Use Case Study on Embedded Systems Serving as Smart Home Gateways

PAVEL MASEK\(^1\), JIRI HOSEK\(^2\), MICHAL RIES\(^3\), DOMINIK KOVAC\(^4\), MILAN BARTL\(^5\), FRANZ KRÖPFL\(^6\)

Department of Telecommunications, Faculty of Electrical Engineering and Communication\(^1\)\(^2\)\(^3\)\(^4\)\(^5\)\(^6\)
Brno University of Technology
Technicka 12, 61600 Brno
CZECH REPUBLIC

Telekom Austria Group\(^6\)
Lassallestraße 9, A-1020 Wien
AUSTRIA

\(\text{xmasek12@phd.feec.vutbr.cz}\)\(^1\), hosek@feec.vutbr.cz\(^2\), ries@feec.vutbr.cz\(^3\)
\(\text{xkovac23@phd.feec.vutbr.cz}\)\(^2\), xbartl02@stud.feec.vutbr.cz\(^5\), franz.kroepfl@telekomaustrlia.com\(^6\)

Abstract: - The telecom providers are deploying new internet protocol multimedia subsystem with emerging the 4th generation network infrastructure. In parallel, the smart home infrastructures (smart metering, alarm systems, etc.) with extensive communication capabilities are massively deployed. This indicates technological readiness on both sides; home infrastructure and telecommunication operator. Finally, it is necessary to bring solution for smart home gateway which will reflect the actual regulations, recommendations, will not generate additional costs and provide user friendly environment. This work presents use case study of utilization of smart home infrastructure with telecom provider infrastructure for alarm systems.

Key-Words: - Alarm System, FXS, IMS, M2M, SIP/SIMPLE, Service Virtualization, Smart Home Gateway

1 Introduction

The traditional human generated communication is sustainably growing [1]. In contrast to human generated traffic, the machine to machine (M2M) technologies are massively emerging. The M2M communication is considered as a form of data exchange that does not require human interaction [2]. The Cisco report [1] estimates 1.7 billion M2M devices/connections spread world wide by 2017. Such massive growths of M2M introduce new challenges for telecom providers. The initial question for the most of them is, if it is feasible to use existing network infrastructure and actual deployed platforms for M2M typical use cases. The Internet Protocol Multimedia Subsystem (IMS) with the SIP (Session Initiation Protocol) as a key component, which is already widely deployed within 3rd and mandatory for 4th generation of mobile networks, seems to be suitable serving platform with good quality of service (QoS) performance [3].

The Smart – Home GateWays (SH-GW) represent one of the typical use cases. SH-GW should serve as gateways for smart home appliances (e.g. smart sensor / actuators) and in parallel provide certain level of security.

The second valid question is, if there is already widely deployed device which can serve as residential (access) gateway (interface technology). The answer for the last question brings the state of the art IP routers based on open embedded operation systems (e.g. OpenWRT). These routers have sufficient processing power and in parallel are already adapted to actual telecommunication infrastructures and services (e.g. they can play a role of SIP clients).

Since the SIP architecture can be easily utilize to provide communication platform for new emerging M2M services, the middleware between SIP components and SH-GW seems to be only missing part within this concept. In order to cover wide spectrum of M2M requirements for our study, the use case with requirements for end to end line
control, actual status update, instant messaging and secured authorized connection was selected. Therefore we decided to demonstrate applicability of these requirements in our use case which utilizes the alarm system with PSTN connectivity, SH–GW (IP router) and IMS infrastructure. In addition, the selected use case should demonstrate the potential solution for provisioning of new SIP based alarm receiving centre (ARC).

The final and maybe the most important question is if such solution generates additional investments to network infrastructure or to end user infrastructure. Therefore, the proposed solution should minimize additional costs.

The rest of paper is organized as follows. The Section 2 describes general concept of alarm use case and all its functionalities. The next Section 3 presents the design and implementation of proposed SIP-based solution for alarm system handling SH-GW. The final analysis of presented use case study and also the potential of existing telco network infrastructures serving as a communication platforms for emerging M2M services are provided in the Conclusion.

2 Alarm Use Case Concept

Our goal was to develop functional demonstrator for the service category "ALARMS" where the router with FXS (Foreign eXchange Station) port is considered as smart home gateway (SH-GW). Such demonstrator should be able to process and forward alarm events from any alarm system with PSTN (Public Switched Telephone Network) connection (with and without dual tone multi frequency (DTMF) signalling functionality). The alarm events are forwarded in form of SIP messages to the ARC or directly to end users. Moreover, the demonstrator should be able to distinguish the alarm system status and notify it to the end user [4].

The SH-GW detects all messages incoming from the alarm system through FXS interface and informs about these security events all relevant persons (end user, alarm service provider, etc.) and/or other systems within the Smart Home Domain (see Fig. 1).

The SH-GW acts as a gateway between alarm systems or sensors and the user. The SH-GW can interface with the installed alarm systems (burglar alarm, fire alarm, etc.), but can also interface directly with the respective sensors, e.g. with fire sensors or door sensors. When connecting to alarm systems, the SH-GW acts as aggregation and mediation service whereas when connecting sensors directly to the SH-GW, the SH-GW integrates the “alarm system” functionality itself. In both cases the SH-GW needs to have an “alarm interpretation logic” which decides the next steps (e.g. notifying the user or security service provider) [4].

The middleware alarm-handling system running on the SH-GW must not have any influence on local alarm signals like flash lights and horns. Thus, even if all broadband connections or monitoring functions of the SH-GW failed, the local alarm signalling should be still working. Besides that, line monitoring function should be also implemented to detect any problem with the link between alarm system and SH-GW, e.g. attempted sabotage.

The Internet access for the SH-GW is either provided by external devices (e.g. DSL modem or 3G/4G USB modem), by communication devices / interfaces integrated directly into the SH-GW or by any combination. So, the alarm use case demonstrator should be the Internet connection type independent solution. There are no special requirements for WAN (Wide Area Network) connection. It is just a service-enabling tool to communicate with SIP servers and other relevant parties.

2.1 Alarm System Communication Protocols

As alarm systems use various protocols and techniques for alarm notifications the SH-GW needs to understand a variety of these protocols and map them to the single “back-end” protocol.

During the development of our demonstrator we were focusing following three alarm systems with different signalling techniques. There was one common characteristic of all systems that the alarm
events were transferred via analogue telephone line (PSTN connection).

The first examined alarm system was based on very simple mechanism where the events are invoked only by changing the state of an analogue 2-wire circuit. This can be either by increasing/decreasing the power level or by open/closing a switch and thus changing the state of a current loop. This system is sometimes referred to as a “hook-on / hook off” alarm system. In this case, SH-GW should be able to detect any change of the state of a phone line loop.

The second alarm system has a "phone" included and may call certain numbers and signal events by playback a predefined voice sample. If such an alarm system is connected to an FXS port, the SH-GW shall interpret the call attempt as an alarm. In this case, the attempted call is terminated inside the SH-GW.

The last alarm system included in our study has also the phone module, but in addition it supports the Contact ID (CID) protocol [5] which is widely used and acknowledged alarm protocol using the DTMF signalling tones. In case of security event, the alarm system is dialling predefined phone number followed by a CID code (in form of a combination of DTMF tones) which represents specific type of alarm event. The structure and meanings of CID codes are defined by standard [5]. When connecting this CID-based alarm system to the FXS interface, the SH-GW should provide the functions for detection of these specific CID codes. After that, the decoded alarm message is sent as a SIP message to the destination node.

Further, there are also some alarm systems which support alarm signalling directly via TCP/IP connections, defined e.g. in the ANSI/SIA DC-09-2007 [6], but these systems were not the subject of our use case study.

2.2 Alarm System Status Notification
Since the alarm systems present complex security solutions, there is a serious need to monitor not only the specific alarm events but also the status if even the alarm system is running correctly. Therefore, the SH-GW has to be able regularly checking the status of alarm system and report any changes.

To treat with the loss of power supply or broadband connection, the whole monitoring system has to notify if the SH-GW is running or not. The implementation of SIP-based status notification within our developed demonstrator is described in the Section 3.2.

3 SIP based solution for Alarm System Handling SH-GW
In order to satisfy all defined requirements for the alarm use case demonstrator, the middleware application was developed. This application is running on the OpenWRT-based SH-GW and is serving all alarm system handling functions to detect and decode alarm events coming from all types of alarm systems described in the previous section. The flowchart of developed alarm application is shown in Fig. 2.

Whole designed system is composed of several interconnected functional blocks. Each block is dealing with specific task or set of tasks. Since the application is started, there is function listening on the FXS port of SH-GW and detecting any activity on this port. If the hook on/off state is detected (which means that alarm system is trying to establish a call and transfer alarm message), another function providing detection and storing of DTMF tones is activated. When all DTMF tones (if any) are stored, the conversion to ASCII characters is provided. The result of the conversion is compared...
to known CID codes and type of alarm message is interpreted. The final functional block of proposed middleware is ensuring the formation of SIP message including decoded alarm event and the sending of SIP message to the end system / user.

Due to presented differences between described types of alarm systems there are some distinctions in the implementation of alarm events detecting functions. In the case of simple Hook on/off alarm system which does not send any DTMF tones, all DTMF and CID related functions are skipped and the SIP alarm message is sent immediately when the hook on/off state is detected.

On the other hand, in case of alarm system using the DTMF and CID signalling, additional handshake procedure has to be provided. This handshake process is originally used for the establishment of connection between the alarm system and alarm receiving centre. It is composed of the sequence of DTMF tones with specific frequencies and time breaks between starting with the kiss-off tone of frequency 1400Hz (see Fig. 3) [5]. When the handshake procedure is finished the alarm system can start sending the CID codes to ARC. To be able detect CID codes at SH-GW side we implemented the handshake procedure into our middleware application and thus provided the virtualization of ACR on SH-GW.

Since the general SIP architecture is using SIP servers as intermediate nodes between two SIP clients where all SIP traffic is forwarded through these servers, the designed SH-GW’s middleware is operating like one SIP client which is sending messages (including alarm events) to another SIP client (e.g. at alarm receiving centre) via defined SIP proxy server.

The secure communication is very important in all modern network services and it is even more important in case of security applications like alarm systems. Therefore we implemented security mechanisms commonly used with the SIP. During the initial phase when the SIP client is registering to the server, it is very important to provide an authentication method [8]. We have used the HTTP Digest Authentication [9], which is a simple challenge-response authentication protocol used for authentication of users in SIP architecture. It uses one-way hash function (e.g. MD5). The same authentication function was used also when the SIP message or status notification were sent to the SIP server. The implemented authentication of communication parties provides the protection against the replay attacks. In order to check if the SIP message was not corrupted or intentionally modified during the transmission the MD5 hash function is utilized. The hash is computed for each SIP message before it is sent towards the server.

The implemented SIP communication message flow including the authentication procedure between the SH-GW and the SIP server (part of a telco operator infrastructure) is shown in Fig. 4.

### 3.2 Implementation of SIP-based Alarm Event State Signalling

As it was already mentioned, it is really important not to only monitor the alarm messages but also the status of alarm system and also the SH-GW providing all alarm-related functions. The SIP protocols is suitable communication platform even enough for the notification about status changes because it supports the signalling of current state of SIP users through it extension defined in [10]. The utilization of this standard mechanism keeps zero additional requirements for the network infrastructure.

We implemented the status control function for our SH-GW which is regularly (every half a second) checking the current status of alarm system (and SH-GW as well) and notifying any change. The

**Fig. 3: Handshake process between DTMF alarm system and SH-GW**

<table>
<thead>
<tr>
<th>DTMF alarm system</th>
<th>1400 Hz</th>
<th>100 ms</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIGNAL STOP</td>
<td>2300 Hz</td>
<td>100 ms</td>
</tr>
<tr>
<td>SIGNAL STOP</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**3.1 SIP Implementation**

Our implementation of SIP protocol inside the SH-GW strictly follows the standard defined in [7]. Therefore, there are no additional requirements to modify actual SIP infrastructure provided by telecommunication network operators.
identified statuses are sent to the server inside the SIP PUBLISH messages.

To distinguish different states of the alarm system and SH-GW we adopted four following SIP statuses well-known from e.g. SIP-based instant messaging.

For the notification about the state when SH-GW is switched off (e.g. due to loss of the power supply) or the network connection is not working properly we are using the “offline” status (black status icon in SIP client, see Fig. 5). The state when the SH-GW is running and the alarm detecting middleware application is activated is notified by the “online” status (green status icon, see Fig. 5). If the alarm system is armed, the status is changed to “away” (orange status icon, see Fig. 5). The last state when the SH-GW is active and alarm event within alarm detecting function is triggered is represented by “busy” status (red status icon, see Fig. 5).

By the help of this event state signalling functionality, whole system is continuously under the control and changes of behaviour are immediately reported to the relevant person.

<table>
<thead>
<tr>
<th>SIP/SIMPLE original statuses</th>
<th>SH-GW’s state</th>
<th>Alarm system’s state</th>
</tr>
</thead>
<tbody>
<tr>
<td>Offline</td>
<td>Switched of or some connection / power supply issue.</td>
<td>Unknown (SH-GW is not running).</td>
</tr>
<tr>
<td>Online</td>
<td>Switched on / running in monitoring mode.</td>
<td>Alarm system is running in unarmed state.</td>
</tr>
<tr>
<td>Away</td>
<td>Switched on / running in monitoring mode.</td>
<td>Alarm system has been armed.</td>
</tr>
<tr>
<td>Busy</td>
<td>Switched on / running in monitoring mode.</td>
<td>Alarm has been triggered.</td>
</tr>
</tbody>
</table>

Fig. 5: Alarm system event status notification

### TABLE 1: Look-up table for status events

4 Conclusion

The smart home gateways are gaining interests of broadband service providers, mobile and fixed network operators, equipment vendors, device manufacturers, as well as research and
standardization bodies. Therefore, our work tries to demonstrate suitable solution based on actual state of technology for use case with wide spectrum of requirements on one side. On other side, our solution extends actual state of art with demonstrating potential of middleware solutions.

The developed middleware does not increase hardware requirements and follows the SIP security standards. This is demonstrated at utilization of smart home infrastructure with IMS infrastructure for service category alarms. The demonstration shows the potential of virtualization of alarm receiving centre at SIP platform. Furthermore our solution provides cost efficient design which does not introduce additional costs at network infrastructure and is based on already deployed residential access technologies.

Acknowledgement

The authors would like to thank Telekom Austria Group for supporting their research, since the views expressed in this paper reflect some of the strategic visions within the Telekom Austria Group. The described research was supported by the project CZ.1.07/2.3.00/30.0005 of Brno University of Technology and performed in laboratories supported by the project SIX, CZ.1.05/2.1.00/03.0072, the operational program Research and Development for Innovation.

References: