Location-Aware Wi-Fi Authentication Scheme

Subjects: Computer Science, Information Systems

Contributor: Yongle Chen , Xiaojian Wang , Yuli Yang , Hong Li

Advanced wireless technology in Internet of Things (IoT) devices is increasing and facing various security threats. The authentication of IoT devices is the first line of defense for the wireless network. Especially in a Wi-Fi network, the existing authentication methods mainly use a password or digital certificate, these methods are inconvenient to manage due to certificate issuance or prone to be attacked because passwords are easily cracked. A location-aware authentication scheme was proposed, using smart contracts to ensure that IoT devices can securely perform Wi-Fi network authentication. The scheme adopts the concept of secondary authentication and consists of two phases: the registration phase, which is mainly designed to complete the generation of the public and private keys, and to link the device information with its related device information; the authentication phase, which is mainly designed to determine whether the requesting device is within a legal location range. The smart contract to ensure the credibility and irreparability of the authentication process. Analysis of the attack model and the attacks at different stages proves that this certification scheme is assured, and the simulation results show that the overhead introduced by this scheme is acceptable, this scheme can provide greater security for the Wi-Fi authentication of IoT devices.

authentication blockchain channel state information smart contracts

1. Introduction

Consider the network access authentication of IoT devices in smart home scenarios, assume that all devices that need to access the network have wireless networking functions and Bluetooth functions. Devices that need to perform network authentication must enter the password to generate a public and private key pair, record the device information, and the information of the related devices that is close to it utilizing smart contract to successfully register, and then initiate the network authentication request. The authentication phase uses the challenge–response system to confirm that the requesting device correctly executes the random instruction, and uses the CSI information returned by the related devices to confirm whether the requesting device is in a legal location. The aggregate signature guarantees the correctness of the returned CSI information.

The authentication scheme proposed by us is mainly aiming at the Wi-Fi network authentication process in the current smart home environment which mainly adopts the authentication methods such as password authentication or digital certificate, they are simple and the management is inconvenient, the security is not high at the same time. This method adopts the idea of secondary authentication and is divided into two phases: the first phase is the registration phase, which is mainly to complete the public key and private key generation and to link the device information with its related devices information. The second phase is the authentication phase, the Challenge-

Response architecture is used in this phase, confirming the legality of the information returned by the requesting device and its related device, determining the similarity between the CSI information of the requesting device and the CSI information returned by the related device, thereby determining whether the requesting device is within a legal location range. The smart contract was used to constrain the behavior of the device and ensure the correct execution of the whole process of identity authentication policy.

2. Registration phase

The first stage is the registration phase, a valid password is required to register successfully. The registration phase is mainly to complete the public key and private key generation and to link the device information with its related devices information. The requesting device A that requests access for the first time needs a password to generate the address of this device on the blockchain and generates the device's own private key, followed by the process of recording device information and related device information. This process is constrained by a smart contract called Register smart contract (RSC). Take device A for Wi-Fi network authentication as an example, the specific steps of this process are as follows:

(1) Device A initiates a request < $Name_A$, ID_A > try to access AP. $Name_A$ is the name of device A and ID_A is the ID of device A.

(2) After receiving this request, the AP initiates a Request Transaction and the smart contract RSC monitors this request information, executes Function 1: Sends a program P which can be run by the requesting device to device A.

(3) A receives the program P and enters <ID_A|password> into this program P.

(4) After the program P confirms that the password inputted is correct, a pair of unique public key P_A and a private key S_A are generated for the device A. The private key of the device is a random number randomly generated by the device A and keep by itself. The public key of the device is calculated by the ECC algorithm. The hash of P_A is used as the address Add_A of the device A, then <Add_A|P_A> is sent to the AP.

(5) After receiving the information, the AP initiates a Register Transaction, which triggers the Function 2 of the smart contract RSC: Record the device information <$Name_A$, ID_A, Add_A, P_A>.

(6) Device A perceives the RSSI value of the Bluetooth of the surrounding devices and calculates the distance corresponding to the different devices, and selects the n devices closest to it as their related devices.

(7) Device A initiates a Related Transaction, which triggers the Function 3 of the smart contract RSC: Confirm whether the device in the Ralated Transaction has legal identity in the network environment (the related device is the device that was previously authenticated), and if the related device is confirmed as a legal device, record the related device information <Num., Distance, Related_dev_Address, Establishment_time, Failure_time>.

3. Authentication phase

The second phase of this scheme is the authentication phase, which uses location information for authentication. The Challenge-Response system is used to confirm that the requesting device correctly executes the random command sent by the AP, and use the aggregate signature to confirm the legitimacy of the information returned by the requesting device and its related device. In order to determine whether the requesting device is within the legal location range, determine whether the CSI information of the requesting device is similar to the CSI information returned by its related devices. If it is within the legal scope, approve the device to access the network. Otherwise, refuse this device to access the network. This process is constrained by a smart contract called Authentication Smart Contract(ASC). The specific steps of this process are as follows:

(1) Device A requests to access the network.

(2) After receiving the request information, the AP initiates an Identity-confirm Transaction, triggering the Function 1 of the smart contract ASC: Confirming that device A is registered legally and querying the related devices information of device A.

(3) The AP sends a Random instruction RI(TargetID, Speed, Duration)encrypted by device A public key to device A, and the content of the random instruction is to collect m packets at a rate of n packets per second, devices around device A need to follow this command to return their respective CSI values.

(4) Device A receives this random instruction and initiates a Query Public Key Transaction which triggers Function 2 of smart contract ASC: Query the public key of its related device, encrypt the random instruction with the corresponding public key of its related device and send it out.

(5) Device A's related devices receive this instruction, decrypts it with their own private key to get the original instruction, collects m packets at the rate of n packets per second (message) according to the instruction. Sign the message with its own private key and encrypt the signed message using the AP's public key and send it to the AP. The related devices perform aggregation signature according to the sequence number, and then the last related device sends this signature to device A, device A collects its CSI information according to the instruction and then performs final signature process. Device A initiates an Aggregate Signature Transaction and put the final signature on the chain.

(6) The AP initiates an Signature-verify Transaction, which triggers the Function 3 of the smart contract ASC: Confirm whether the aggregate signature in the transaction is legal and whether at least 2/3n devices participate in the aggregate signature, whether the similarity of CSI collected by device A and its related devices are within the threshold, where n is the total number of related devices of device A. If all the conditions are met, the AP allows device A to access the network. Otherwise, device A is denied access to the network.

Among them, all transactions are sent by the corresponding initiator with their own private key signature.