5.3.5 ID-Based One-Pass Authenticated Key-Establishment Protocol for WSN

Authenticated session key-establishment techniques have been an integral part of any legacy network such as IP networks. These protocols provide the concerned communicating parties with an authentic shared session key in a secure way. For WSN, the use of such session keys is particularly important because there is a need to securely exchange data between the sink and the leaf nodes. In addition, external users also access the aggregated data from the sink or from the leaf nodes directly. However, the use of a two-pass key-establishment protocol (e.g., the Diffie-Hellman key exchange mechanism) in a resource constraint environment such as WSN could incur increased storage, communication, and computational costs. Hence, there is a need for an authenticated session key-establishment scheme that should provide adequate security and be resource efficient in an environment such as WSN.

An easy alternative that could be resource efficient and provide reasonable security is a one-pass authenticated key-establishment method. As the name states, the sender generates an ephemeral private key, and its corresponding public key is only sent once to the receiver. Subsequently, both parties compute the shared session key using the ephemeral key and their private key.

ID-based one-pass authenticated key-establishment protocol by utilizing the four phases (Yasmin et al. 2011): *System Initialization*, *Private Key Generation*, *User Registration*, and *Key Establishment*. The first two phases are performed once, before the deployment of the sensor network. In an ID-based cryptosystem, a PKG computes the private keys cor-responding to the IDs. In WSNs, the base station (a resourceful device) is considered as trustworthy. In this scheme, the base station plays the role of PKG and computes the private keys for sensor nodes and users.

5.3.5.1 System Initialization

In this phase, the Setup algorithm runs on the sink node and generates the system parameters, including the master public key (*Puk*) and the corresponding master secret key (*Prk*), by using a security parameter *k*.

This algorithm performs the following steps:

- Specify q, p, E/F_p, P and G, where q is a large prime number and p is the field size, E/F_p is an elliptic curve E over a finite field F_p, P is a base point of order q on the curve E, and G is a cyclic group of order q under the point addition "+" generated by P.
- For *Prk*, $s \in Z_q^*$, compute *Puk* as $P_{PKG} = sP$.
- Choose one hash function $H : \{0,1\}^* \times G \rightarrow Z_q^*$.
- Choose one key derivation function $\chi : G \rightarrow \{0,1\}^k$
- Output system parameters $\{q, p, E / F_p, P, G, P_{PKG}, H, \chi\}$ and keep s secret.