WIRELESS COMMUNICATIONS AND MOBILE COMPUTING
Wirel. Commun. Mob. Comput. 2011; **11**:1197–1212
Published online 4 May 2010 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/wcm.976

SPECIAL ISSUE PAPER

Survey and experiments of WIA-PA specification of industrial wireless network

Wei Liang[1], Xiaoling Zhang[1,2], Yang Xiao[3]*, Fuqiang Wang[1], Peng Zeng[1] and Haibin Yu[1]

[1] Shenyang Institute of Automation, Chinese Academy of Sciences, Shenyang 110016, P.R. China
[2] Graduate School of the Chinese Academy of Sciences, Beijing 100049, P.R. China
[3] Department of Computer Science, The University of Alabama, Tuscaloosa, AL 35487-0290, USA

ABSTRACT

Wireless process control has been a popular topic recently in the field of industrial control. In the industrial field, wireless technologies are considered despite the lack of an ideal industrial wireless standard. However, application development of industrial wireless networks is slow due to the lack of an ideal standard. Open standards are the foundation of industrial wireless application extensions. This paper first summarizes a standardized process for industrial wireless network technologies and then introduces network composition, network topology, protocol stack architecture, and some key protocol technologies of WIA-PA, which is an international specification of industrial wireless networks for process automation. Furthermore, a comparison between WIA-PA and other main industrial wireless network specifications like WirelessHART and ISA100.11a is provided. Architecture and key technologies of a WIA-PA are also introduced. Our first-hand experiences in developing WIA-PA testbed based on the modularization method are given. Finally, experiment results illustrate the performance and efficiency of WIA-PA. Copyright © 2010 John Wiley & Sons, Ltd.

KEYWORDS

architecture; communication standards; industrial plants; protocols

***Correspondence**

Yang Xiao, Department of Computer Science, The University of Alabama, Tuscaloosa, AL 35487-0290, USA.
E-mail: yangxiao@ieee.org

1. STANDARDIZATION OF INDUSTRIAL WIRELESS NETWORK

An industrial wireless network is a revolutionary technology for reducing costs and expanding the application scope of industrial measurement and control systems [1–2]. In the field of industrial control, the industrial wireless network has become another hot spot after field bus, which has changed the information delivery of existing control systems. Wireless communication technology makes measurement and control systems to be low cost, easy to use and maintain, and has more broad potential applications. However, specific requirements of industrial measurement and control applications bring some new challenges to wireless networks, specifically regarding the more strict and deterministic performance of real-time and reliability, the dynamic adaptability of the environment, low cost, and low power consumption [3,4].

A key problem hindering the acceptance of the industrial wireless network is the lack of a mature and unified international standard. Recently, some international organizations have been actively promoting the standardized process of industrial wireless network and have achieved several productions, such as WirelessHART [5–17], ISA100.11a, [18] and the Wireless network for Industrial Automation–Process Automation (WIA-PA) [19–21].

WirelessHART is a specification of the industrial wireless network, which is formulated by HART Communication Foundation (HCF). In 2004, HCF announced the beginning of the WirelessHART standard and set up a wireless work group. WirelessHART specification and communication protocols were formally passed by members of HCF in June, 2007. Now, WirelessHART has become a Public Available Specification (PAS) of IEC via IEC voting on October 19, 2008 with number IEC/PAS 62591.

ISA100.11a is a standard draft of industrial wireless measurement and control systems proposed by the United States Institute of Instrumentation, Systems, and Automation Society. In December 2004, the United States Institute of Instrumentation, Systems, and Automation Association set up the ISA100 group of the industrial wireless standard and initiated the standardization process of industrial wireless

technologies. Currently, ISA100.11 and ISA100.14, which are two sub-groups of the ISA100 committee, have ended their proposal collection process.

WIA-PA is a kind of system architecture and communication protocol of wireless networks for industrial process automation that was first developed by the Chinese Industrial Wireless Alliance (CIWA) under the urgent requirements of process automation. In 2007, CIWA was established by Shenyang Institute of Automation as a leader (all of the co-authors of this paper were involved), along with more than 10 universities, academies, and companies. WIA-PA became a Public Available Specification (PAS) of IEC via IEC voting on October 31, 2008 with number IEC/PAS 62601. Now, WIA-PA has become a draft of the Chinese national standard.

WIA-PA adopts characteristic schemes, such as two-stage communication resource allocation, adaptive frequency hopping, and two-level packet aggregation to solve some special problems of industrial process applications.

In this paper, we first provide a survey for WIA-PA, then compare it with two other industrial wireless specifications, and finally provide some of our experiments for WIA-PA.

The rest of the paper is organized as follows. Section 2 introduces the WIA-PA standard architecture and its key technologies. Section 3 describes the architecture of the WIA-PA network. The comparison and analyses of WIA-PA, WirelessHART, and ISA100.11a standards are provided in Section 4. A realization of the WIA-PA testbed is presented in Section 5. Some physical experiments on the WIA-PA are illustrated in Section 6. Finally, we conclude the paper in Section 7.

2. WIA-PA STANDARD

2.1. Network composition

WIA-PA specifies five types of physical devices:

- *Host computer*: An interface through which users and maintenance/management personnel perform transactions to the WIA-PA network and the management networks.
- *Gateway device (GW)*: A device connecting the WIA-PA network and other plant networks with the functions of protocol translation and data mapping.
- *Routing device*: A device forwarding packets from one network device to another in the WIA-PA network.
- *Field device*: A device installed in the industrial field, which is connected to or controls processes such as sensors, actuators, etc.
- *Handheld device*: A portable device that is responsible for configuring network devices and monitoring network performance.

WIA-PA also specifies two types of uppermost logical devices:

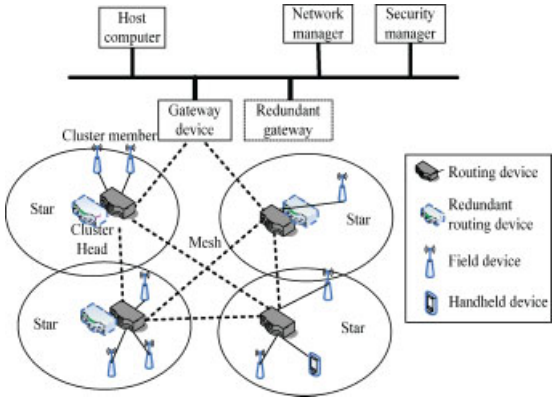

Figure 1. Topology of WIA-PA, which is a typical topology used in the WIA-PA network.

- *Network manager (NM)*: Responsible for configuring the network, scheduling communication between routing devices, managing the routing table, and monitoring the performance of the whole network.
- *Security manager (SM)*: Responsible for configuring the security mechanism, managing the security key, and authenticating routing devices and field devices.

2.2. Network topology

As illustrated in Figure 1, a WIA-PA network supports a hybrid star and mesh hierarchical network topology.

The first level of the network is in mesh topology where routing devices and gateway devices are deployed. The network manager and the security manager can be realized on the gateway device or the host computer.

The second level of the network is in star topology, which is called a cluster where routing devices and field/handheld devices are deployed. The routing devices in the WIA-PA network act as cluster heads, and the field devices act as cluster members.

2.3. Protocol stack

The WIA-PA protocol stack is based on the ISO/OSI 7-layer reference model and only defines the Data Link Sub-Layer (DLSL), Network Layer (NL), and Application Layer (AL). Its physical layer and MAC layer are based on IEEE 802.15.4 [22–34], which is illustrated in Figure 2. The AL includes the User Application Process (UAP), the Device Management Application Process (DMAP), and the Application Sub-layer. The UAP is made up of User Application Objects (UAOs). The DMAP is responsible for management of the network, security, and Management Information Base (MIB).

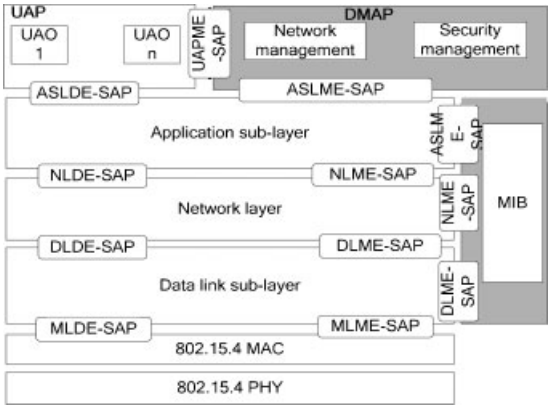

Figure 2. WIA-PA protocol stack. WIA-PA is based on IEEE 802.15.4 physical layer and MAC layer, and defines data link sub-layer, network layer, and application layer.

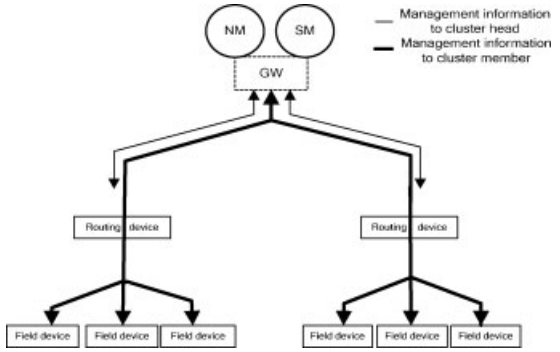

Figure 3. Centralized system management scheme, the NM, SM, and GW are the abbreviations of network manager, security manager, and gateway device.

2.4. Key technologies

2.4.1. Hybrid centralized and distributed management scheme.

The WIA-PA network employs both centralized and distributed management schemes to complete network management and security management. As illustrated in Figure 3, system management is centrally implemented by the network manager (NM) and the security manager (SM). Routing devices and field devices are managed directly by the NM and the SM. When a field device is managed by the NM and the SM directly, the routing device shall only relay the management information originated from the NM and the SM, and shall not act as a cluster head.

The distributed management framework is illustrated in Figure 4. The system management is implemented by the NM, the SM, and the cluster heads. The routing devices are directly managed by the NM and the SM, and are used in the management of field devices. The routing devices, serving as cluster heads, implement the tasks of an agent of the NM and the SM.

The NM is responsible for the following three tasks: (1) constructing and maintaining the mesh topology, (2) allocating communication resources for routing devices in a mesh topology and pre-allocating communication resources for field devices by the routing devices in a star topology, and (3) monitoring the performance of the WIA-PA network, including device status, path health, and channel condition.

The SM is responsible for the following three tasks: (1) authorizing the routing devices and field devices that are

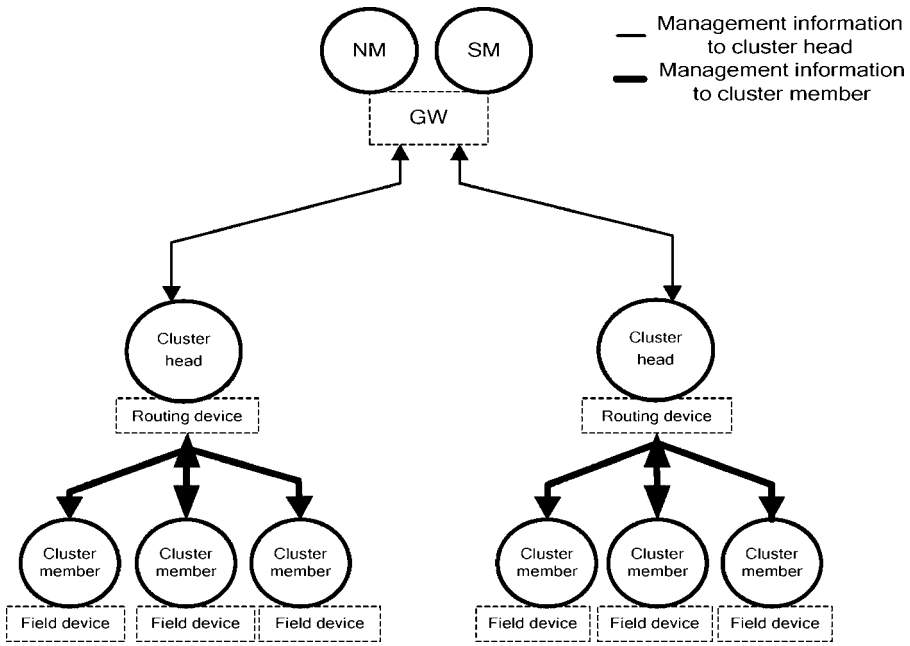

Figure 4. Distributed system management scheme, the NM, SM, and GW are the abbreviations of network manager, security manager, and gateway device.

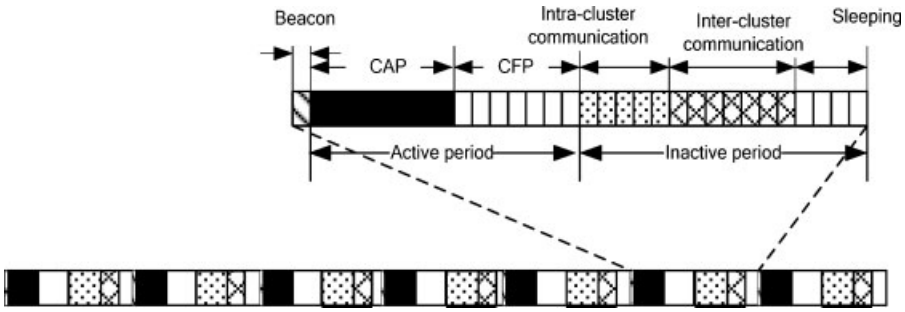

Figure 5. WIA-PA superframe. It is based on the beacon-enabled IEEE 802.15.4 superframe.

attempting to join in the WIA-PA network, (2) managing keys in the whole network, including key generation, key distribution, key recovery, and key revocation, etc., and (3) authorizing the relationship of end-to-end communication.

The cluster head is responsible for the following two tasks:

- As an agent of the NM: constructing and maintaining the star topology constructed by a routing device and field devices; allocating communication resources to field devices in the cluster, which is allocated to star topology by the NM; and providing the monitoring results of the star topology to the NM.
- As an agent of the SM: managing keys used in star topology; authorizing the communication relationship among routing devices; and authorizing the communication relationship between a routing device and field devices.

In summary, authorization of joining devices and performance monitoring are implemented by the NM and the SM in a centralized scheme. The other management tasks are implemented by the NM, the SM, and the cluster heads in a distributed scheme.

2.4.2. Superframe structure.

The WIA-PA specification only takes into account the beacon-enabled IEEE 802.15.4 superframe structure. The WIA-PA superframe structure is shown in Figure 5.

- Contention Access Period (CAP), as defined in the IEEE 802.15.4 superframe, is used for device joining, intra-cluster management, and retry in a WIA-PA superframe;
- Contention Free Period (CFP), as defined in the IEEE 802.15.4 superframe, is used for communication between mobile devices and the cluster head in a WIA-PA superframe; and
- An inactive period, as defined in the IEEE 802.15.4 superframe, is used for intra-cluster communication, inter-cluster communication, and sleeping in the WIA-PA superframe.

2.4.3. Multi-access and adaptive frequency hopping.

The multi-address access and adaptive frequency hopping mechanisms are listed in Table I.

The WIA-PA network supports the following multi-address access mechanisms:

- Intra-superframe: Beacon, CFP, intra- and inter-cluster communication periods use the Time Division Multiple Access (TDMA) mechanism. CAP uses the Carrier Sense Multiple Access (CSMA) mechanism.
- Inter-superframe: Different routing devices use different channels in the Active period by adopting the Frequency Division Multiple Access (FDMA) mechanism. If there are not enough channels, the WIA-PA network uses the TDMA mechanism to enhance the system capacity. Suppose that three routing devices,

Table I. Hopping mechanisms.

IEEE 802.15.4	WIA-PA	Basic MAC mechanism		DLSL hopping mechanism
Beacon	Beacon	TDMA	FDMA	AFS
CAP	CAP	CSMA		
CFP	CFP	TDMA		
Inactive	Intra-cluster period	TDMA		AFH
	Inter-cluster period	TDMA		TH
	Sleeping	--		--

This table is used to summarize the multi-access mechanisms and frequency hopping mechanisms of WIA-PA standard.

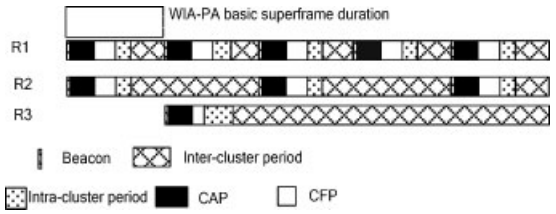

Figure 6. R1, R2, and R3 superframe structures, using mixed TDMA and FDMA mechanisms.

labeled R1, R2, and R3, are in the WIA-PA network. The superframe lengths of R1, R2, and R3 are respectively one, two, and four WIA-PA basic superframe duration(s), as shown in Figure 6. According to the superframe definition, the R1's active period cannot be multiplexed with the R2 and R3's active periods, while the active periods of R2 and R3 can be multiplexed with each other. The R1' active period must use a different channel than the active periods of R2 and R3, while the active periods of R2 and R3 can use the same channel.

The WIA-PA network supports three frequency hopping mechanisms:

- Adaptive Frequency Switch (AFS): In the WIA superframe, Beacon, CAP, and CFP use the same channel in the same superframe cycle and change the channel according to the channel condition in the different superframe cycle.
- Adaptive Frequency Hopping (AFH): In the WIA superframe, the Intra-cluster period irregularly changes communication channels per timeslot according to the actual channel condition.
- Timeslot Hopping (TH): In the WIA superframe, the Inter-cluster period regularly changes the transmit/receive frequency per timeslot to combat interference and fading.

2.4.4. Packet aggregation and disaggregation.

The WIA-PA network supports a two-level packet aggregation mechanism in order to reduce the number of the forwarding packets.

- *Data aggregation*: If a field device has more than one UAO, it chooses to invoke a data aggregation mechanism according to its aggregation flag. This mechanism will reduce communication frequency and enhance network efficiency.
- *Packet aggregation*: If a routing device receives packets from more than one field device, it chooses to invoke the packet aggregation mechanism according to its aggregation flag. This mechanism will reduce the number of packets from the routing device to the gateway device and enhance network efficiency.

The aggregation function is implemented by the Data AGgregation Objects (DAGOs) in field devices and by the Packet AGgregation Objects (PAGOs) in routing devices. The operation parameters of DAGOs and PAGOs are configured by the aggregation management object in the NM.

The packet aggregation mechanism supported by the WIA-PA network includes the following four situations:

- A field device supports the packet aggregation mechanism, while its routing device does not.
- A routing device supports the packet aggregation mechanism, while its field device does not.
- Both a field device and its routing device support the packet aggregation mechanism.
- Neither a field device nor its routing device supports the packet aggregation mechanism.

Disaggregation is carried out by a DisaGgregation Object (DGO) of GW.

3. COMPARISONS AMONG WIA-PA, WIRELESSHART, AND ISA100.11A

WIA-PA, WirelessHART, and ISA100.11a are three apposite and mainstream standards of industrial wireless network. We compare them with the five aspects listed in Table II: architecture, system management, communication technologies, networking technologies, and application technologies.

3.1. Comparisons of architecture

3.1.1. Network composition.

The WIA-PA specification specifies the following five types of physical devices: the host computer, gateway device, routing device, field device, and handheld device. The WirelessHART specification defines three: the network manager, gateway, and field device. The ISA100.11a specification comprises two kinds of devices: the field device and infrastructure device. In an ISA100.11a network, the field devices are divided into devices without routing capability, routing devices, and handheld devices. The infrastructure devices are divided into the gateway, backbone router, system manager, and security manager in local.

3.1.2. Protocol stack.

The WIA-PA specification is based on the physical layer and the MAC layer of IEEE 802.15.4 and defines the data link sub-layer, the network layer, and the application layer. The WrelessHART and ISA100.11a specifications are based on the physical layer of IEEE 802.15.4 and define the data link, network, transport, and application layers.

Table II. Comparisons among WIA-PA, WirelessHART, and ISA100.11A.

	Comparison	WIA-PA	WirelessHART	ISA100.11a
Architecture	Network composition	Host computer, gateway device, routing device, field device, and handheld device	Network manager, gateway and field device	Field device and infrastructure device
	Protocol stack	IEEE802.15.4 physical layer and MAC layer; DLSL, network, and application layer	IEEE802.15.4 physical layer; defining DLL, network, transport, and application layer	IEEE802.15.4 physical layer; DLL, network, transport, and application layer
System management	System management scheme	Hybrid centralized and distributed	Centralized	Centralized; distributed discussed, but not specified
	Single point of failure of the system manager	No, redundancy allowed	No, redundancy allowed	No, redundancy allowed
	Manager address Assignment	Fixed assignment	Fixed assignment	Dynamically assigned
	Packet aggregation function	Two-level aggregation	Not supporting	Field device aggregation
	Security	DLL and application layer; optional; symmetric and asymmetric keys	DLL and transport layer. symmetric key	DLL and network layer; optional; symmetric and public (128-bit)
	Time measurement	UTC TAI (alternative)	Time measured in absolute slot counts that is translated to UTC	Time is measured using International Atomic Time (TAI)
	Timeslot durations	All slots are 10 ms	All slots are 10 ms	Flexible: one duration per network
	Time standard	All nodes align to UTC/TAI time	ASN to UTC conversion all nodes align to UTC	All nodes align to TAI time
Communication technologies	IEEE802.15.4 compatibility	Physical layer and MAC layer	Physical layer	Physical layer
	Superframe structure	Based on IEEE802.15.4 superframe structure	No structure	No structure
	Multi-access mechanism	Mixed CSMA, TDMA, and FDMA	Mixed TDMA and CSMA	Mixed TDMA and CSMA
	Frequency hopping	AFH, AFS, and TH	Channel hopping	Slow hopping, fast hopping, and mixed hopping
Networking technologies	Network topology	Hybrid mesh and star	Mesh or star (star is not recommended)	Mesh
	Routing function	Field device have no routing function	All devices have routing function	Field device have no routing function
	Routing technology	Static redundant routing	Source, graph, hybrid source/graph and superframe	Source, graph, and hybrid source/graph
	Fragmentation and reassembly	Network layer	Network and application layers	Application layer
	Device joining pattern	Distinguishing joining pattern between field device and routing device	Not distinguishing	Not distinguishing
	Device leaving pattern	Active leaving and passive leaving	Not distinguishing	Not distinguishing
Application technologies	Support for legacy protocols	Wired/Wireless HART, Profibus, Modbus, and FF; Virtual device	Wired HART EDDL	Wired/Wireless HART, Profibus, Modbus, and FF; Informative material on adapters and tunneling protocols
	Multiple application protocols	Yes, Gateway side	No	Yes, Gateway side
	Application definition	Object-oriented (UAO), simple	Commands	Object-oriented (UFO), complex
	Alert function	Report method	Command	Alter object
	Communication between application Objects	VCR	Not support	Parameter of UFO

This table contains the comparisons among three industrial wireless standards: WIA-PA, WirelssHART, and ISA100.11a.

3.2. Comparisons of system management

3.2.1. System management scheme.

WIA-PA supports hybrid distributed and centralized management. The network manager in the WIA-PA manages the whole network in a centralized way and authorizes parts of the management function to routing devices that manage field devices in clusters. WirelessHART supports centralized management only, in which the network manager manages the whole network. ISA100.11a supports either centralized or distributed management, and the distributed management is discussed but not specified.

3.2.2. Network manager.

There is no single point of failure of the network manager in WIA-PA, WirelessHART, and ISA100.11a. The address of the system manager is dynamically assigned for ISA100.11a and is a fixed assignment for WirelessHART and WIA-PA.

3.2.3. Aggregation function.

WIA-PA supports two-level aggregation in order to reduce the number packet, including data aggregation and packet aggregation. ISA100.11a only supports field device aggregation via concentrator object. WirelessHART does not support this function.

3.2.4. Security.

WIA-PA realizes the point-to-point communication security in the data link layer and end-to-end security in the application layer. The security function of WirelessHART is realized in both the data link layer and the transport layer. The security function of ISA100.11a is realized in both the data link layer and the network layer.

3.2.5. Time.

TAI time is the time standard of ISA100.11a. All nodes in a WirelessHART network align to UTC through ASN to UTC conversion. UTC is the time standard of WIA-PA and TAI time is the alternative time standard of WIA-PA. ISA100.11a has a settable timeslot period. The timeslot in WirelessHART and WIA-PA is fixed for IEEE802.15.4 PHY. The optimal timeslot duration for the IEEE802.15.4, 2.4 GHz radio is 10 ms.

3.3. Comparisons of communication technologies

3.3.1. IEEE 802.15.4 compatibility.

WIA-PA is fully compatible with the IEEE 802.15.4 standard, and WirelessHART and ISA100.11a are only based on the IEEE 802.15.4 physical layer in the strict sense.

3.3.2. Superframe structure.

WIA-PA uses the beacon-enable IEEE 802.15.4 superframe, and extends it. WirelessHART and ISA100.11a have no superframe structures. Their superframes are comprised of timeslots and do not divide the superframe structure according to the functions of the timeslots.

3.3.3. Multi-access mechanisms.

Three standards adopt timeslots for communication and mixed access technology of TDMA and CSMA. Besides, WIA-PA also supports hybrid FDMA and TDMA mechanisms among superframes in order to increase network capability and reliability. Collision based access is only an option of ISA100.11a, and CSMA timeslots of ISA100.11a are not fixed. Timeslots of WirelessHART can be configured for CSMA.

3.3.4. Frequency hopping technology.

WIA-PA adopts three kinds of frequency hopping technologies: AFH, AFS, and TH. AFH and AFS of WIA-PA change the channel according to the channel condition. ISA100.11a supports three kinds of frequency hopping technologies: slow frequency hopping, fast frequency hopping, and mixed frequency hopping. WirelessHART supports channel hopping. However, frequency hopping mechanisms of WirelessHART and ISA100.11a have blindness causing them to lack the feedback and process of the real-time channel quality.

3.4. Comparisons of networking technologies

3.4.1. Network topology.

WIA-PA supports hybrid mesh and star topology. WirelessHART supports either mesh or star topology, but the star topology is not recommended. ISA100.11a supports multiple kinds of topologies, i.e., star, hub-and-spoke, mesh, star-mesh, and combined topology.

3.4.2. Routing function.

Devices in the WIA-PA network and the ISA100.11a network are divided into routing devices with routing function and field devices without routing function. All devices of WirelessHART have routing function. WirelessHART has no reduced-function devices.

3.4.3. Routing technology.

All of these standards support redundant routing in order to enhance reliability. WIA-PA supports all static routing algorithms. Meanwhile, it also supports health monitoring of the paths. When a path is interrupted, WIA-PA devices can automatically switch to other channels that have good quality. WirelessHART supports source routing, graph routing, hybrid source/graph routing, and superframe routing.

ISA100.11a supports source routing, graph routing, and hybrid source/graph routing.

3.4.4. Device joining pattern.

The WIA-PA network simplifies the processes of device joining and communication resource allocation according to device types. WirelessHART and ISA100.11a networks do not distinguish the joining process according to device types.

3.4.5. Device leaving pattern.

The WIA-PA network designs the active leaving process and the passive leaving process. WirelessHART and ISA100.11a do not distinguish the leaving process and have no concepts of active leaving and passive leaving.

3.5. Comparisons of application technologies

3.5.1. Legacy protocol support.

WirelessHART is only compatible with Wired HART and EDDL. WIA-PA and ISA100.11a are compatible with Profibus, FF, Modbus, and Wired/WirelessHART. ISA100.11a supports multiple legacy protocols through informative material on adapters and tunneling protocols, and WIA-PA does this through a virtual device.

3.5.2. Fragmentation and reassembly.

Fragmentation and Reassembly are implemented in the network layer of WIA-PA, the application layer of WirelessHART, and the network and application layers of ISA100.11a.

3.5.3. Application definition.

The user applications of WirelessHART are realized by using the HART commands. The user applications of WIA-PA and ISA100.11a are realized by using the object-oriented methods. The user application objects of WIA-PA are simple, while the user application objects of ISA100.11a are complex and have functions of mode switching.

3.5.4. Alarm function.

The WIA-PA alarm function is carried out by the report method directly. The WirelessHART alarm function is finished by alarm commands. The ISA100.11a alarm function is implemented by the alarm object.

3.5.5. Communication between application objects.

WIA-PA defines the communication relations between UAOs through VCR. ISA100.11a denotes communication relations between Unified Field Objects (UFOs) through parameters of UFOs. WirelessHART has no object definition, does not support communication between objects, and adopts a master–slave communication manner.

4. MODULARIZATION DESIGN OF WIA-PA TESTBED

4.1. Modularization design method for WIA-PA testbed

As shown in Figure 2, a WIA-PA network device has the DLSL, NL, AL, and DMAP besides the IEEE802.15.4 PHY and MAC, and most of the network services are realized in the DMAP. In the design process of the WIA-PA testbed, the designing and realizing issues of the WIA-PA DMAP are difficult because of its multiple function modules. In this paper, we adopt the modularization method to overcome these problems.

The DMAP is the kernel of the WIA-PA network device, and it includes a network initialization module, a device registration module, a routing management module, a communication resource management module, a device maintenance module, and a security management module.

4.1.1. Network initialization module.

The *Network Initialization Module* is responsible for the self-initializing of the NM, generating related communication resources, and establishing a connection with the SM. This module in the NM is also responsible for initializing the gateway device and allocating a superframe, link, and short address for the gateway device.

4.1.2. Device registration module.

When a new device joins the WIA-PA network, the *Device Registration Module* is responsible for authenticating it and allocating a short address, communication resources, and routes for the legal device. When a device leaves the WIA-PA network, this module is responsible for updating the routing table and recycling communication resources. In order to simplify the management of device information, the NM maintains a device state table, which is used to track the joining and leaving processes. This module has a complex state machine due to its complicated function and structure. This module represents the focus and difficulty of the design process.

4.1.3. Routing management module.

The *Routing Management Module* is responsible for collecting neighbor information, constructing network topology, and choosing multiple optimal routes according to packet loss rate, radio signal intensity, and residual energy, which are used for transmitting the uplink/downlink management packet and the uplink data packet. In order to

guarantee reliability, there should be more than two routes for packet transmission.

4.1.4. Communication resource management module.

The *Communication Resource Management Module* is responsible for allocating communication resources and avoiding packet collision according to the routing information calculated by the routing management module. The superframe length of a routing device is decided by the data update rates in a cluster.

4.1.5. Device maintenance module.

The *Device Maintenance Module* is responsible for monitoring the device state. If a device is off-line or its routes fail, this module is started up and reports the abnormal information to the NM. The NM makes some adjustment or update and notifies users the abnormal information.

4.1.6. Security management module.

The *Security Management Module* is responsible for interacting with the SM and verifying the new device.

4.2. Main modules design

The device joining process is the most difficult procedure in the WIA-PA network and involves many function modules. Therefore, this paper discusses the design method through an example of the device joining process.

4.2.1. Main data structures of joining process.

- DEVICE_INFO structure is used to store device information. The device information will be inserted into the device table when a device is verified successfully, and the device information will be deleted from the device table after a device leaves the WIA-PA network.

```
typedef struct _DEVICE_INFO
{
LONG_ADDR                DevInfoID;//Long address
USIGN16                  uNickName;//Short address
USIGN8                   ucUpdateRate;//Data update rate
USIGN8                   JoinKey[25];//Join key
USIGN8                   ucDevState;//Current state
USIGN8                   ucJoiningState;//Sub-state during
                         joining process
vector<USIGN8>           LinkID;//Link ID
vector<USIGN16>          SuperFrmID;//Superframe ID
NB_ENTRY*                NBTable;//Neighbor table
struct _DEVICE_INFO*     pNext;//List pointer
}DEVICE_INFO;//Device
information
```

- DEVICE_RES-INFO structure is used to store routes and communication resources allocated by the NM.

```
typedef struct _DEVICE_RES_INFO
{
USIGN8                   ucFrameID;//Superframe ID
USIGN8                   ucLinkOpt;//Link option
USIGN8                   ucLinkTyp;//Link type
USIGN16                  uLinkID;//Link ID
USIGN16                  uSlot;//Timeslot number
USIGN16                  uOffSet;//Channel offset
USIGN16                  uNBShortAddr;//Neighbor
                         short address
USIGN16                  uSrcShortAddr;//Source
                         address
USIGN16                  uDestShortAddr;//Destination
                         address
}DEV_RES_INFO; // Device
resource allocation table
```

4.2.2. Main functions and calling relations during joining process.

- Initialization function*void InitialManager(void)*: Used to initialize the NM and establish related communication resources.*void InitialGateWay(USIGN16 uNickName)*: Used to initialize the gateway device and allocate the related short address and communication resources.
- Security related function*AuthenJoinKey()*: Verifies the legality of the join key.
- Address allocation function*AllocShortAddr()*: Allocates short addresses for network devices.
- Routing function*USIGN8 CountRoute (USIGN16 uSrcAddr, USIGN16 uDestAddr, USIGN8 ucPathNum)*: Belong to the routing management module. This function is used to calculate the optimal routes from source to destination according to hops, signal strength, and residual power.
- Communication resource allocation function

USIGN8 AllocRes (USIGN8 ucFrameTyp, USIGN16 uDestAddr, USIGN16 uSFRLen): Belong to the communication resource management module. This function is used to call the communication resource allocation algorithm to allocate channels and timeslots for devices according to the device address and superframe length. This function is the kernel function for the WIA-PA network.

The joining process and function calling relations of a routing device are illustrated in Figure 7. The joining process and function calling relations of a field device are illustrated in Figure 8. At the beginning of the networking, the NM and the gateway device should be initialized first. The NM calls *InitialManager()* to initialize itself, and the gateway device calls *InitialGateWay()* to initialize itself. The gateway device broadcasts its Beacon frame after initializing in order to allow network devices to join

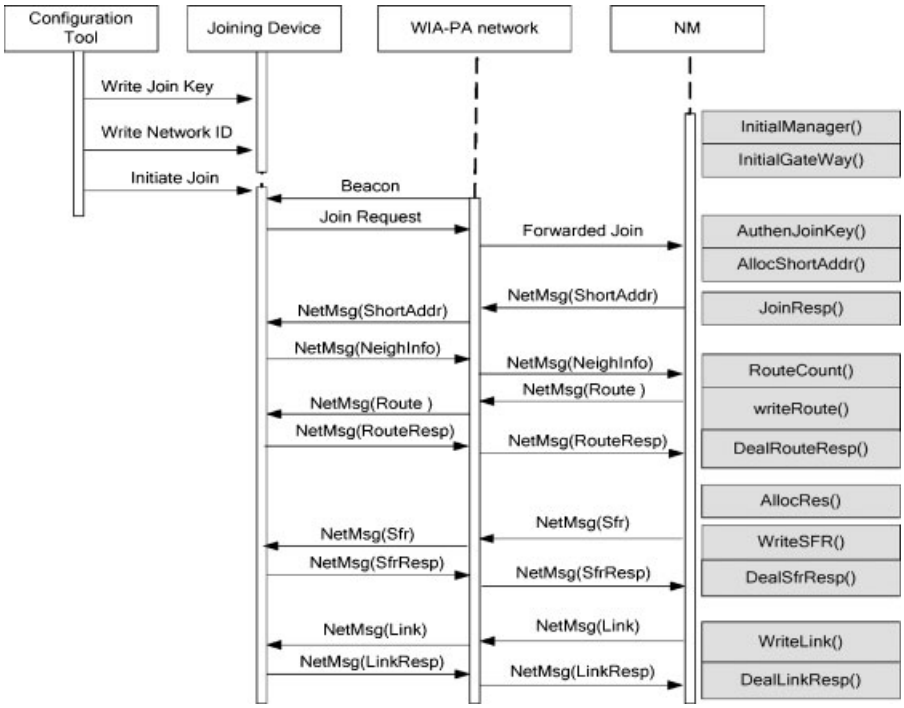

Figure 7. Joining sequence and function calling of routing device.

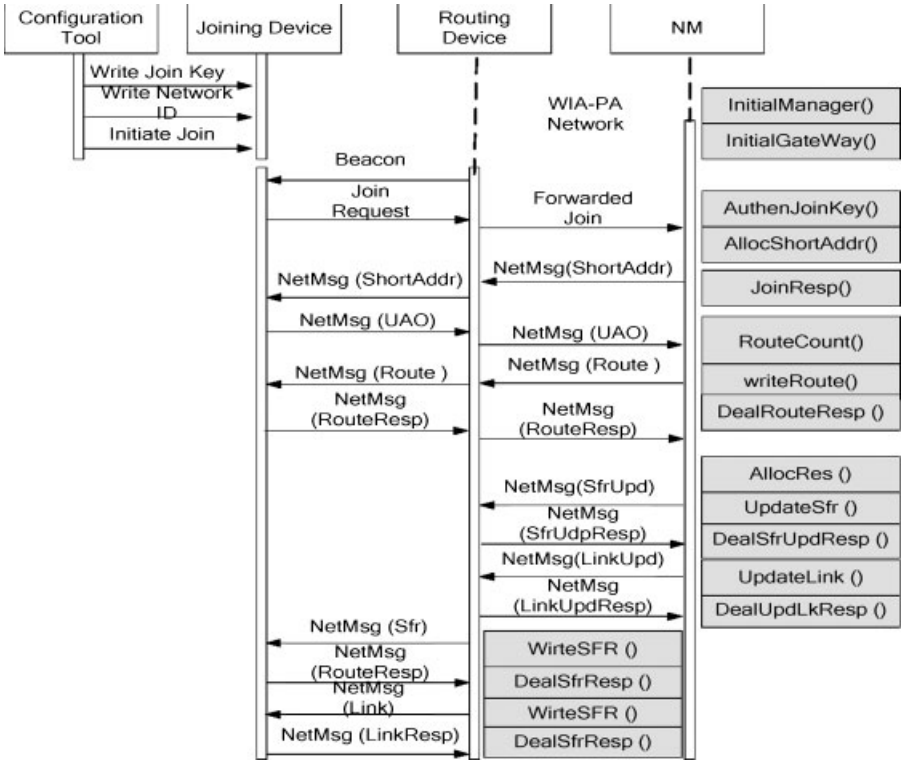

Figure 8. Joining sequence and function calling of field device.

the WIA-PA network. A routing device that wants to join the WIA-PA network should only choose a gateway device or an online routing device as its agent to join the network. A field device that wants to join the WIA-PA network should only choose an online routing device as its cluster head. After receiving a joining request from network devices, the NM verifies the new devices by calling *AuthenJoinKey()*, allocates short addresses by calling *AllocShortAddr()*, and returns a joining response by calling *JoinResp()*. After reporting neighbor device information by using the new routing device or reporting UAOs by using the new field device, the NM will allocate routes and communication resources for these devices by calling *RouteCount()* and *AllocRes()*.The NM will allocate default communication resource to a new routing device. With a new field device, the NM will first update the communication resources of its cluster head according to its variation of cluster members. Then the cluster head will write communication resources for the new field device.

5. REALIZATION OF WIA-PA TESTBED

5.1. Realization

The WIA-PA testbed is based on two kinds of platforms as follows:

- *Gateway platform*: The WIA-PA Gateway device is realized on the ARM9 platform and based on the Nucleus operational system as shown in the left of Figure 9. ARM9 has the advantages of high performance and low power-consumption. It has a five-level integer pipeline, supports 1.1MIPS/MHz Harvard architecture, and supports data cache and instruction cache. The Nucleus operational system is designed by the GreenHills Company and has good portability. It is compiled by using pure C language and integrated IDE on the Multi2000.
- *Node platform*: The WIA-PA routing device and field device are realized on the MSP430 platform and based on the μC/OS operational system as shown in the right of Figure 9. The MSP430 is a kind of microcontroller built around a 16-bit CPU and is designed for low cost, low power consumption embedded applications. The MSP430 is particularly well suited for wireless RF or battery powered applications and is a low-cost, priority-based, pre-emptive, real time multitasking operating system kernel for microprocessors, i.e., written mainly in the C programming language. It is mainly intended for use in embedded systems.

5.2. Test result

The WIA-PA testbed is shown in Figure 10. Figure 10(a) is the console program displaying the operational platform and related instructions. Figure 10(b) and Figure 10(c) are examples of the device joining process.

6. PHYSICAL EXPERIMENTS

6.1. Experiments environment and settings

Experiments are conducted in a small factory shown in the left of Figure 11. The layout of the devices is shown in Figure 11(a). The network consists of a gateway device and at most 40 devices and field devices. All devices are organized in mesh and star topology. The data update rate of each field device is 40 s. Experiments lasted two weeks.

6.2. Distributed communication resource allocation

A centralized scheme of communication resource allocation is adopted by WirelessHART and a two-stage one is used by WIA-PA. The performance and overhead of the two

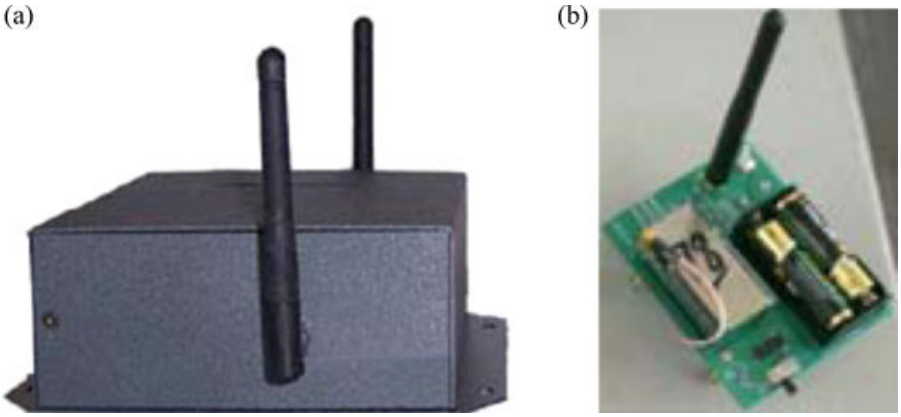

Figure 9. (a) Gateway and (b) node.

Figure 10. Device joining process demonstration.

schemes are tested. The communication resource allocation uses the greedy search algorithm. The performance index is the *success delivery ratio*, which is the probability that a packet can be successfully transmitted before its associated deadline. By successful we mean that the transmitting device must receive an acknowledgement packet for it. The deadline allows transmitting the packet, the corresponding acknowledgement, and a fair number of retransmissions that are carried out by either the source device or some repeaters.

Figure 12 is the success delivery ratio comparison between distributed and centralized algorithms, where 10, 20, 30, 40 nodes include 2, 4, 5, 5 routing devices and 4, 4, 5, 7 field devices of each routing device. The success delivery ratio of WIA-PA will decrease with an increase in the network scale when compared with WirelessHART. This occurs because WIA-PA allocates the communication resource block to routing devices and wastes some communication resources.

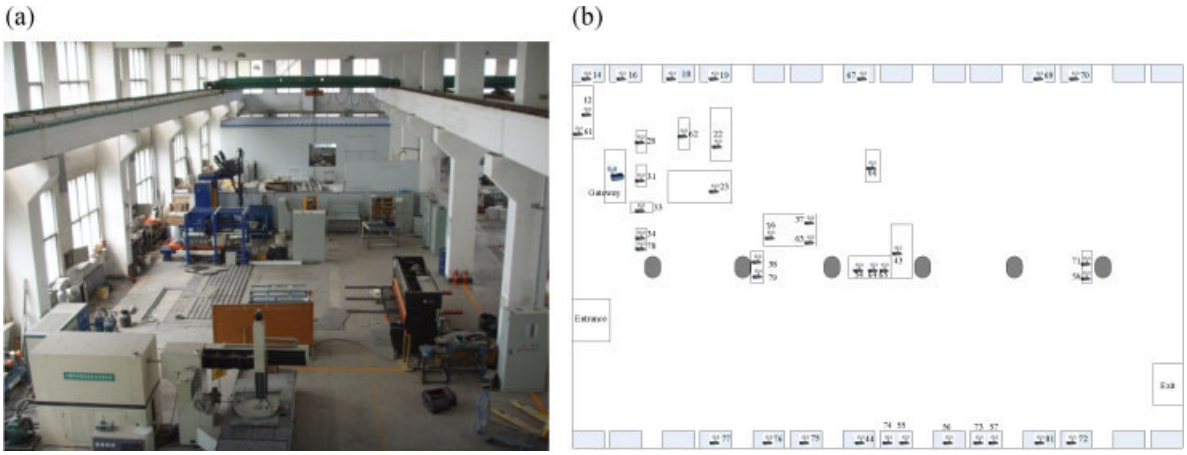

Figure 11. Experiment scenario.

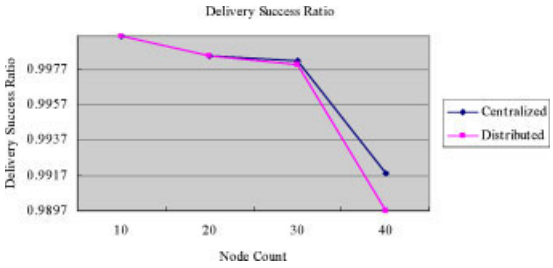

Figure 12. Performance comparison between distributed and centralized algorithms.

Figure 13 illustrates the calculating time and packet overhead of two resource allocation schemes. Figure 13(a) shows that the calculation time of the two-stage scheme is obviously better than the centralized one, which is easy to understand. The packet overhead of the WIA-PA scheme is lower than the centralized one in Figure 13(b). This is because the clumpy allocation can save some packets used by resource allocation.

6.3. Adaptive frequency hopping

The graph of Figure 14 provides some interesting data regarding communication quality for different channels of the IEEE 802.15.4 physical layer in our experiment factory. Figure 14(a) illustrates the results of transport success rates for different channels with increased of packet counts. The bar chart in Figure 14(b) shows the average transport success rate for all channels. The communication conditions of most channels have almost no difference besides channels 16, 17, 18, and 20. The communication quality of channel 16 is bad at all times. The bad communication quality of channels 17, 18, and 20 appears in certain time intervals. The blacklist technology of WirelessHART is static and can be used to simply screen networks from using bad channels, as in channel 16. If an adaptive frequency hopping strategy is used, the worst channels can be filtered dynamically, as in channels 17, 18, and 20.

6.4. Packet aggregation

WIA-PA supports the two-level packet aggregation schemes. Experiments to determine transport success rates for different packet lengths were conducted. The results of these experiments are shown in Figure 11. Figure 15(a) shows the change in the transport success rate for different packet lengths with the increasing of packet counts. There are some points in which transport success rates are obviously low. Transport success rates for all packets of different length are lower at that time. Because experiments

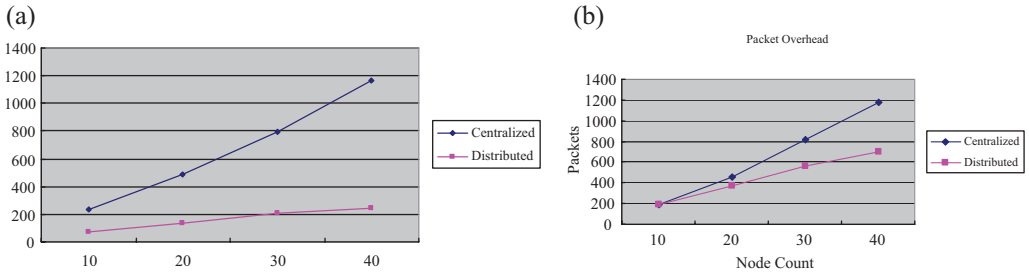

Figure 13. Overhead comparison between distributed and centralized algorithms.

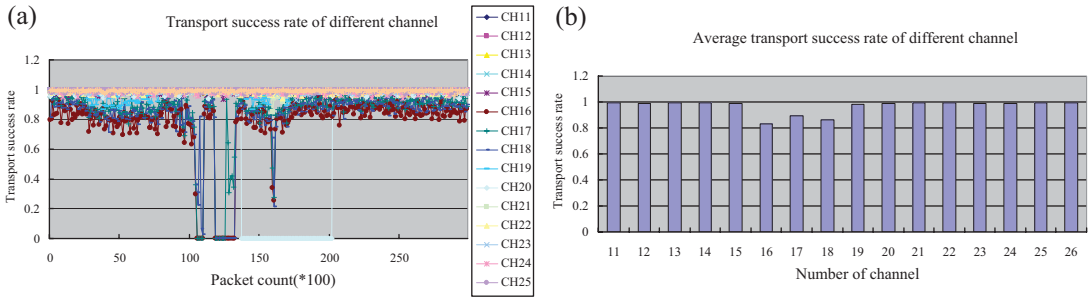

Figure 14. Experiment results of different channels.

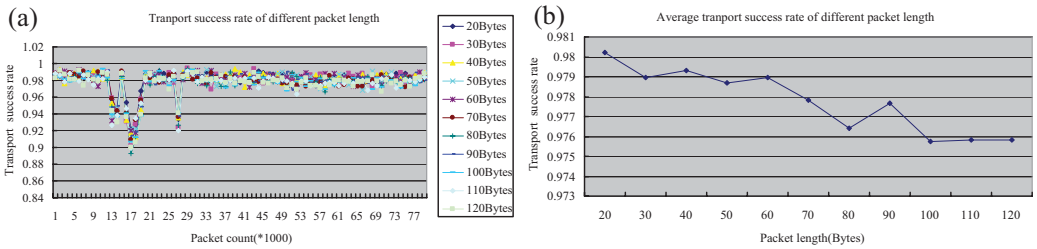

Figure 15. Experiment results of different packet length.

of different packet lengths are conducted synchronously through different channels, one possible reason is that the conditions of channels are worse. Figure 15(b) describes the change trend of average transport success rate with increasing packet length. The cure graph shows that the change in the average transport success rate has not changed a lot within certain a range of packet lengths. In other words, packet aggregation is effective when the aggregated packet is not too long. For the process automation application, the packets transported are mainly process data, and the packet length is very short. Therefore, a packet aggregation mechanism should be adopted.

7. CONCLUSION

The hot-spot of the industrial wireless network is standardization. WIA-PA is a kind of industrial wireless network specification that has its features compared with other industrial wireless network specifications. WIA-PA has obtained some preliminary applications, such as in the metallurgical and petrochemical areas, and has been approved by users. Our future works are major algorithms of WIA-PA.

ACKNOWLEDGEMENTS

This work is supported by the Natural Science Foundation of China under contract 60704046 and 60725312, and National high-tech research development plan (863 plan) of China under contract 2007AA04Z173 and 2007AA041201. Prof. Xiao is supported in part by the US National Science Foundation (NSF) under grants #: CNS-0716211 and CCF-0829827.

REFERENCES

1. www.eere.energy.gov/industry/sensors_automation
2. CIWA (Chinese Industrial Wireless Alliance).
3. Willig A. Recent and emerging topics in wireless industrial communications: a selection. *IEEE Transactions on Industrial Informatics* 2008; **4**(2): 102–124.
4. O'Neill O. Industrial wireless LAN applications, supplying solutions to industry demands. *The IEE Seminar on Industrial Networking and Wireless Communications for Control, 2006. (Ref. No. 2006/11301)*, February 2, 2006; 1–26.
5. HART Communication. Available at: www.hartcomm2.org/index.html
6. Song J, Han S, Mok AK, Chen D, Lucas M, Nixon M. WirelessHART: applying wireless technology in real-time industrial process control. *IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS '08)*, 2008; 377–386.
7. Kim AN, Hekland F, Petersen S, Doyle P. When HART goes wireless: understanding and implementing the WirelessHART standard. *IEEE International Conference on Emerging Technologies and Factory Automation, 2008 (ETFA 2008)*, September 15–18, 2008; 899–907.

8. Lennvall T, Svensson S, Hekland F. A comparison of WirelessHART and ZigBee for industrial applications. *IEEE International Workshop on Factory Communication Systems, 2008 (WFCS 2008)*, 21–23 May 2008; 85–88.
9. Zhu X, Dong W, Wei M, Aloysius KH, Han S Song J, Chen D, Nixon M. A location-determination application in WirelessHART. *15th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications, 2009 (RTCSA '09)*, August 24–26, 2009; 263–270.
10. Taroni A, Sisinni E, Rinaldi S, Marioli D, Flammini A, Ferrari P. An innovative distributed instrument for WirelessHART testing, *IEEE Conference on Instrumentation and Measurement Technology, 2009 (I2MTC '09)*, May 5–7, 2009; 1091–1096.
11. Kim AN, Hekland F, Petersen S, Doyle P. When HART goes wireless: understanding and implementing the WirelessHART standard. *IEEE International Conference on Emerging Technologies and Factory Automation, 2008 (ETFA 2008)*. September 15–18, 2008; 899–907.
12. De Dominicis CM, Ferrari P, Flammini A, Sisinni E, Bertocco M, Giorgi G, Narduzzi C, Tramarin F. Investigating WirelessHART coexistence issues through a specifically designed simulator, *IEEE Conference on Instrumentation and Measurement Technology, 2009 (I2MTC '09)*, May 5–7, 2009; 1085–1090.
13. Lennvall T, Svensson S, Hekland F. A comparison of WirelessHART and ZigBee for industrial applications. *IEEE International Workshop on Factory Communication Systems, 2008 (WFCS 2008)*, May 21–23, 2008; 85–88.
14. De Biasi M, Snickars C, Landernas K, Isaksson AJ. Simulation of process control with WirelessHART networks subject to packet losses. *IEEE International Conference on Automation Science and Engineering, 2008 (CASE 2008)*, August 23–26, 2008; 548–553.
15. De Biasi M, Snickars C, Landernas K, Isaksson A. Simulation of Process Control with WirelessHART Networks Subject to Clock Drift, *The 32nd Annual IEEE International Computer Software and Applications Conference, 2008 (COMPSAC '08)*, July 28, 2008–August 1, 2008; 1355–1360.
16. Zhang H, Soldati P, Johansson M. Optimal link scheduling and channel assignment for convergecast in linear WirelessHART networks. *7th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks, 2009 (WiOPT 2009)*, June 23–27, 2009; 1–8.
17. Zand P, Shiva M. Defining a new frame based on IEEE 802.15.4 for having the synchronized mesh networks with channel hopping capability, *11th IEEE International Conference on Communication Technology, 2008 (ICCT 2008)*, November 10–12, 2008; 54–57.
18. IS A100: Wireless Systems for Automation. Available at: www.isa.org
19. www.industrialwireless.cn/en/06.asp
20. Industrial Communication Network—Fieldbus Specifications—WIA-PA Communication Network and Communication Profile. Available at: www.iec.ch
21. Chinese Industrial Wireless Alliance. Available at: www.industrialwireless.cn/en/06.asp
22. Han S, Song J, Zhu X, Mok AK, Chen D, Nixon M, Pratt W, Gondhalekar V. Wi-HTest: compliance test suite for diagnosing devices in real-time WirelessHART network. *15th IEEE Real-Time and Embedded Technology and Applications Symposium, 2009 (RTAS 2009)*, April 13–16, 2009; 327–336.
23. Dang T, Devic C. OCARI: optimization of communication for ad hoc reliable industrial networks. *6th IEEE International Conference on Industrial Informatics, 2008 (INDIN 2008)*, 688–693.
24. Afolabi O, Richard O, Ahmad A, Kiseon K. Security assessments of IEEE 802.15.4 standard based on X.805 framework. *International Journal of Security and Networks* 2010; **5**(2/3): 188–197.
25. Misic J, Shafi S, Misic VB. Real-time admission control in 802.15.4 sensor clusters. *International Journal of Sensor Networks* 2006; **1**(1/2): 34–40.
26. Misic J, Amini F, Khan M. Performance implications of periodic key exchanges and packet integrity overhead in an 802.15.4 beacon enabled cluster. *International Journal of Sensor Networks* 2008; **2**(1): 33–42.
27. Musaloiu-E R, Terzis A. Minimising the effect of WiFi interference in 802.15.4 wireless sensor networks. *International Journal of Sensor Networks* 2008; **2**(1): 43–54.
28. Yin Z, Leung VCM. Connection data rate optimisation of IEEE 802.15.3 scatternets with multirate carriers. *International Journal of Sensor Networks* 2008; **3**(2): 95–106.
29. Krishnamurthy V, Sazonov E. Reservation-based protocol for monitoring applications using IEEE 802.15.4 sensor networks. *International Journal of Sensor Networks* 2008; **4**(3): 155–171.
30. Xiao Y, Chen H, Sun B, Wang R, Sethi S. MAC security and security overhead analysis in the IEEE 802.15.4 wireless sensor networks. *EURASIP Journal on Wireless Communications and Networking* 2006; Article ID 93830, 12 pages. DOI:10.1155/WCN/2006/93830
31. Xiao Y, Sethi S, Chen H, Sun B. Security services and enhancements in the IEEE 802.15.4 wireless sensor networks. *Proceedings of The IEEE Global Telecommunications Conference 2005 (IEEE GLOBECOM 2005)*, 1796–1800.

32. Shuaib AH, Aghvami AH. Dynamic topology control for the IEEE 802.15.4 network. *International Journal of Sensor Networks* 2009; **6**(3/4): 212–223.
33. Wang K, Tang L, Huang Y. Transmission error analysis and avoidance for IEEE 802.15.4 wireless sensors on rotating structures. *International Journal of Sensor Networks* 2009; **6**(3/4): 224–233.
34. Zhang X, Tan L, Li J, Zhao S, Chen H. ATBAS: an efficient fair bandwidth allocation approach for multihop wireless ad hoc network. *International Journal of Sensor Networks* 2008; **3**(2): 134–140.

Authors' Biographies

Wei Liang received the Ph.D. degree in Mechatronic Engineering from Shenyang Institute of Automation, Chinese Academy of Sciences, in 2002. She is currently serving as an associate professor of Shenyang Institute of Automation. Her research interests are in the areas of wireless sensor network, dynamic scheduling theory, and system simulation.

Xiaoling Zhang is a doctor candidate of Shenyang Institute of Automation, Chinese Academy of Sciences (CAS) and Graduate School of the CAS. She is focusing on industrial wireless network, transmission scheduling, and power control.

Dr Yang Xiao is currently with Department of Computer Science at The University of Alabama. He presently serves as Editor-in-Chief for International Journal of Security and Networks (IJSN), International Journal of Sensor Networks (IJSNet), and International Journal of Telemedicine and Applications (IJTA). He serves as an associate editor for several journals, e.g., IEEE Transactions on Vehicular Technology. His research areas are security, telemedicine, robot, sensor networks, and wireless networks. He has published more than 300 papers in major journals, refereed conference proceedings, book chapters related to these research areas.

Fuqiang Wang is a doctor candidate of Shenyang Institute of Automation, Chinese Academy of Sciences (CAS) and Graduate School of the CAS. He is focusing on industrial wireless network and time synchronization.

Haibin Yu holds a Ph.D. degree in Automation Control from Northeastern University, Shenyang, China. He is a professor at Shenyang Institute of Automation, Chinese Academy of Sciences. His research has involved wireless sensor network, networked control systems, and networked manufacturing.

Peng Zeng received the Ph.D. degree in Mechatronic Engineering from Shenyang Institute of Automation, Chinese Academy of Sciences, in 2005. He is an associate professor at Shenyang Institute of Automation. His research has involved wireless sensor network and industry communication.