# Models and Assumptions

SWIB adopting threshold signature technology allows nodes to agree on block in blockchain system under wireless networks with unreliable channels efficiently. We describe the basic preli(基础设置) of SWIB including network model, communication model, blockchain setting, threshold signature scheme and adversary assumptions.

## 3.1 Network Model

We consider a wireless broadcast network consisting of nodes, which are located within communication range of each other, and communicating with each other by transmitting messages. All nodes have same functions. Each node equipped with transceiver works in a half-duplex manner. This means that nodes can transmit or receive messages, but not both simultaneously. In practice, such a network can be formed by a group of unmanned aerial vehicles or intelligent vehicles.

(加一个过渡句子，引入共识过程)For simplicity, we assume that the consensus processing is divided into synchronous rounds, each of which contains multiple slots. A slot is the time unit for nodes to transmit or receive a packet.

(加一个过渡句，引入密钥)We assume that each node can get its private-public key pair and a main public key by independently running a secure distributed key generation protocol. Each node can obtain other nodes(名词复数后面的be用什么形式) public keys and identities by exchanging messages. Thus, each node knows the identities and public keys of all other nodes.

## 3.2 Communication Model

We consider a wireless communication model of blockchain systems.

During consensus process, all consensus nodes compete for the channel to transmit messages. (我们的通信是p坚持的，解释一下) Each node transmits a message with probability when detecting channel idle.

We assume that the wireless channels follow the Rayleigh fading model [32]. In detail, the wireless channel between nodes and experiences path-loss is modeled as

where is defined as the path-loss of reference distance , and is the Euclidean distance between nodes , and path-loss exponent . (重新描述) Let be the channel gain from to , following the complex normal distribution with zero mean and variance (i.e., ). When a signal is transmitted from to with transmission power , the Signal-to-Noise (SNR) ratio at receiving node is formulated as

where is the additive white Gaussian noise.

Messages losses can lead to consensus failure. In addition, message losses are mainly caused by channel collision and channel fading. Therefore, a successful transmission should satisfy two conditions: 1) if and only if there only one node transmitting in a time slot; and 2) the receiving/received SNR ratio is equal to or bigger than the target one.

In channel contention process, nodes compete for the channel with same transmit probability . Only if(用法) one node transmits in a time slot, can the node transmit a message. Thus, transmission contention success probability can be expressed as

Even a node competes the channel successful, it may fail to transmit a message due to channel fading. The SNR between nodes changes with time-variant communication environment. When SNR fails below the target value, the communication between nodes is interrupted. Since is exponentially distributed, the communication interruption probability between nodes and is expressed as follows

(加一句过渡，总结-消息丢失-解决方案)When a communication interruption occurs, retransmissions are carried out until the lost messages are successfully delivered.

（数学严谨，公式统一）