

Chapter 2

System Model

2.1 Network and Communication Models

For military and disaster recovery applications, the multi-hop wireless network can be considered ephemeral because it is used for a specific purpose and short duration. This brief considers the civilian applications of MWNs, where the network has long lifetime and the nodes have long-term relations with the network. Thus, with every interaction, there is always an expectation of future reaction.

As illustrated in Fig. 2.1, the considered multi-hop wireless network has an off-line trusted party (Tp) and mobile nodes. The mobile nodes have different hardware and energy capabilities. We assume that the clocks of the nodes are synchronized. The details of this synchronization process are out of the scope of the brief, but several mechanisms have been proposed to synchronize the nodes' clocks [1]. We consider only the unicast communications. If a source node needs to communicate with a remote destination node, the mobile nodes should act as routers and relay the source node's packets to the destination node.

The mobile nodes should contact Tp periodically at least once during a time interval, called updating time, that can be in the range of few days. During this connection, the nodes submit the payment reports and the *Evidences* (if requested) and receive renewed certificates. Without holding a valid certificates, the nodes cannot work as source, destination, or intermediate nodes. During this connection, the nodes can also purchase credits with real money. This can enable the nodes that cannot earn sufficient credits, such as those at the network border, to communicate. This can also protect the network from credit decline because the total charges may be more than the rewards, as will be discussed later. The connection to Tp can occur via the cellular networks' base stations, Wi-Fi hot spots, or wired networks such as the Internet.

Tp and its public key are known for all the mobile nodes. Tp stores and manages the nodes' credit accounts and trust values. When Tp receives the payment reports of a session, it verifies them. If the reports are fair, Tp updates the involved nodes' credit accounts and trust values. For the cheating reports, it requests the *Evidences*

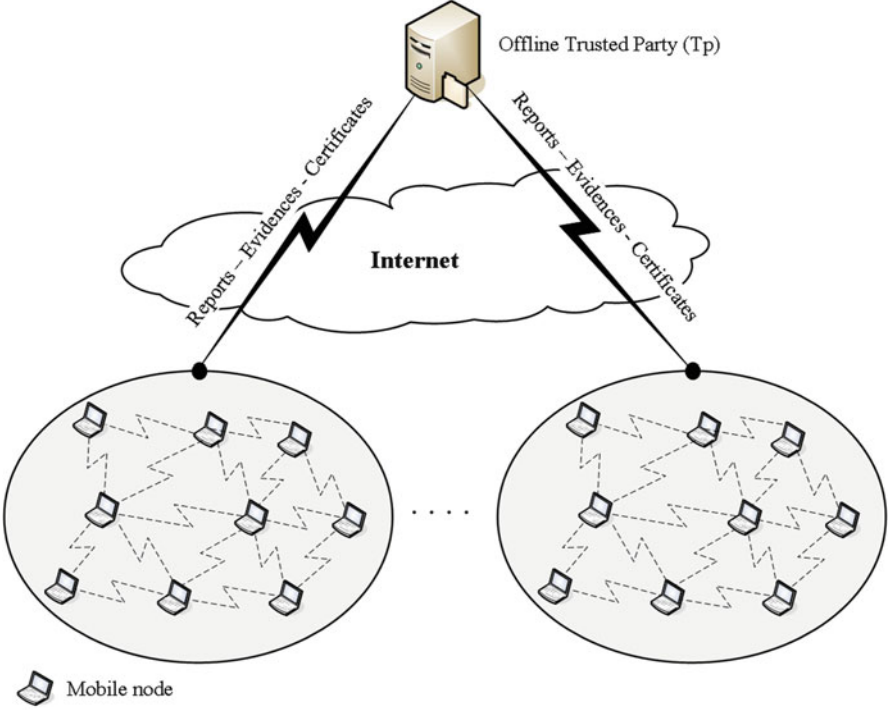


Fig. 2.1 The architecture of the multi-hop wireless network

to identify the cheating nodes that send incorrect payment reports. Tp evicts the cheating nodes by denying renewing their certificates. It issues private/public key pair and a limited-time certificate with a unique identity for each node. For example, \mathcal{N}_A will receive an identity ID_A and certificate $Cert_A$.

An identity-based key exchange protocol based on bilinear pairing is used by ESIP. The protocol is efficient because two nodes can compute a shared symmetric key without the need for exchanging messages. Tp generates a prime \mathcal{P} , a cyclic additive group \mathcal{G} , and a cyclic multiplicative group \mathcal{G}_T of the same order \mathcal{P} such that an efficiently computable bilinear pairing $\hat{e} : \mathcal{G} \times \mathcal{G} \rightarrow \mathcal{G}_T$ is known. The bilinear mapping has the following properties:

- **Bilinear:** $\hat{e}(aP, bQ) = \hat{e}(bP, aQ) = \hat{e}(P, Q)^{ab} \forall P, Q \in \mathcal{G}$ and $a, b \in \mathbb{Z}_P^*$.
- **Non-degeneracy:** $\hat{e}(P, Q) \neq 1_{\mathcal{G}_T}$.
- **Symmetric:** $\hat{e}(P, Q) = \hat{e}(Q, P) \forall P, Q \in \mathcal{G}$.
- **Admissible:** There is an efficient algorithm that can compute $\hat{e}(P, Q) \forall P, Q \in \mathcal{G}$.

The bilinear mapping \hat{e} can be implemented efficiently using the Weil and Tate pairings on elliptic curves [2]. Tp selects a random element $\mu \in \mathbb{Z}_P^*$ known as the

master key, and computes the secret keys for the nodes based on their identities. The secret key for node ID_i is $Sk_i = \mu \cdot \mathcal{H}(ID_i) \in \mathcal{G}$, where $\mathcal{H} : \{0, 1\}^* \rightarrow \mathcal{G}$.

Each node, e.g., \mathcal{N}_A has to register with Tp to receive a unique identity (ID_A), symmetric key K_A , private/public key pair, a valid certificate, and the required cryptographic data to enable any two nodes to share a symmetric key. The symmetric key is used to submit the payment reports and the private/public keys are required to act as source, intermediate or destination node.

2.2 Threat and Trust Models

The mobile nodes are probable attackers but Tp is fully secure. The mobile nodes are autonomous and self-interested and thus motivated to misbehave to maximize their welfare and minimize their contributions. However, Tp is run by an operator that is interested in ensuring the network secure operation. As proven in [3], it is impossible to realize secure payment between two entities without involving a trusted third party.

The attackers have full control on their devices, and thus they can change their normal operation and obtain the cryptographic credentials. These strong assumptions are necessary due to using payment in the network. Non-participation in packet relay is not an abuse because the nodes are stimulated and not forced to relay others' packets with their own devices, but the large rate of packet dropping is an abuse due to disrupting the packets routing process.

Some attackers may act rationally by misbehaving only when they can achieve more benefits than behaving honestly. For example, they may attempt to attack the payment system to steal credits, pay less, and communicate freely. Some adversaries may report incorrect battery energy level to increase their chance to be selected by the routing protocol, e.g., to earn more credits. On the contrary, other attackers may act irrationally without considering their interests. For example, they may launch *Denial-of-Service* attacks by involving their devices in communication routes and dropping the data packets intentionally to break the routes. When an attacker \mathcal{N}_B receives packets from \mathcal{N}_A to forward to the next node in the route, \mathcal{N}_B drops the packets and keeps silent to let \mathcal{N}_A believe that \mathcal{N}_B is out of transmission range and the link between them is broken. The attackers may launch *Black-Hole* attack by continuously breaking all the routes they participate in. They may also launch *Gray-Hole* attack by intentionally breaking some routes and behaving regularly in other routes to circumvent Tp , but the ratio of the broken routes should be large to launch effective attacks. These attacks may be launched by compromised, malfunctioned, or low-resource nodes.

The adversaries may attempt to attack the trust system by launching *Trust-Boost* attack to falsely augment their trust and reputation values to escape the consequence of dropping packets or increase their chance to be selected in routes. They may also try to launch *False-Accusation* attacks to degrade honest nodes' trust values to evict them from the network.

The attackers may work individually or collude with each other to launch sophisticated attacks. The gained experience from the currently used protocols in civilian applications confirms that large-scale irrational collusion attacks are highly unlikely [4]. The trust/reputation systems are susceptible to the large-scale collusion attacks due to the nature of these systems. Our objective is to protect the payment against all types of collusion attacks, and protect the trust/reputation system against small-scale irrational collusion attacks and improve the system's robustness against large-scale attacks.

For the trust models, the nodes fully trust Tp to perform billing and auditing and trust calculations, but Tp does not trust any node in the network.

References

1. B. Wehbi, A. Laouiti, and A. Cavalli. Efficient time synchronization mechanism for wireless multi hop networks. *Proc. IEEE Personal, Indoor and Mobile Radio Comm. (PIMRC)*, 2008.
2. D. Boneh and M. Franklin. Identity based encryption from the weil pairing. *Proc. of Crypto'01, LNCS, Springer-Verlag*, 2139:213–229, 2001.
3. H. Pagnia and F. Gartner. On the impossibility of fair exchange without a trusted third party. *Technical Report TUD-BS-1999-02, Darmstadt University of Technology*, Mar. 1999.
4. C. Cachin, K. Kursawe, A. Lysyanskaya, and R. Strohli. Asynchronous verifiable secret sharing and proactive cryptosystems. *Proc. ACM Conference on Computer and Communications Security, CCS02*, pages 88–97, 2002.

Security for Multi-hop Wireless Networks

A. M. El-Bendary, M.; Shen, X.S.

2014, XIII, 99 p. 45 illus., 27 illus. in color., Softcover

ISBN: 978-3-319-04602-0