DECENTRALIZED RECONFIGURATION CONTROL

Rainer Falk (Siemens AG, Munich, Germany, rainer.falk@siemens.com)
Markus Dillinger (Siemens AG, Munich, Germany, markus.dillinger@siemens.com)

ABSTRACT

Reconfiguration allows adapting the configuration of a wireless communication device to reflect the current network conditions. When a user is roaming to different networks, this implies that the configuration if his reconfigurable device should by adapted to correspond to the currently used network. This paper describes approaches for decentralized control of the device re-configuration, allowing the modification and adaptation of the device configuration according to the preferences and current conditions of the currently used network.

1. INTRODUCTION

Reconfiguration is about the definition and adaptation of the configuration of reconfigurable devices to allow the optimized usage of different networks respecting their changing conditions as utilization, radio channel quality, or interference (software defined radio). The focus of this paper is on reconfigurable terminals used in a commercial environment comprising cellular networks as e.g. UMTS and public and private wireless networks (WLAN). Reconfiguration control is concerned about the authority to define the configuration that IS actually used at a certain point in time; that is it deals with the operational process of defining and modifying the device configuration. This is in particular challenging in decentralized reconfiguration scenarios where more than one party has a legitimate interest to influence a device configuration. In particular, in the roaming case the currently used visited network has an intention to modify the configuration of accessing devices. Access for modifying the device configuration needs to be established for the reconfiguration manager in the visited network. To ensure a correct and reliable operation of the whole reconfigurable communication system, also authorization of a piece of software needs to be investigated (secure download), defining which software CAN be downloaded securely, see [1].

This paper describes both central and distributed approaches for reconfiguration control in sections 2 and 3, and the usage of several configuration profiles to support distributed reconfiguration control in section 4.

2. CENTRAL RECONFIGURATION CONTROL

The simple case is where a single, central reconfiguration manager defines the device configuration. For example, the user's service provider (home network) wants to define and modify configuration parameters and install software updates (customer care).

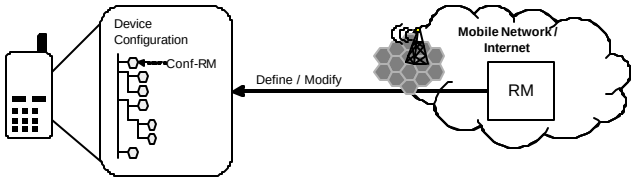

Figure 1: Central Reconfiguration Control

Figure 1 shows a reconfigurable device and its configuration, and a single central reconfiguration manager RM that defines and modifies the device configuration over the air. The reconfiguration manager could be part of the mobile network, or it could be located in the public Internet. The device configuration is represented as a management tree with leaf nodes representing configurable data as parameters or software modules. This structure serves only for illustration, the configuration data could also be organized in other ways. A part of the overall configuration is the configuration Conf-RM (address, cryptographic key and or password) related to the single trusted reconfiguration manager.

From a security perspective, it needs to be ensured that only the single trusted reconfiguration manager can actually define and modify the device configuration. This requires protection of the communication between the reconfiguration manager and the reconfigurable device (authentication of reconfiguration manager, optionally also authentication of reconfigurable device; integrity, possibly confidentiality of communication). The communication protocol between the reconfiguration manager and the reconfigurable device could be protected itself as e.g. in the case of SyncML Device Management [2], or it can be transporting over a secure transport channel, protected e.g. using IPsec or SSL/TLS [3].

On the end device, the configuration parameters Conf-RM (address, password/cryptographic keys) related to the

(single) trusted reconfiguration manager can be pre-configured by the service provider or device manufacturer, they could be configured manually by the end user, or the needed parameters could be configured on the device by sending a message (SMS, MMS) containing the configuration information.

3. DECENTRALIZED RECONFIGURATION CONTROL

The case that more than one reconfiguration manager wants to influence a device configuration occurs for example when beside the service provider also the currently used network (visited network) wants to modify the device configuration according to its needs, or when a device manufacturer provides customer care service (e.g. software update service) in addition to reconfiguration a service provider, or when the user's employer wants to manage the device configuration to install and manage company-provided applications. Decentralized or distributed reconfiguration control occurs however already when the configuration can be defined both using a local interface (setting by the user), remotely over the air, or when possibly contradictory configuration information can be set using different ways for provisioning, e.g. when parameters can be set both over-the-air and by data contained on a plugged-in smart-card as a SIM or USIM [4].

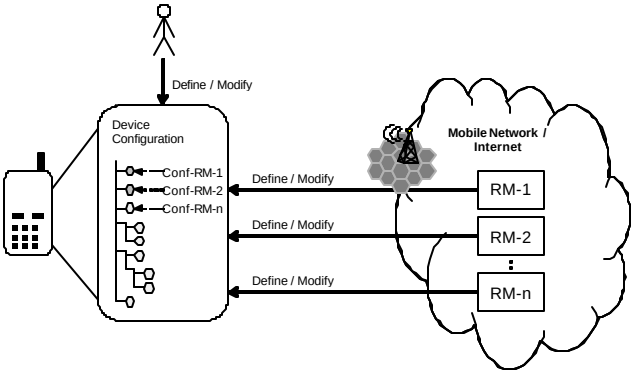

Figure 2: Decentralized Reconfiguration Control

Figure 2 shows the case where several reconfiguration managers RM-x define resp. modify the device configuration. These reconfiguration managers belong for example to the user's service provider, the currently used network, the enterprise network of the user's employer, or to the user's own home network. Also the user himself can define and modify the configuration of his device.

In general, the same reconfigurable device is used in different environments, e.g. in an operated cellular network that can belong to the user's service provider (home network) or a different network the user is roaming to (visited network), the user's home network, or the enterprise network. This implies that the device needs to be configured accordingly so that it can be used in these different environments. The device will have to hold several configuration profiles for the different networking environments that are defined by different stakeholders.

One objective of reconfiguration is the dynamic adaptation of the device configuration to correspond to the currently used network respecting its capabilities, preferences and dynamic properties as network load and radio link properties. This implies that the currently used network needs to have the possibility to modify the current configuration of accessing devices. As the user is roaming to different networks over time, different networks will get access to modify the device configuration. But this should be possible only as long as the user is roaming in those networks, or only to a configuration profile that is specific to that network (see section 4). A currently used visited network gets "temporal" access to modify the device configuration in addition to the "static" stakeholders as the user's service provider (home network) or employer.

The control on the device configuration by different networks leads to a specific security problem: The user attaches over time to networks that are trustworthy to varying degrees. Some might be trusted by the user or his reconfiguration service provider to operate responsibly and to perform only changes that are in line with their preferences and expectations. These networks could get increased degree of direct control on the device configuration. In contrast, less trusted networks like e.g. a public hot spot should only get the possibility to change the configuration of the user's device restricted to a safe sub-set that can hardly cause any harm. Furthermore, there is no fixed set of known reconfiguration managers that have the possibility to modify the device configuration. When the user is roaming to different networks over time, the reconfiguration manager of the currently used visited network has to be established so that it gets access to modify the device configuration.

The security requirements as in the centralized control case described in section 2 apply here to each reconfiguration manager. Additionally it has to be possible to give a reconfiguration manager only the possibility to modify a certain part of the overall configuration. Access control to management objects may be useful also for the case of a single, central reconfiguration manager. But it will be definitely required when several reconfiguration managers can modify the device configuration. Each reconfiguration manager gets only access to a sub-set of the overall reconfigurable functionality. An access control

mechanism enforces restrictions for read and write access to certain management objects; for parameters, even the allowable value range could depend on the reconfiguration manager.

The following subsections describe different ways how an additional reconfiguration manager could be established. This is relevant in particular in roaming scenarios where a user accesses over time different networks that have local reconfiguration managers, and the local reconfiguration manager shall be established so that it gets access for modifying the device configuration.

3.1. Independent Reconfiguration Managers

This case is similar to the case described in section 2 with a single, central reconfiguration manager. But here several of these central reconfiguration managers exist that are established independently from each other. Most probably, they will have different access privileges. For each reconfiguration manager, the reconfigurable device has to hold some configuration parameters (address, security material) as in the centralized case for the single reconfiguration manager. Furthermore, the reconfigurable device will need to manage and enforce access restrictions on the device configuration. This data would be established independently for each reconfiguration manager.

3.2. Establishment by a Reconfiguration Manager

A pre-configured reconfiguration manager (home network, service provider) establishes (delegates) responsibility to a different reconfiguration manager (e.g. in a visited network). The objective is that the local reconfiguration of a currently used visited network can modify the device configuration only when that network is actually used. The reconfiguration manager RM-H in the home network sets configuration settings on the reconfigurable device for a sub-ordinate reconfiguration manager RM-V in a visited network, comprising address, security material (keys or password) and the access control policy that defines what can be changed by RM-V, see Figure 3. This can be considered as a delegation of authority to perform certain kinds of reconfigurations by the home network towards a specific visited network. Exchange of signaling messages between these reconfiguration managers is required so that RM-V is informed about the respective security material. Additionally, RM-V could also inform RM-H about the changes it performed, or request profile and preference information related to the reconfigurable device. So in contrast to the case of independent reconfiguration managers, also an interface between reconfiguration managers has to be provided.

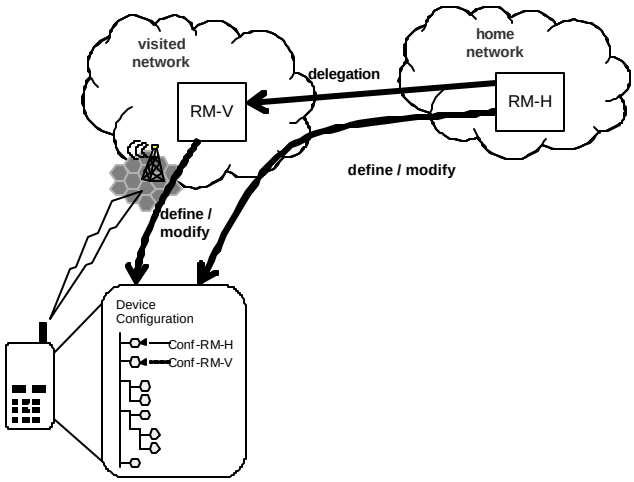

Figure 3: Delegated Reconfiguration Control

The main reconfiguration service provider in the home network or the user himself would set the reconfiguration policy for visited networks. This policy defines which changes a visited network can perform on its own. It is an access control policy that defines which (visited) network (subjects) may change what parts of the device configuration (objects). There could be a default policy that applies to all visited networks, and possibly specific policies for certain visited networks (e.g. preferred roaming partner). This allows giving increased control to some visited networks that are trusted to a greater degree.

When a specific visited network (RM-V) would like to perform a reconfiguration that it has not the authority to perform, it could still signal to the main reconfiguration manager RM-H the changes it would like to be performed. It lies then at the discretion of the main reconfiguration manager RM-H whether to modify the device configuration accordingly or whether to reject the request.

A local reconfiguration manager RM-V of a visited network could be added to the device configuration automatically when the user attaches to the visited network and registers with his home network, or it could be done only upon explicit request by the visited network. Besides adding a reconfiguration manager configuration, it is also needed to remove it once it is not needed anymore, i.e. when the current visited network is not used anymore. This could happen in a way similar to the addition: Either it is explicitly removed or deactivated by the main reconfiguration manager (home network) when the device de-registers from the current visited network or when it performs a hand-over to a different network. Alternatively, when the configuration is established for the new reconfiguration manager, it could be made in such a way that the

reconfigurable device automatically removes or inactivates this entry as soon as the device does not use the current visited network anymore.

3.3. Autonomous Establishment

In contrast to the case described above, a reconfiguration manager associated with the currently used network could also be established without the involvement of another reconfiguration manager.

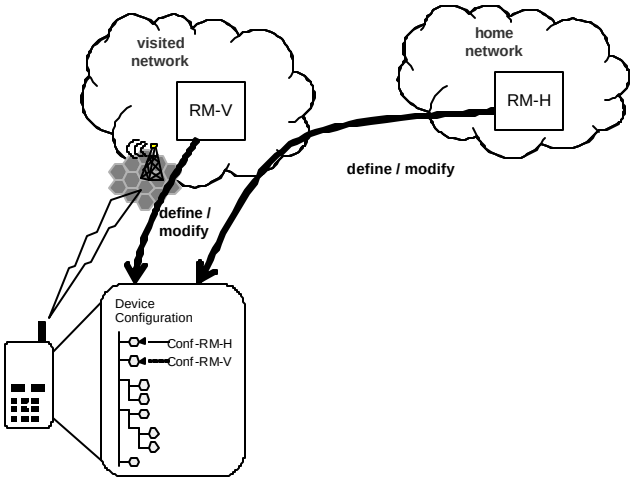

Figure 4: Autonomous Establishment of Reconfiguration Manager in a Visited Network

Figure 4 illustrates this case: In contrast to the case shown in Figure 3, here the reconfiguration manager RM-H of the home network is not involved in the establishment if the configuration information related to the reconfiguration RM-V in the visited network. The required information related to the reconfiguration manager RM-V of the currently visited network (address, security material, policy) is established autonomously between the reconfigurable device and the currently used visited network. The address of the reconfiguration manager RM-V could be discovered using e.g. DHCP (dynamic host configuration protocol) or SDP (service discovery protocol), or it could be implicitly known, e.g. when a specific, fixed local address is used to address the "local" reconfiguration manager RM-V, or when reconfiguration signaling is embedded in lower layer signaling messages (e.g. IEEE 802.11 management frames or UMTS Radio Resource Control RRC signaling) targeted towards the currently used visited network. Security material could be established using the 3GPP generic bootstrapping architecture GBA [5], or based on lower-layer signaling security. The GBA is part of Release 6 standards. It allows establishing a shared secret key between the mobile device and a server, re-using the available UMTS authentication and key agreement protocol and infrastructure. In this case, the secret key would be established between the mobile device and the new reconfiguration manager, allowing both to establish a secure communication. An access control policy would be needed that defines to which degree a currently used network can modify the device configuration, that is which parts of the device configuration can be changed by the new reconfiguration manager.

4. CONFIGURATION PROFILES

The conventional assumption is that the reconfigurable device hosts a single configuration that can be defined and modified. However, when a single device is used in different environments (e.g. public cellular, public hot spot, enterprise, home), different configuration profiles can be available for these different environments. Depending on the current environment, i.e. which network is used currently, the corresponding configuration profile is activated. Profiles are supported e.g. in Microsoft Windows XP where they allow to define different WLAN profiles to be used in different environments (e.g. home, enterprise, public hot spot).

4.1. Configured Configuration Profiles

Configuration profiles can be set-up and configured explicitly, that is by the end user or a reconfiguration manager.

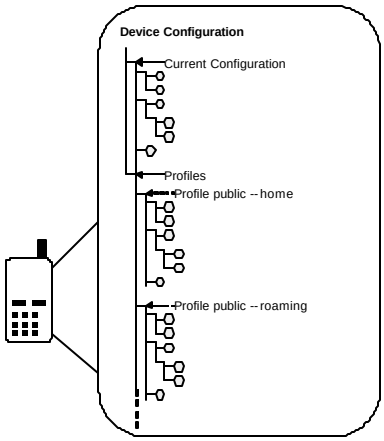

Figure 5: Configured Configuration Profiles

Configuration profiles are based on the distinction of the description of a configuration (profile) and the actual current configuration, see Figure 5. The overall configuration information includes the current configuration that describes the active configuration, corresponding to the currently active configuration profile,

and several available configuration profiles that can be activated. Also the conditions when to use which profile needs to be configured. In the example, only two profiles are shown for the case the device is using the home network or when it is roaming in a different, visited network.

4.2. Automatically Established Configuration Profiles

The concept of profiles maps well to distributed reconfiguration control: The settings are organized as profiles, and a specific reconfiguration manager can define and adapt only its "own" profile. To support reconfiguration in the roaming case, a new configuration profile can be established automatically as soon as the user is roaming into that network. There could be a single base configuration profile, or there could be several base configuration profiles to be selected from depending on kind of the currently used network. The configuration profile template would also define and restrict the modifications that a visited network can perform. So an automatically established transient configuration profile could modify parts of the overall device configuration only as far as allowed.

The reconfiguration manager in the currently used network can modify only this automatically configuration profile. This profile is active only as long as that specific network is used (transient configuration). As soon as a different network is used, the configuration profile corresponding to that different network is created and activated. When a currently used network makes changes to "its" configuration profile, these changes have an effect only as long that network is actually used. Automatically established configuration profiles can be preserved (cached) so that when the device is used later on with the same network, the proper configuration is already available. So the network is not required to perform parameter settings and possibly even software download again.

Figure 6 shows an example where the device configuration contains several profiles: A configuration profile serving as base configuration defined by the user's service provider (home network), and several automatically established configuration profiles for networks 1..n that the user has been roaming to. When for example the user is currently roaming in network-2, the current configuration, i.e. the actual device configuration, would correspond to configuration profile for network–2. The figure shows also a fixed failure mode configuration profile that would serve as fall back configuration should the adaptable configurations not work properly, see section 4.3.

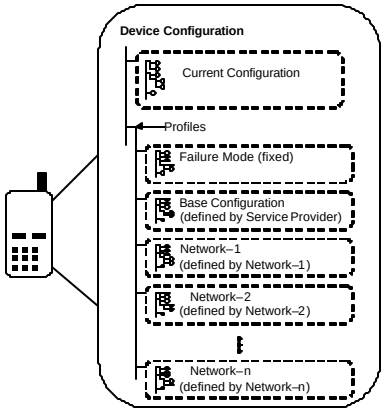

Figure 6: Automatically Established Network-specific Configuration Profiles

Specific here is that that automatically established, transient configuration profiles are bound to a specific communication network. They are created automatically as soon as that network is used, or as soon as that network performs a change of the device configuration. So the configuration profiles needs not to be established explicitly, but they are created automatically from a template when needed. However, the user's service provider could also pre-configure some network-specific configurations for preferred roaming partners, or it could pre-establish network-specific configuration profiles for networks that are a candidate for a hand-over.

Transient configuration profiles have in particular the following advantages: A specific network can modify only its "own" profile and has no possibility to negatively influence the device operation when used in another network. Furthermore, the configuration of a specific network can be "cached" by retaining the corresponding profile, so the next time the same network is used only the already existing profile has to be reactivated instead of re-defining all network-specific configuration elements. Additionally, the configuration of a specific network can be updated even when a different network is used. So a candidate network for a future handover can define all required configuration settings before the actual handover is performed, so that during the actual handover only the transient configuration profile corresponding to the target network has to be activated.

Using transient configuration profiles simplifies also the access control to the device configuration by a local reconfiguration manager in the currently used visited network: A local reconfiguration manager could update its profile arbitrarily, even when the corresponding network is not used currently. It is not required that a local

reconfiguration of a currently used network shall have the possibility to make changes to the device configuration only as long as that network is actually used.

This approach of transient configurations profiles increases the reliability and robustness: It is by design not possible that a specific network modifies the device configuration in a way that would have a negative effect when used in other networks. This allows in particular that even non-fully trusted or unknown networks can be given an increased degree of modifying the device configuration, as possible problems are confined to the time when that specific network is actually used. So the worst thing a specific network with a badly operating or malicious reconfiguration manager could achieve is that the user cannot use that network correctly. This is not worse than the case where a network itself is badly configured so that it would not provide the expected service.

4.3. Fall-Back Configuration Profile

A profile defines parts of the overall device configuration. But these are effective only as long as the corresponding profile is active. Also a fixed configuration profile could also be pre-configured as fall-back configuration to be used in the case of a configuration failure. When the device, user or the network detects that the device is not operating correctly in the current configuration, and if switching back to the base configuration does not help, there would be a further level of fall-back. Even when the base configuration profile would be badly configured so that the reconfigurable device cannot be used correctly, there is always a fixed configuration profile available that allows to establish limited communication, e.g. to contact a special fault management function in the network that tries to bring the modifiable configuration profiles (base configuration, further configuration profiles) in a correct state. So even in the case of a serious configuration error, the device needs not to be brought to a customer care center.

5. CONCLUSION

One relevant question is why decentralized reconfiguration control by a currently used visited network is needed? Simple cases as setting of configuration parameters and installation of a bug fix or of a new feature could be performed by a central reconfiguration manager. The more advanced – and complex – reconfiguration control comes with more sophisticated reconfiguration system architectures as those developed in the European projects SCOUT and E^{2}R where reconfiguration support functions are introduced in the system close to the reconfigurable device, on the one hand for efficiency (e.g. support for muss upgrades), on the other hand to have the possibility to perform dynamic adaptations to local conditions. The concept for network-specific transient configuration profiles allows a visited network to perform changes to the device configuration that are effective only as long as that network is actually used. As configuration changes do by design not have any influence on the configuration used with other networks, greater control can be given to visited networks without putting the correct and reliable operation in other networks at risk.

6. ACKNOWLEDGEMENT

This work has been performed in the framework of the EU funded project E^{2}R. The authors would like to acknowledge the contributions of their colleagues from E^{2}R consortium.

7. REFERENCES

[1] R. Falk, M. Dillinger: "Approaches for Secure SDR Software Download", Proc. of *SDR Forum Technical Conference*, Phoenix, Arizona, Nov. 2004.

[2] *SyncML Device Management Security*, Version 1.1, 2002-02-15. http://www.openmobilealliance.org/tech/affiliates/syncml/

[3] R. Oppliger: *Security Technologies for the World Wide Web*, 2nd Edition, Artech House, Norwood MA, 2003.

[4] Open Mobile Alliance: "OMA DM - 3GPP alignment for SC provisioning", *OMA-DM-2004-0131-OMA-3GPP_SC_Alignment*, 14 June 2004. http://member.openmobilealliance.org/ftp/public_documents/dm/2004/OMA-DM-2004-0131-OMA-DM-3GPP-alignment-for-SC-provisioning.zip

[5] 3GPP: "Generic Bootstrapping Architecture", *3GPP TS 33.220 V6.2.0*, June 2004. http://www.3gpp.org/ftp/Specs/archive/33_series/33.220/33220-610.zip

[6] IST-SCOUT "Architecture, Functions and Security Analysis and Traffic Management Schemes for IP-Based Mobile Networks and Re-configurable Terminals in Cellular and Ad-Hoc Networks", *IST-SCOUT Deliverable D4.1.2*, 2004. http://www.ist-scout.org/

[7] IST-E2R "End-to-End Reconfigurability", Project Web Site, http://www.e2r.motlabs.com/