# Models and Assumptions

SWIB adopting threshold signature technology allows nodes to agree on block in blockchain system under wireless networks with unreliable channels efficiently. In this section, we describe network model, communication model, blockchain setting, threshold signature scheme and adversary assumptions.

## 3.1 Network Model

In this study, we consider a wireless network consisting of nodes, which are deployed in Euclidean space. Let be the set of nodes. We assume any node can communicate with any other node in the network directly, which means the network under study forms a complete graph. In practice, such a network can be formed by a group of Unmanned Aerial Vehicles or intelligent vehicles. The transceiver at each node works in a half-duplex manner, which can transmit or receive messages, but not both at a time. Time is divided into rounds, each of which contains a fixed number of slots. A slot is the time unit for nodes to transmit or receive a message. Each node can generate its private-public key pair and main public key by running a secure distributed key generation protocol. Each node can obtain other nodes' public keys and identities by exchanging messages. In this paper, we assume that the number of honest nodes satisfies the requirement of threshold BLS signature scheme, which ensures the security of the proposed protocol.

In this study, we consider a wireless broadcast network consisting of nodes, which are located within communication range of each other. Let be the set of the nodes. In the wireless network, nodes communicate with each other by broadcasting messages. The transceiver at each node works in a half-duplex manner, which 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. 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 data packet. We assume that each node can generate its private-public key pair and obtain the main public key by independently running a secure distributed key generation protocol. Each node can obtain other nodes' 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 simultaneously contend for the channel to transmit message. Each node transmits a message with probability when detecting channel idle. Besides, nodes disseminate messages over wireless channels, of which reliability is affected by large and small scale fading effects. We assume that the wireless channels follow the Rayleigh fading model [32]. In detail, the wireless channel between nodes and experiences path-loss with path-loss exponent is modeled as

Where is defined as the path loss of reference distance , and is the Euclidean distance between nodes , path loss exponent . 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 ratio at receiving node :

where is the additive white Gaussian noise power.

In the presence of unreliable communication, consensus may not be achieved if majority messages sent in a consensus round can be lost. Message losses can be caused by collision and channel fading. Thus, a successful transmission should satisfy two conditions: 1) if and only if there only one node transmitting in a time slot; and 2) the receive SNR is equal to or bigger than the target SNR ratio of each transmission.

In channel contention process, nodes compete for the channel with same transmit probability. let be the transmit probability of consensus nodes. Since a successful transmission occurs if and only if one node transmitting in a time slot. Thus, the 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. Message transmission rate between nodes is determined by the SNR., and the SNR between nodes changes with time-variant communication environment of blockchain system. When SNR fails below the minimum SNR threshold, the communication between nodes is interrupted. Since is exponentially distributed, the communication interruption probability between nodes and is expressed as follows,

For an operation point of view in the actual channel condition, if an communication interruption occurs caused by poor condition of actual channel, retransmissions are carried out until the lost messages are successfully delivered.

These channel contention, transmission failures, and retransmissions are taken into account in the performance analysis and the consensus protocol design.