 1-second intervals, and failure diagnosis is performed on the basis of delay in ACK response. The existence of interference is determined by comparing the ACK response delay with a threshold value. We used 2.27–2.31 ms as the threshold; it was arrived at by taking the average value of the ACK response delays from all terminals when transmitting and receiving signals when there was no interference and adding to it three times the standard deviation as determined from the fluctuation in observed values. The interfering terminal transmits packets at intervals corresponding to an exponential distribution in terms of average period, as indicated in Table 1. The AP, terminals, interfering AP, and interfering terminal each transmit at a minimum bit rate of 6 Mbps in conformance with the IEEE 802.11 g standard. We evaluated the characteristics of the proposed method with respect to interference traffic density by varying the interfering-packet generation period, which represents the frequency at which interference traffic is generated. The interference traffic density is the ratio of the interference packet length (2 ms) to the interfering-packet generation period. This ratio ranges from 10% to 50%.

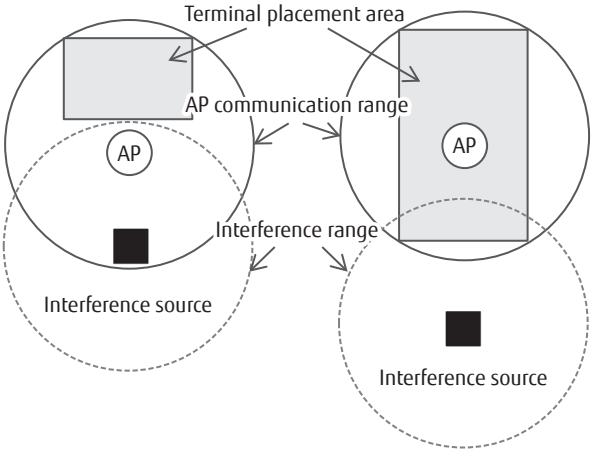
Table 1
Simulation conditions.

Item	Condition
No. of APs	1
No. of terminals	20
No. of interfering APs	1
No. of interfering terminals	1
Communication system	IEEE 802.11g
Bit rate	6 Mbps
Max. no. of retransmissions	4
Path model	2-ray ground reflection model
Antenna height	2 m
Transmission power	20 dBm
Minimum receive sensitivity	-88 dBm
Diagnostic packet size	1500 bytes (2 ms @ 6 Mbps)
Interfering packet size	1500 bytes (2 ms @ 6 Mbps)
Diagnostic-packet transmit interval	1 s, fixed period
Interfering-packet transmit interval	20, 10, 6, 5 ms on average, exponentially distributed period

The distributions of the ACK response delays for each terminal as determined by interference diagnostics are shown in **Figures 4** and **5**. With AP-side interference (Figure 4), the ACK response delay was above the threshold for all terminals; with terminal-side interference (Figure 5), the delay was above the threshold only for those terminals within the range of that interference. In this way, the locations where interference is occurring can be determined by taking a comprehensive view of ACK response delay across all terminals.

The validity of this approach can be checked on the basis of two types of diagnostic accuracy. One is the "successful detection rate," which is the ratio of terminals judged to have interference on the basis of terminal (or AP) diagnostics for which the interference power is equal to or greater than the receive sensitivity. The other is the "erroneous detection rate," which is the ratio of terminals erroneously judged to have interference on the basis of terminal (or AP) diagnostics for which the interference power is less than the receive sensitivity. In other words, a high successful detection rate and low erroneous detection rate means high diagnostic accuracy.

The simulation results are listed in **Table 2**. With



(a) AP-side interference scenario (b) Terminal-side interference scenario

Figure 3
AP and terminal placement for simulating operation.

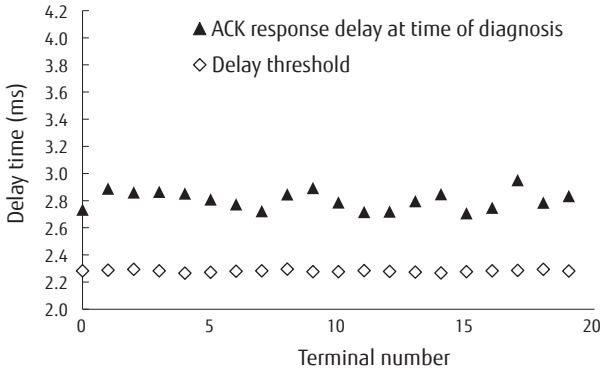


Figure 4
Example of ACK response delay for AP-side interference.

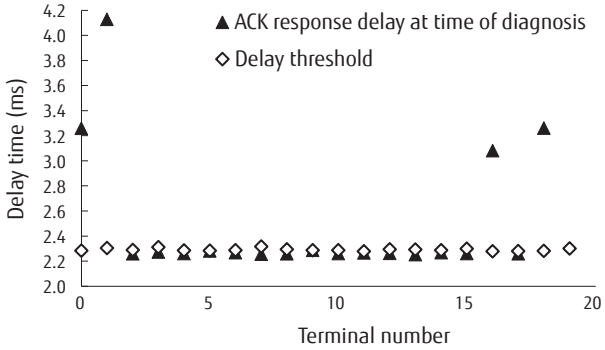


Figure 5
Example of ACK response delay for terminal-side interference.

the AP-side interference scenario, the proposed method achieved high diagnostic accuracy with a successful detection rate of 100% and an erroneous detection rate of 0% for an interference traffic density of 20% or more. With the terminal-side interference scenario, it achieved a successful detection rate of 100% and an erroneous detection rate under 4%. When the source of interference is on the terminal side, data packets are resent, so resend delay is greater than transmission wait time in AP-side interference. High detection accuracy can thus be achieved even for low interference traffic density. These results demonstrate that application of the proposed method enables the occurrence of failures due to blocking or interference and their locations to be correctly determined remotely from the network side. The remote failure diagnostic method that we propose can therefore reduce management costs previously associated with manager dispatch and on-site inspection. Additionally, prompt detection and understanding of the causes of failures can shorten the time to communications recovery and improve the degree of user satisfaction.

Table 2
Simulation results.

Interference scenario	Interference traffic density (%)	Successful detection rate (%)	Erroneous detection rate (%)
AP-side interference	No interference	–	0
	10	85.6	13.1
	20	100	0
	33	100	0
	50	100	0
Terminal-side interference	No interference	–	0
	10	100	2.2
	20	100	2.7
	33	100	2.4
	50	100	3.1

5. Conclusion

The spread of wireless systems using unlicensed frequency bands typified by wireless LAN is increasing the importance of having operation and management systems that can maintain the quality of communications during operations.

This paper described a remote failure diagnostic method that enables failures in a wireless LAN to be diagnosed remotely from the network side so that the LAN can be operated and managed simply and efficiently. With this method, the cause of a failure (blocking/interference) and its location can be determined from the network side by an AP-driven scheme independent of user terminals. Simulation showed that the method can effectively and accurately diagnose network problems. The use of general-purpose parameters such as response delay in normal/failure diagnoses means that the method can also be applied to wireless networks other than wireless LANs.

We plan to hold trials aimed at the introduction of wireless LAN operation and management services based on this method and to improve diagnostic accuracy even further. Moreover, as operation and management include both failure diagnosis and recovery, we will research means of making recovery operations more efficient. Through these R&D efforts, we aim to support the spread of wireless systems by

making them easy to use in a stable state not only in offices but also in the field such as at primary and secondary manufacturing sites.

References

1) Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. IEEE Std 802.11, 2012.
2) Fujitsu Offers FENICS II Business Wi-Fi Service to Promote Business Use of Smart Devices. Press Release, August 2014. *http://www.fujitsu.com/global/about/resources/news/press-releases/2014/0805-01.html*
3) H. Fujita et al: Operation and Management Framework designed for Sensor Networks, Proceedings of the Society Conference of IEICE 2014, BP-3-5 (in Japanese).
4) S. Rayanchu et al.: Diagnosing Wireless Packet Losses in 802.11: Separating Collision from Weak Signal. INFOCOM 2008. The 27th Conference on Computer Communications, IEEE. pp. 13–18 (2008).
5) Amendment 2: Fast Basic Service Set (BSS) Transition. IEEE Std 802.11r-2008, July 2008.
6) T. Huang et al.: EasiPLED: Discriminating the causes of packet losses and errors in indoor WSNs. Global Communications Conference (GLOBECOM), 2012, IEEE, pp. 487–493.
7) H. Fujita et al.: Access Point Initiated Approach for Interfered Node Detection in 802.11 WLANs. IEEE Vehicular Technology Conference (VTC Spring), 11–14 May 2015.

Hiroshi Fujita
Fujitsu Laboratories Ltd.
Mr. Fujita is currently engaged in research and development of wireless LAN operation and management technology.

Kazuyuki Ozaki
Fujitsu Laboratories Ltd.
Mr. Ozaki is currently engaged in research and development of wireless LAN operation and management technology.

Yun Wen
Fujitsu Laboratories Ltd.
Mr. Wen is currently engaged in research and development of wireless LAN operation and management technology.

Chikara Kojima
Fujitsu Laboratories Ltd.
Mr. Kojima is currently engaged in research and development of wireless LAN operation and management technology.