PAWS Framework

- **draft-lei-paws-framework-datamodel-00**

Zhu Lei, e-mail address: lei.zhu@huawei.com Mobile phone: +86-10-13910157020

Wei Xinpeng, e-mail address: weixinpeng@huawei.com

Contents

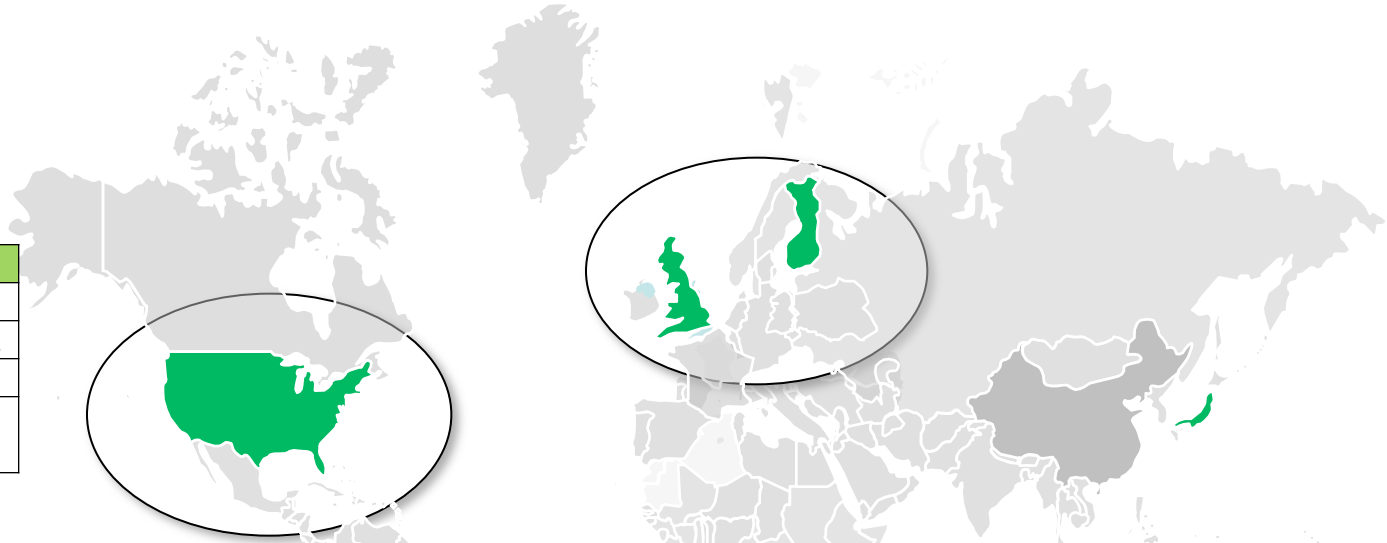
- **Requirements and audience**
- **Real scenarios**
- **Issues of PAWS protocol**
- **Data model**
- **Security**
- **Need extensibility**

Use cases and requirements

- **In the scope: a protocol to access white space data base**
- **Out of the scope: interference avoidance, provisioning**
- **Use cases: discovery, registration, hotspot, wide area, wireless backhaul, ad hoc deployment, mobile MSD, indoor and M2M.**
- **Requirements satisfied by this document:**
  - Data model: D.1-D.10 (all)
  - Protocol: P.1, P.2 (partial), P.3-P.12, P.18-P.19
  - Operational requirements: O.1-O.9, O.15-O.18, O21-O22
  - What are others: some process involving slave devices
- **Security requirements:**
  - Reasons: The spectrum is lasting limited resource dominated by regulatory from long term perspective and assumed to be used properly.
  - Requirements in general:
    - Bidirectional authentication
    - Integrity protection

Scenarios

Roles	
Administrator	FCC, Ofcom, etc
Primary user	TV
secondary user	Wifi, cellular
Service provider	ISP, property owner, Enterprise

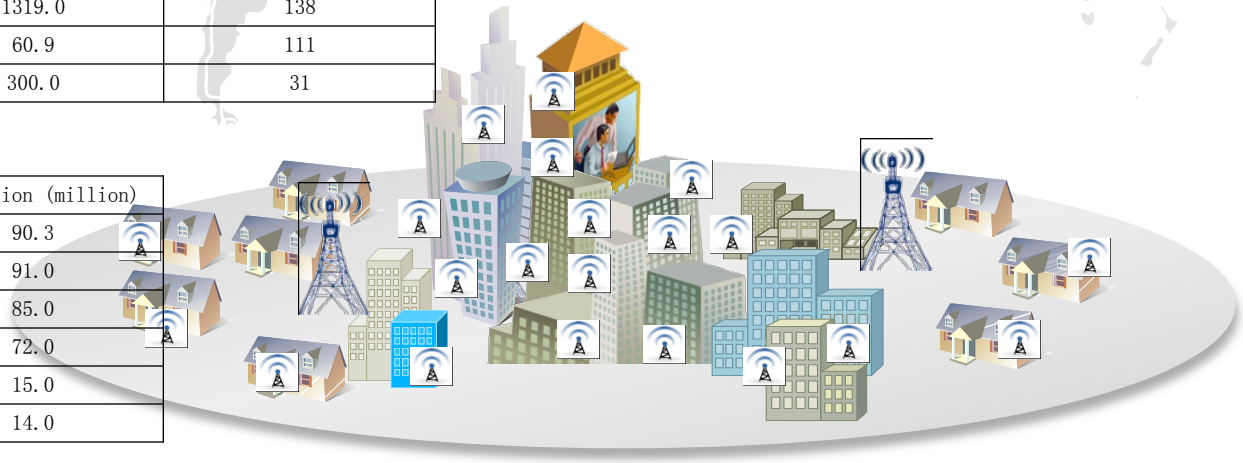


Countries

Country	Area (million square kilometer)	Population (million)	Density (per sq.km.)
Bangladeshi	0.14	147.4	1023
Japan	0.37	127.6	338
Indian	2.98	1095.4	333
UK	0.24	60.6	248
China	9.6	1319.0	138
France	0.55	60.9	111
US	9.82	300.0	31

Provinces of China

Province	Area (million square kilometer)	Population (million)
Henan	0.16	90.3
Shandong	0.15	91.0
Sichuan	0.48	85.0
Guangdong	0.18	72.0
Beijing	0.016	15.0
Shanghai	0.006	14.0



Issues of framework

Figure 1 shows a common system model consisting of Master Device and Database merely. The Master Device connects to the database directly using *WS interface*.

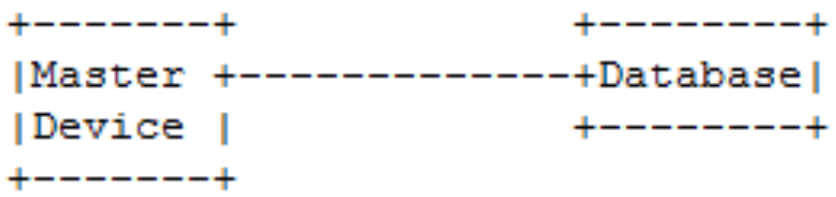


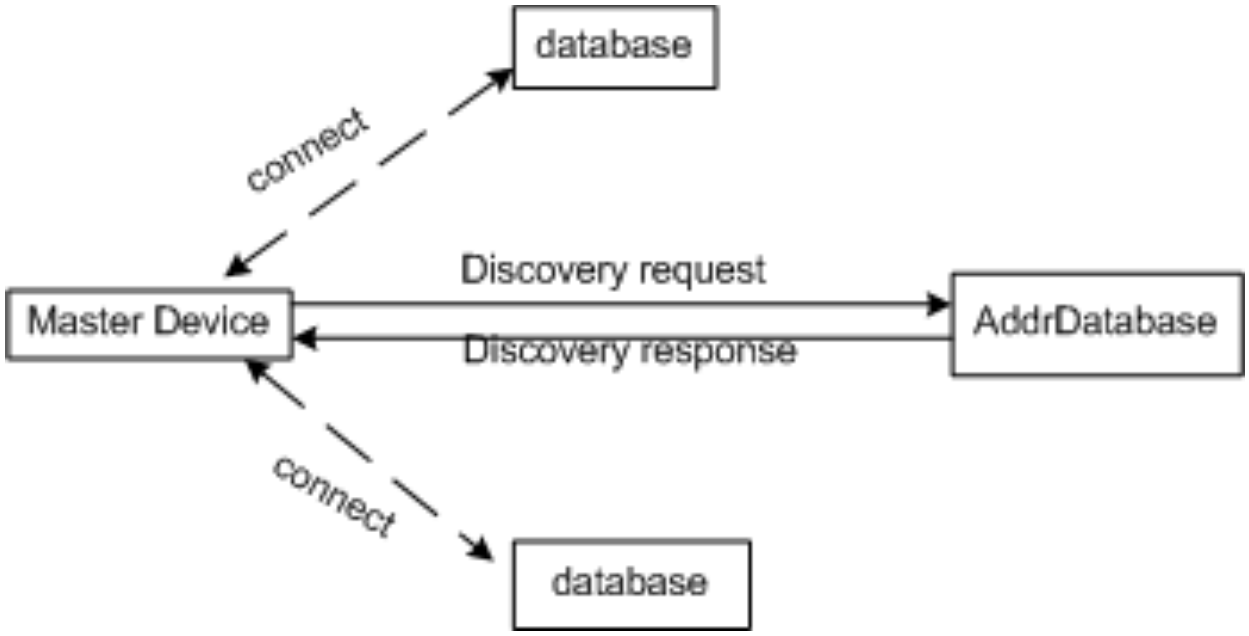
Figure 1: Framework of PAWS

Master device **in Figure 1 is a kind of white space device which querying available channel list from database providing radio access to user equipments. Due to PAWS principle of access technology agnostic, it can be access point of WiFi, NodeB of 3GPP WCDMA or eNodeB of 3GPP LTE etc.**

Database **in Figure 1 is in charge of storing and maintaining white space channel information for certain area(s), it may be operated by regulatory. When the database receives request of white space**

spectrum querying from the master device, it will respond a list of available white space channel list to the master device if there are available spectrums.

Protocol framework: framework of PAWS database discovery



The function of AddrDatabase is to provide the list of trusted databases in the relevant regulatory domain to the master device. The AddrDatabase is either hosted by or under control of the national regulator.

Protocol framework: protocol stack

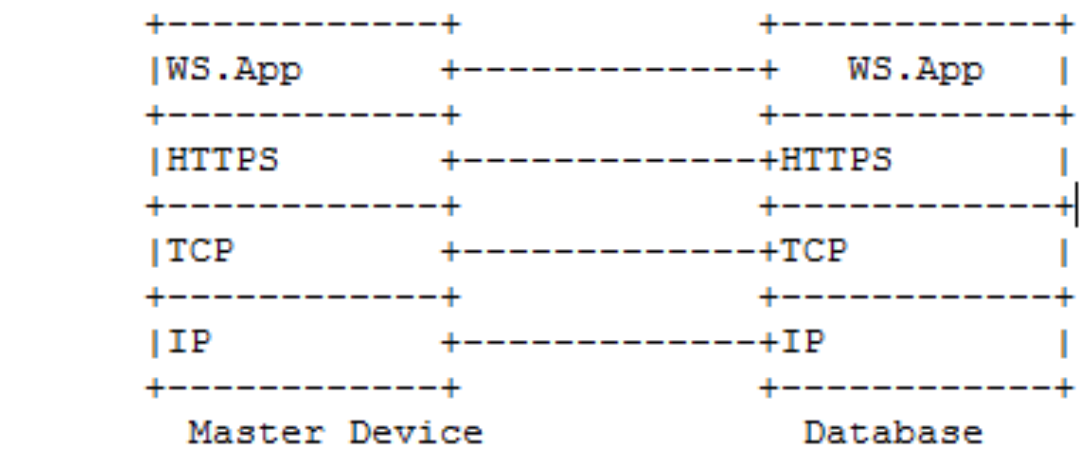


Figure 5: Protocol stack of PAWS protocol

WS.App **is the white space spectrum application protocol. This protocol stack is**

Protocol framework : interface of PAWS

- **Database Discovery**
- **Device Registration with Trusted Database**
- **White Space Channel Query**
- **White Space Channel Update**

Interface of PAWS: WS Channel Update

In order to avoid interfering with the primary user or other secondary user, the white space updating mechanism is provided in this draft. There are two methods for white space updating:

METHOD1 : The white space device MUST access the database to obtain and update the list of available channels that could be utilized by the device. According to some regulatory rules the white space device SHOULD update the white space channel periodically, and the period may be different due to different regulatory rules.

METHOD2 : Database push updates in channel availability changes to the master device, when the availability of channel changes database SHOULD inform the master device and after receiving the notification the master device SHOULD begin the white space channel query procedure to get the updated white space channel.

The update procedure of method 1 is shown in Figure 9.

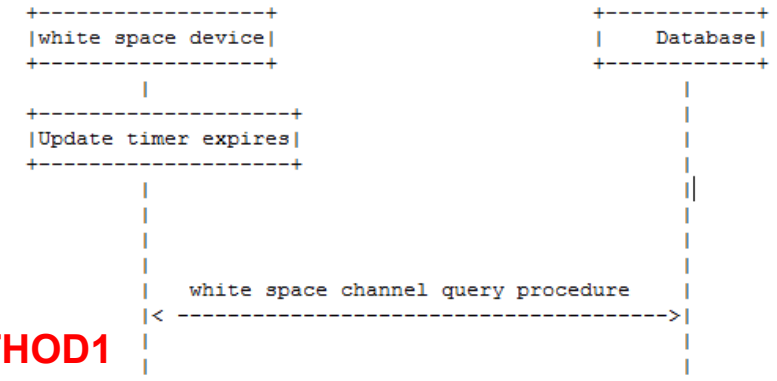


Figure 9: White space channel update procedure for method 1

The update procedure of method 2 is shown in Figure 10.

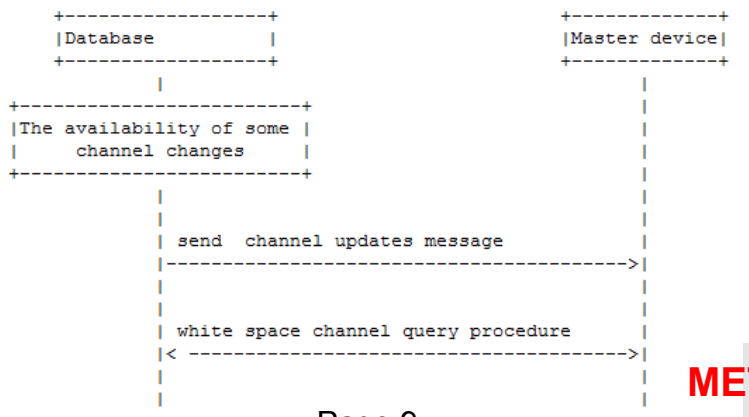


Figure 10: White space channel update procedure for method 2

METHOD1

METHOD2

Message encoding

In this framework XML is used to encode the message. HTTPS is used to carry the
In this framework XML is used to encode the message. HTTPS is used to carry the

<xs:element name="DISCOVERY_REQ_MSG">

<xs:element name="DISCOVERY_RESP_MSG">

<xs:element name="REGISTRATION_REQ_MSG">

<xs:element name="REGISTRATION_RESP_MSG">

<xs:element name="AVAIL_WS_REQ_MSG">

<xs:element name="AVAIL_WS_RESP_MSG">

<xs:element name="CHANNEL_UPDATE_NOTIFICATION">

For the request message:
For the request message:

GET destination_url HTTP/1.0
Content-Type: text/xml

<?xml version="1.0" encoding="UTF-8"?
>

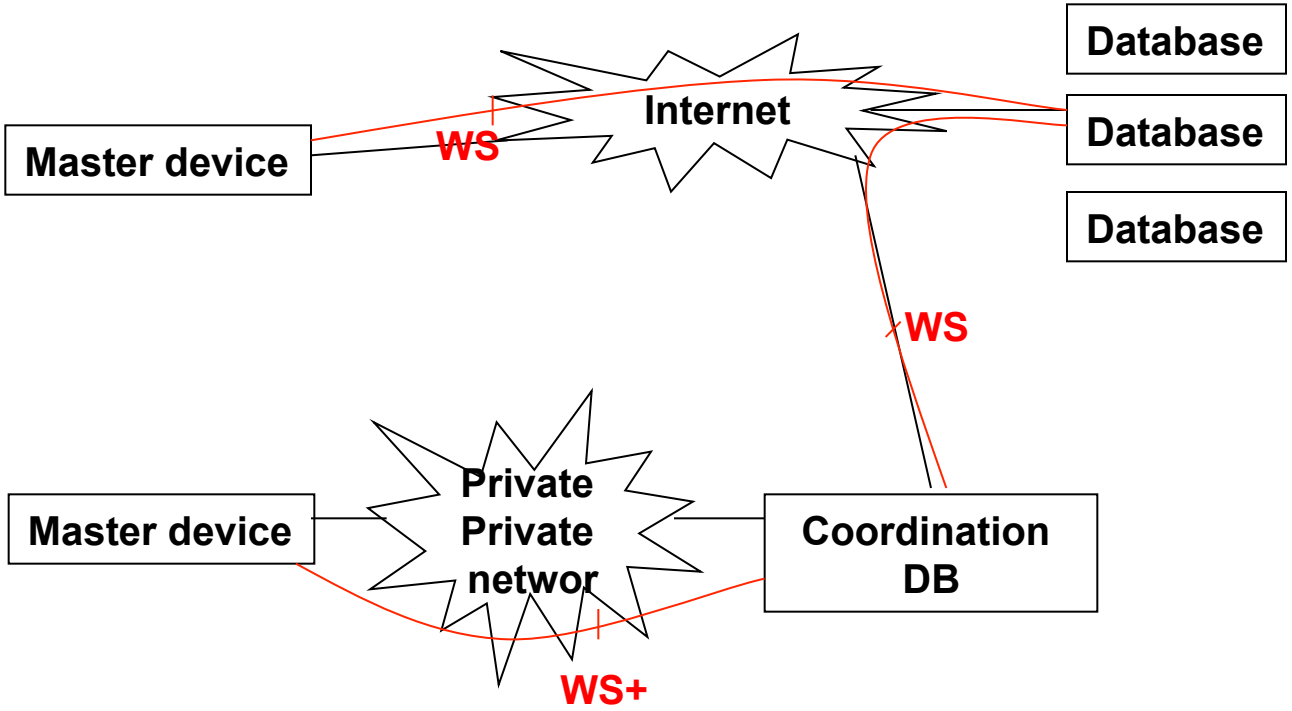
Security countermeasures

- The master device shall be authenticated by database based on a globally unique and permanent master device identity.
- The master device shall authenticate the database.
- Sensitive data including authentication credentials, user information, cryptographic keys shall not be transmitted between the master device and the database in plaintext in unauthorized access. It means that the link between the master device and the database shall provide integrity, confidentiality, and replay protection of transmitted data.
- The master device should have a secure module to store long term key or certificate. The identity of master device could be stored in a trusted physical module and/or a possible non-removable smartcard.

Security schemes

- According to the RFC 5246, RSA or Diffie-Hellman can be used for authentication and key exchange.
- The identity of the master device and the database can be authenticated using asymmetric, or public key, and cryptography (e.g., RSA,DSA, etc)
- symmetric cryptography is used for data encryption (e.g., AES, RC4, etc).
- A keyed MAC is used to message integrity check. Secure hash functions (e.g., SHA-1, etc) are used for MAC generated.

Additional coordination role of DB



Protocol framework: coordinating DB

Coordinating Database **is logical function which is a combination of master device and Database (which stores a part or all of the white space spectrum information in certain area), the Coordinating Database gets white space spectrum from database acting as Master Device, the logical function of Coordinating Database is depicted in Figure 3.**

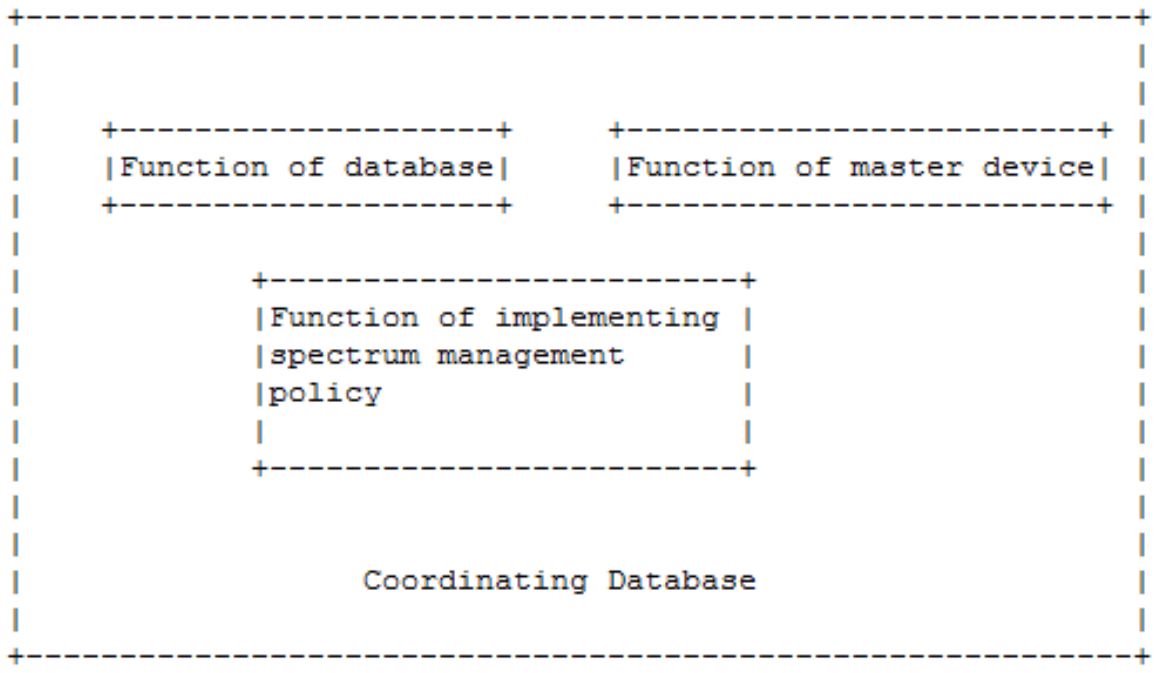


Figure 3: Logical Function of Coordinating Database

Protocol framework: coordinating DB functions

Coordinating database includes three main functions:

(1) The function of master device. It can retrieve available channel list from Database on behaviors of master device (fulfilled by function of white space device).

(2) The function of database. To master device the coordinating database acts just like a proper available channel list when receiving query request from master device etc.

(3) The function of implementing spectrum management policies. For example, the