Content-centric Wireless Networking

Hanno Wirtz, Matteo Ceriotti, Klaus Wehrle
Chair of Communication and Distributed Systems (COMSYS)
RWTH Aachen University
{wirtz, ceriotti, wehrle}@comsys.rwth-aachen.de

1. MOTIVATION

Mobile devices, such as smartphones, provide a readily available basis for mobile offloading [2] and mobile applications [3]. Given the density of devices in urban scenarios, the key challenge is to discover and connect to devices participating in the same application, i.e., that provide or request *content of interest*. However, the *network-centric* design of 802.11 requires instantiation of and association to a network prior to communication, requiring iterative network associations and subsequent discovery. This is because, device and network discovery can not indicate content or application availability; conversely, content discovery requires a shared network. The associated time and communication overhead of trial-and-error associations thereby renders discovery of the right devices within an application impractical.

2. CONTENT-CENTRIC WIRELESS NETWORKING

We propose SO-Fi (Secure On-demand Wi-Fi), broadcasting content requests in standard 802.11 frames and only subsequently instantiating corresponding 802.11 networks at matching devices. SO-Fi consists of two parts:

Content-centric wireless networking: SO-Fi encodes content queries (cf. Figure 1, step 1) and broadcasts them in the SSID field of 802.11 Probe Request frames (step 2). At providing devices, SO-Fi encodes application content in a content table (step 0) and extends the 802.11 AP functionality with the ability to establish a network with SSID E^3 on-demand upon reception of a PREQ for E^3 (step 2) and a positive look-up of the content query in H (step 3). Resuming the 802.11 association process, establishing the network entails transmission of a PRES with SSID E^3 (step 9), triggering an association by the client to the AP at the providing device (step 10). SO-Fi thereby enables full and instant discovery coverage and is able to directly "pair" matching devices. Connecting requester and provider in a common network, at the cost of a single-step 802.11 association, mitigates time and communication overhead.

Security in content discovery and provision: SO-Fi incorporates offline established, use-case-specific security credentials k into requests to provide security functionality. Credentials can be application-specific passwords, keys, or iterative one-time tokens, e.g., cryptographic hash-chain elements. To authenticate, a requester XORs the request E^3 with the shared key (Figure 1, step 2). Providers reconstruct the request as [SSID $\oplus$ *key*], authenticates the requester using k, and eventually provides the associated content.

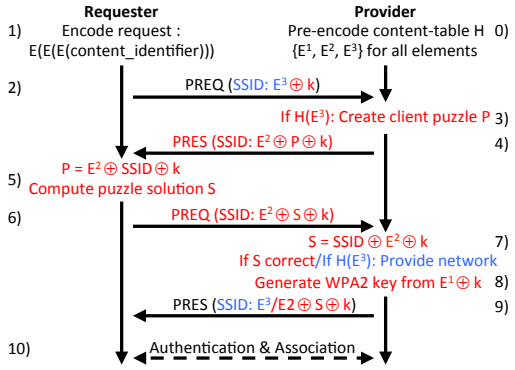

Figure 1: Content-centric wireless networking (blue), incorporating WPA2 network security and encryption as well as DoS protection (red) into an (two-step) 802.11 association mechanism (black).

Upon reception of an encrypted content identifier (Figure 1, step 6 with DoS protection, step 2 otherwise), devices generate a 802.11 WPA2 PSK using $E^1 \oplus k$ (step 8) as input to the 802.11 PBKDF2 function. Using this key, both requester and provider secure network access and encrypt traffic.

SO-Fi protects providers from DoS attacks via replayed content requests using *cryptographic client puzzles* [1]. When receiving $E^3 \oplus k$, providers generate a puzzle P (step 3) and pose this to the client in a PRES with SSID [$E^2 \oplus P \oplus k$] (step 4). The requester extracts P as [$E^2 \oplus$ SSID $\oplus k$], and computes the solution S (step 5). A PREQ with SSID [$E^2 \oplus S \oplus k$] (step 6) proves S to the provider, triggering the instantiation of a network for content provision (steps 7–9).

3. CONCLUSION

SO-Fi provides a novel building block for mobile applications and offloading approaches. Applications thereby can exploit SO-Fi to specify user- or event-triggered or continuous background discovery as well as alert the user of discovered content or users. Similarity preserving hashes as encoding functions may allow requests based on domain knowledge.

4. REFERENCES

[1] A. Juels and J. G. Brainard. Client puzzles: A cryptographic countermeasure against connection depletion attacks. In *NDSS*, 1999.

[2] Y. Li, G. Su, P. Hui, D. Jin, L. Su, and L. Zeng. Multiple mobile data offloading through delay tolerant networks. In *CHANTS*, 2011.

[3] K. Thilakarathna, A. C. Viana, A. Seneviratne, and H. Petander. Mobile social networking through friend-to-friend opportunistic content dissemination. In *MobiHoc*, 2013.