

# A Novel Wireless Network Infrastructure for Manufacturing Equipment Based on Wi-Fi Technology

Shang-Liang Chen, Sin-Ru Wang, You-Chen Lin and Yun-Yao Chen\*

Institute of Manufacturing Information and Systems, National Cheng Kung University,  
No. 1, University Road, Tainan City 701, Taiwan (R.O.C.)

(Received July 2, 2014; accepted March 26, 2015)

**Key words:** Wi-Fi, network infrastructure, manufacturing equipment, wireless data acquisition infrastructure

Production information collection is an important issue for manufacturing. Therefore, data transmission techniques for manufacturing equipment are attracting the attention of researchers nowadays. Traditional equipment data transmissions are based on Ethernet, which encounters issues such as high maintenance cost and unreal-time data transmission. Therefore, a Wi-Fi resource monitoring module (Wi-Fi RMM) is proposed in this research. In addition, a wireless network infrastructure for manufacturing equipment based on Wi-Fi technology is also designed for ensuring data transmission quality in factories.

## 1. Introduction

Some injection molding machine manufacturers are still facing the problem of production management having low efficiency, high consumption, and low yield. The reasons can be analyzed as follows.<sup>(1,2)</sup>

- (1) Low reliability and poor real-time performance due to manual collection of factory statistics. There may be errors and modifications in the process.
- (2) Excess production due to incapability of real-time monitoring of the actual speed of each order and incapability of effective control over factory production schedule.
- (3) No unified network architecture of machines and limited inspection through several connected computers, causing lack of information sharing and inadequate production data for analysis by factory managers.
- (4) Difficulty in real-time feedback owing to the requirement of considerable manpower for on-site inspection when a machine is out of order. In summary, the factory

---

\*Corresponding author: e-mail: yewyewchen@gmail.com

production line has problems, such as inadequate data collection and real-time information feedback, owing to the lack of real-time manufacturing information collection. In general, priority is mostly given to wired networks (*e.g.*, Ethernet), and now some factories employ a wired network architecture based on a factory network, which encounters problems such as maintenance inconvenience and poor real-time performance subject to production environment and line maintenance costs. In this study, we solve the above problems by using Wi-Fi for manufacturing information acquisition.

On the basis of a summary of factory environments, a comparison between wired and wireless networks for factory deployment is shown in Table 1.

Table 1  
Comparison between wired and wireless networks for factory deployment.

	Wireless network	Ethernet wired network
Deployment costs	Low setup cost. Only setup of AP, wireless node, and switch to meet network requirements are needed.	High setup cost. Setup contains a variety of components and equipment such as computer UTP cable and piping. Taking a room for 10 machines as an example, building a wired network would need 10 UTP cables.
Maintenance costs	No need to change settings and construction and no worry about cost changes in the wireless network environment.	Changes in the number and location of wired network users require modifications in settings and line construction, resulting in increased management costs.
Mobile convenience	High mobile convenience. May change wireless node and AP location based on current plan.	Difficult to move machines after set up, and the mobile convenience of the wired network is lower than that of a wireless network when a wired network needs update or modification.
Stability	Average stability. Stability of Wi-Fi transmission will be affected by distance, material, weather, and barrier.	High stability. Transmission occurs through fiber-optic lines; thus, the probability of transmission stability problems is low, except for traffic congestion.
Security	High security. Provides end-to-end encryption and a firewall is built to improve security.	High security. Can build a firewall with enhanced security.
Speed	Depends on Wi-Fi device; the transmission rate of the Wi-Fi module in this study may be up to 300 Mbps.	Depends on factory needs.
Mobility	High mobility; mobile devices can be used directly online for information checking.	No mobility; may only check a machine status via a networked computer.

## 2. Research Perspective

In this study, we build a wireless network for machines in a factory through application of Wi-Fi technology, including the following projects.

- (1) Building a wireless network to improve machine production information via a Wi-Fi setup and achieving the M2M concept for machines in the factory to increase real-time performance.
- (2) Designing a network resource monitoring module, through which the staff can master the wireless network resources in the factory. When the number of connections/flow reaches a threshold, it can automatically alert engineers and provide them with the basis for deployment of wireless network resources to avoid machine data transmission delay.

We conducted Wi-Fi wireless network tests to prove that the Wi-Fi deployment architecture proposed in this study can achieve stable wireless data transmission in the factory.

## 3. Literature Review

Chen *et al.* proposed a remote monitoring platform design for cloud-based machines based on a Wi-Fi wireless factory. In this study, we propose to gather machine information based on Wi-Fi and plan a manufacturing information machine service cloud architecture.<sup>(3)</sup> Moreover, in this study, we consider the Wi-Fi that was proposed as the basic machine information acquisition concept for in-depth analysis of factory disturbances and stability of machine transmission and networking as well as to design and test the factory networking deployment architecture and network resources monitoring module.

### 3.1 Factory networking deployment

A wired Ethernet network is often adopted to set up a network of factory machines. In recent years, the popularity of mobile devices has enabled companies to focus on the provisioning of wireless networks. End-to-end encryption is required for wireless network security, and it provides scalability, security, and mobility, and lowers the cost of wireless networks; its technology has been developed. By considering costs, equipment, back-end management, application, and security, the wired Ethernet network is no longer the best choice.<sup>(4,5)</sup> In this study, we also consider end-to-end encryption in the criteria for networked device selection. Some remote monitoring systems proposed ZigBee for data collection.<sup>(6,7)</sup> ZigBee is characterized by small size, low cost, and considerable reliability, but with a short transmission distance (distance between adjacent nodes of 10–100 m). An increase in power may extend the distance, but it would also shorten the life of the internal battery. By considering the large number of machines and expensive unit price of online machines (often millions of Taiwan dollars), reliable networking equipment without frequent replacement is needed. Therefore, Wi-Fi is used in this study for machine networking.

### 3.2 *Wi-Fi deployment method*

Wireless local area network (WLAN) replaces wired networks through radio technology and communicates with devices via access points (APs) for wireless access. Many devices can use Wi-Fi, *e.g.*, personal computers, smartphones, and digital cameras. These devices can connect to a network resource such as the Internet via a wireless network AP. Such an AP (or hotspot) has a range of about 20 m (66 feet) indoors and a greater range outdoors. Many studies also proposed possible Wi-Fi interference sources as follows.<sup>(8–10)</sup>

- (1) External electronic sources such as power lines, tramways, and generators.
- (2) Use of 2.4 GHz and 5 GHz electronic products, or “dual-band”, “Wi-Fi”, and “wireless” devices in the Wi-Fi range.
- (3) Barriers that prevent Wi-Fi radio wave transmission, including concrete slabs and metal, with the highest interference of approximately greater than 30 dB, and bricks with the second highest interference of 8–12 dB.

When barriers exist, they will cause different wireless transmission range attenuations according to different materials. Interference is the main reason why the wireless network cannot be fully utilized. Two types of interference can be distinguished: (1) adjacent channel interference, which is produced by its transmissions on adjacent or partly overlapped channels, and (2) co-channel interference, which is caused by the same frequency channel.<sup>(11)</sup> The wireless signal interference between both types of interference will be significant and may have the following effects:<sup>(12,13)</sup>

- (1) decrease in transmission range of a wireless network,
- (2) decreases in transmission rate and amount of data transfer per second, and
- (3) intermittent wireless network connection or absolutely no connection.

Many barriers in the factory, such as injection molding machines (metal) and building materials (steel and concrete), pose a great challenge to the Wi-Fi signal transmission range and signal strength. Therefore, in this study, we develop a factory Wi-Fi deployment architecture by simulating wireless signal barriers in space.

## 4. Research Method

### 4.1 *Factory Wi-Fi deployment architecture*

On the basis of our previous research framework “multifactory cloud manufacture information system (m-CMIS)”,<sup>(14)</sup> in this study, we consider the following for factory Wi-Fi module deployment.

- (1) Factory environment: Many barriers in the factory will interfere with Wi-Fi radio signals; therefore, ceilings, beams, and stands will be considered as the position for AP deployment to reduce ground interference.
- (2) Machine data backhaul traffic: Production data will continue to return through the network connection to the server in machine production. When multiple machines return data simultaneously, it may cause a large amount of traffic, hence, the need for backhaul traffic monitoring to ensure transmission stability.

The machine data backhaul traffic monitored and estimated in this study is shown in Table 2. When data transmission starts, the machine needs to exchange packets with the

server to confirm network connection and transfer old data into the database; hence, the traffic is greater than that of average transmissions. In addition, system crashes, server errors, and multiple new machine launches may result in peak traffic. Therefore, in this study, we consider the peak flow caused by these conditions.

In this study, the simulated factory is 26.7 m long, 18 m wide, and approximately 470 m<sup>2</sup>, and the warehouse is 22.8 m long, 10.8 m wide, and approximately 240 m<sup>2</sup>. Each machine is installed with an industrial-grade Wi-Fi transmission module of heat proofing and shock resistance. In addition, in this study, we divide the Wi-Fi transmission module into Wi-Fi nodes and Wi-Fi AP, and plan machine information collection AP deployment by setting up four Wi-Fi APs and 1 switch in the factory, as described in Table 3. The Wi-Fi node installed via an RJ-45 port on the machine provides the machine with wireless capabilities through network settings to transmit machine information to the cloud database through AP connection.

#### 4.2 Design of Wi-Fi resource monitoring module (Wi-Fi RMM)

In this study, the Wi-Fi RMM monitors the number of Wi-Fi nodes connected to APs. We analyzed the loading of network traffic flow of Wi-Fi APs. When APs are overloaded, Wi-Fi RMM automatically warns engineers to allocate network resources. Figure 1 shows a Wi-Fi RMM operational flow diagram. When deployed on the server,

Table 2  
Machine traffic flow estimate.

Number	Steady traffic flow	Simultaneous traffic flow
1	396 kB	—
5	$396 \text{ kB} \times 5 = 1980 \text{ kB}$	4587 kB
10	$396 \text{ kB} \times 10 = 3960 \text{ kB}$	9174 kB
20	$396 \text{ kB} \times 20 = 7920 \text{ kB}$	18348 kB
100	$396 \text{ kB} \times 100 = 39600 \text{ kB}$	91740 kB

Table 3  
Factory network provisioning.

Ethernet wired network			
Number	Region	Location	Scope of services
E1	Office 2	Desk	Office 2
Wireless network (Wi-Fi)			
Number	Region	Location	Scope of services
W1	Manufacturing and processing area (left)	Ceiling	Manufacturing, processing, and testing area
W2	Manufacturing and processing area (right)	Ceiling	Manufacturing area
W3	Office 1	Desk	Meeting room, Office 1, mold warehouse
W4	Product warehouse	Ceiling	Product warehouse

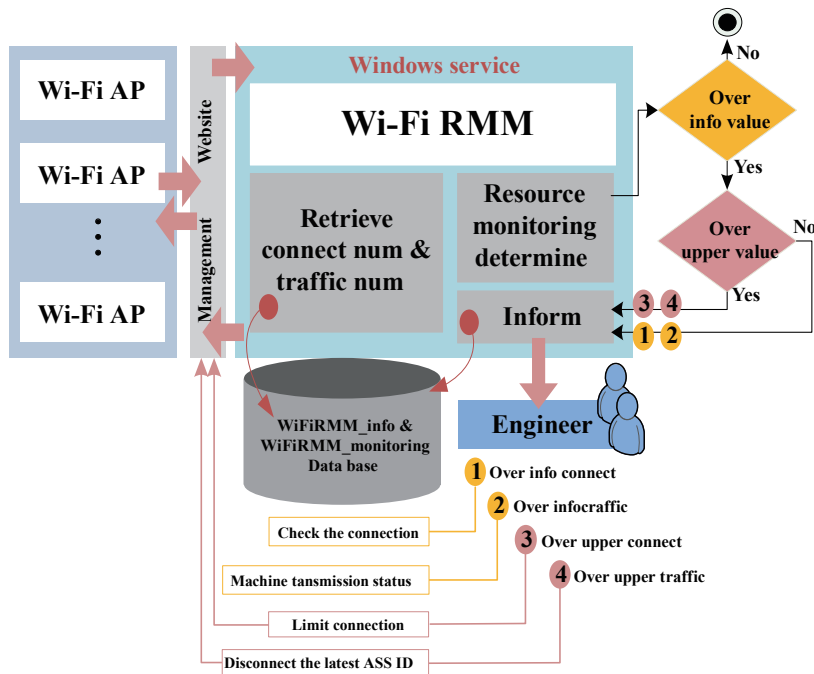


Fig. 1. (Color online) Wi-Fi RMM operational flow diagram.

Wi-Fi RMM will automatically collect the number of connections to and network traffic of each Wi-Fi AP regularly. When the number exceeds a predetermined threshold, engineers will be automatically warned about the connection number. When the number reaches a predetermined threshold, it will reject access to the network through this AP. When network traffic exceeds a predetermined threshold, engineers will be automatically warned and will be needed to check the transmission of each machine. When network traffic reaches a predetermined threshold, engineers will be warned to restrict the IP connections of lower priority by Association ID (ASS ID) because these are nonessential IPs for mobile devices held by factory users. This Wi-Fi RMM runs as a Windows resident service continuously on the system to monitor individual Wi-Fi AP network resource load. Its virtual program code is shown in Table 4.

## 5. Experimental Results and Discussion

### 5.1 Factory machine Wi-Fi node deployment

In this study, we employ an industrial-level Wi-Fi module, with a transmission distance of up to 100 m and a distance of 200–500 m between factories. The bridge between APs and their dynamic host configuration protocol (DHCP) feature enable automatic assignment of IP addresses to the clients that log in TCP/IP networks to allow

central APs to distribute IPs to other bridge APs and then to factory APs, and finally allow factory APs to redistribute IP addresses to the machine Wi-Fi node. The DHCP IP assignment simulation is shown in Table 5.

### 5.2 Wi-Fi RMM implementation

Wi-Fi RMM in this study is developed in the Windows Service mode, which is executed in the Windows session of the application. Service can start automatically when the computer starts, pauses, or restarts, without passing through any user interface. Service can also run in the security context of a specific user account that differs from the logged-in user or default computer account. When the number of connections or traffic exceeds the warning threshold, it will automatically deliver a warning message to factory engineers, as shown in Fig. 2.

Table 4  
Wi-Fi RMM program pseudocode.

---

**denotes** *ConnectNum*, *TrafficNum* initial value is **0**  
**denotes** *Info*, *OverLoad* initial value is **false**  
**if** (*ConnectNum*>*InfoConnect* **or** *TrafficNum*>*InfoTraffic*)  
**then** set *Info* as **true**  
**else if** (*ConnectNum*>*UpperConnect* **or** *TrafficNum*>*UpperTraffic*) **then** set *OverLoad* as **true**

---

**OverLoad:** Record whether the traffic/connection number is overloaded, type Boolean  
**ConnectNum:** Record the current number of connections through this AP  
**TrafficNum:** Record the current AP flow number  
**InfoConnect:** Warning connection number  
**InfoTraffic:** Warning traffic number  
**UpperConnect:** Upper connection number  
**UpperTraffic:** Upper traffic number

---

Table 5  
AP DHCP IP assignment simulation.

AP Name	IP	Description
Center AP	192.168.1.1 192.168.2.1	Central Aps
Bridge AP	192.168.3.1 192.168.4.1	Bridge APs to extend the wireless network range
Factory AP	192.168.2.2 192.168.3.2 192.168.4.2	Factory DHCP APs, responsible for distributing IPs to other zone APs
Zone AP	192.168.2.3-254 192.168.3.3-254 192.168.4.3-254	Zone APs, responsible for distributing IPs to machines and mobile devices

### 5.3 Wi-Fi deployment verification

The Wi-Fi module specifications and functions for this study are shown in Table 6. Xirrus Wi-Fi Inspector is used in this study for Wi-Fi deployment architecture signal strength, network quality, and connection testing. The data of distance and obstruction tests in this study are shown in Table 7. The experimental data show that obstacles with cement walls and metal doors have significant interference with the Wi-Fi signal; hence, in this study, we deploy Wi-Fi APs approximately one storey high on factory beams to avoid factory metal frames and machines, and reduce signal interference caused by them. The actual tests show that the m-CMIS network speed may be up to 52 Mbps, Ping 63 ms, and the network quality may reach Grade B (no packet loss).



Fig. 2. (Color online) m-CMIS Wi-Fi RMM warning message.

Table 6 (Color online)  
Wi-Fi module specifications and functions.



Wi-Fi AP		Device specification	Compatibility standard	IEEE802.11 a/b/g/n
			Transmission rate	300 Mbps
			Encryption type	TKIP, AES
			Support protocol	IPv4, TCP, UDP, DHCP Client, SNMP, SMTP, HTTP, DNS, RADIUS, RFC2217, WPS
		Feature	Can be an AP, WDS bridge and AP client	
		Function	Wi-Fi AP is used for connecting and bridging Wi-Fi nodes, deployed in the factory over wireless network.	
Wi-Fi node		Device specification	Compatibility standard	IEEE802.11 a/b/g/n
			Transmission rate	300 Mbps
			Encryption type	TKIP, AES
			Support protocol	IPv4, TCP, UDP, DHCP client, SNMP, SMTP, HTTP, DNS, RADIUS, WDS, WPS
		Feature	Serial transmission function	
		Function	The Wi-Fi node is used for connecting to injection machines via the Ethernet cable (RJ-45), bridging the Wi-Fi APs over a wireless network.	



Table 7  
Wi-Fi signal test.

Distance	Environment	Signal strength	Online test
10 m	No obstacles	-57 dBm	Pass
20 m	No obstacles	-62 dBm	Pass
28 m	No obstacles	-75 dBm	Pass
35 m	Cement walls	-88 dBm	Pass
	Metal doors		
0 m	One floor	-71 dBm	Pass
10 m	One floor	-79 dBm	Pass
28 m	One floor	-85 dBm	Pass

## 6. Conclusions

In this study, we propose the deployment and implementation of a wireless networking architecture for factory machines based on Wi-Fi technology. Through Wi-Fi RMM and Wi-Fi machine wireless network deployment and implementation, engineers may monitor the wireless network in the factory and can be automatically warned when the flow and connection number reach the threshold, without data transmission delay. The experimental results demonstrate that the factory Wi-Fi deployment architecture proposed in this study is stable for data transmission and the results are remarkable. Two considerations for future researchers to discuss for factory Wi-Fi module deployment are also addressed in this paper. First, the factory environment should be considered. Many barriers in the factory will interfere with Wi-Fi radio signals; therefore, ceilings, beams, and stands will be considered as the position for AP deployment to reduce ground interference. Second, machine data backhaul traffic should be properly estimated. Production data will continue to return through the network connection to the server in machine production. When multiple machines return data simultaneously, it may cause a large amount of traffic, hence, the need for backhaul traffic monitoring to ensure transmission stability. The obtained data can be further used to perform tool or process scheduling or even optimization.<sup>(15)</sup>

## Acknowledgements

We are grateful to the Ministry of Science and Technology (Grant no. 103-2221-E-006-085) for funding and supporting this study.

## References

- 1 National Development Council: Homepage of National Development Council, <http://www.ndc.gov.tw/> (accessed October 2013).
- 2 Y. Y. Chen, S. L. Chen, Y. H. Hsiao and S. R. Wang: Adv. Mech. Eng. Article ID 516061 (2013).

- 3 S. L. Chen, S. R. Wang and Y. Y. Chen: Conf. Precis. Mach. Manuf. Technol. (PMMT, Taiwan, 2014) (in Chinese).
- 4 A. Mahanti, C. Williamson, M. Arlitt and A. Mahantit: 32nd IEEE Conf. Local Comput. Networks (IEEE, Dublin, 2007) pp. 901–910.
- 5 M. Jung, N. B. Karayiannis and S. Pei: Int. Conf. Networking Serv. (IEEE, Washington, 2006) pp. 20–20.
- 6 X. L. Zhang, Y. Kun, Y. Jin and L. Jian: Int. Conf. Comput. Sci. Network Technol. (IEEE, Changchun, 2012) pp. 221–224.
- 7 Q. Ruan, W. Xu and G. Wang: Electr. Inf. Control Eng. (IEEE, Wuhan, 2011) pp. 1672–1675.
- 8 L. Lusheng, B. Feldman and J. Arge: Aerosp. Conf. (IEEE, Montana, 2004) pp. 1231–1240.
- 9 K. Jaeseok, Y. Liuqing, L. Jenshan and J. Liu: Radio Wireless Symp. (IEEE, San Diego, 2006) pp. 319–322.
- 10 K. Gancarz and K. Prole: IEEE Conf. Technol. Homeland Secur. (IEEE, Waltham, 2012) pp. 341–347.
- 11 P.K. Tiwary, N. Maskey, S. Khakurel and G. Sachdeva: Int. Conf. Adv. Recent Technol. Commun. Comput. (IEEE, Kottayam, 2010) pp. 158–160.
- 12 C. Wei, Y. Zhang and W. Yuanchun: 14th IEEE Int. Conf. Parallel Distrib. Syst. (IEEE, Melbourne, 2008) pp. 517–524.
- 13 J. Seitz, T. Vaupel, S. Haimerl, S. Meyer, J. Gutierrez Boronat, G. Rohmer and J. Thielecke: Wi-Fi Attitude and Position Tracking, eds. A. Heuberger, G. Elst and R. Hanke (Springer, Berlin, 2011) pp. 173–185.
- 14 S. L. Chen, S. R. Wang, Y. C. Lin and Y. Y. Chen: to be published in Appl. Mech. Mater.
- 15 X. Wenbin, H. Chris and P. Pupong: Int. J. Eng. Technol. Innov. **4** (2014) 18.