A Framework for Smart Home Services with Secure and QoS-aware Communications

Markus Hager, Sebastian Schellenberg, Jochen Seitz, Sebastian Mann, Gunar Schorcht

***Abstract*—The scenario of smart home services will be discussed with regard to two important aspects: the quality of service problem for the in-house communication and the need for a security scheme for the whole system. We focus on an installation with smart computers in each flat interconnected using a switched Ethernet network. These smart devices are responsible for performing local services, user control and operate as a gateway for the different types of sensor and actor networks installed at each flat. We propose a QoS scheme to prevent congestion situation for the Ethernet network which is applicable to currently available cost-sensitive hardware. Furthermore, the whole system, all communication channels, user data and the access to the framework are secured by our proposed security architecture. Finally, we will present the latest improvements on Ethernet network standards, the ongoing work on this topics and our next steps for future work.**

***Keywords*—smart home, quality of service, Ethernet, security**

I. Introduction

Smart home services (SHS) are software modules that expand the concept of the home automation scenario. The idea is to do more than just switching the heating operation status, based on the available temperature sensor information. To create a smart home, the necessary basis are different sensor units collecting as many information as possible and actors to perform the desired actions. Due to the fact, that there is no base technology comprising sensors and actors for all of the comprehensive use cases, there is the need for a solution, that offers the possibility to integrate the different sensor and actor networks into one system. This was one of the main goals of the SHS research project [1]. There are also some products which are established in the market like the "ViciOne" home and building automation system [2]. For the rest of the paper we will use the HAM (home automation module) notation, used by [3] as name for their developed automation computer unit as a placeholder for similar technologies like this, allowing to realize the interconnection of different sensor and actor networks.

The advantage of such a solution is that all information about the state of the house or flat is now available at one central point. This offers the chance to combine the data of the installed technologies to realize better services, known as smart services. This means for example that the heating control is no longer just based on the temperature sensor, also the information if a window is opened, someone is inside the room and maybe also the weather forecast is taken into account to make a better decision for how the heating should be controlled. Also, the recorded history could be used to make a prediction which could be useful if the costs of a resource varies over time.

Such systems make it more comfortable to live in those houses and therefore the current focus in the already mentioned SHS research project is to adapt these concepts for housing associations. This cannot be done by a simple expansion of the system, because a larger network must be established, it must use standard low cost hardware and especially the control and the data of the system must be secured. As we know, the existing systems are either designed for private houses and/or have no special security and quality of service concept. Due to that, in this paper we present our solution offering a security and quality of service system for this scenario.

Fig. 1 shows an example of a typical SHS network. The mentioned HAM units are installed in each flat and are interconnected with Ethernet, because it is one of the main network standards and highly available, cost efficient and guarantees a simple installation. The HAM units have a touch screen to give the user the chance to interact with the system. Moreover, a NAT gateway with Internet connection gives the user the option to get Internet access based on the installed network. Further applications like VoIP phones or other multimedia devices could also use the network. Finally, the HAM units are controlled and administrated by a central server which could be part of the network or a computer from the Internet.

II. Related Work

A. Security

There exists a variety of different home automation systems. All these systems have in common, that they are interchanging information and personal data via unsecured communication channels. If a malicious intruder has access to these data, he is able to obtain a complete picture of the regarding individual. It is possible to gather information of the private behavior, of the presence in the flat or of Internet usage. To prevent this leakage it is necessary to secure these data concerning information interchange, access, storage and processing. Furthermore, it is necessary to check the authentication of the participating entities and the integrity of each delivered message to ensure that the received message is sent by the claimed originator and is not altered.

M. Hager, S. Schellenberg, J. Seitz are with the Department of Electronic Engineering and Information Technology, Communication Networks Group, Ilmenau University of Technology, Germany,
e-mail: (see http://www.tu-ilmenau.de/kn)

S. Mann, G. Schorcht are with the Department of Applied Informatics Research Laboratory, Erfurt University of Applied Science, Germany,
e-mail: (see http://www.ai.fh-erfurt.de)

Manuscript received October 26, 2012; revised December 18, 2012.

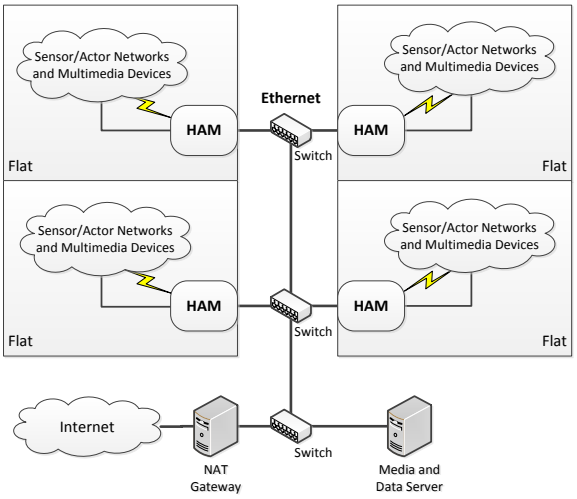

Fig. 1. Structure of the SHS network.

There are many different ways to secure each of these aspects. To secure the storage or the data interchange it is possible to encrypt the data, so that an eavesdropper is not able to retrieve the data. But this leads to a new problem, the key exchange management. How to provide the encryption keys to the eligible entity?

Some exemplary home automation systems are ”Smart Home”, ”Smarter Wohnen ®NRW”, ”SerCHo” and ”ViciOne” (see [2, 4–6]). All of these existing security concepts for home automation systems are having one problem in common. All of them are providing some singular security features, but there is no comprehensive concept, which fits to all of the named aspects. Only ”ViciOne” provides a comprehensive home automation system, with a security concept. This concept provides many security features, but some important features, like authentication of users and devices, are missing. All of them are isolated applications for each regarded system.

B. Quality of Service

Every quality of service solution is mainly designed based on the used hardware and due to the fact, that switched Ethernet is used for the SHS network, we will only focus on solutions based on this technology. Furthermore, quality of service is a collective term for many aspects classifying a connection. In the SHS scenario, the most important aspects are the available data rate for an end to end connection inside the SHS network and the delay and/or the jitter for this connection.

Moreover, a separation based on the different services running on the HAM units must be done, because on the one side we have applications with high priority, for example the message of a smoke detector or some administration commands and on the other side less important data streams like the heating control communication or the Internet session of a user. Ethernet offers a well-known scheme to mark each packet either in the type of service field of the IP header or in the QoS field of the Ethernet frame (see IEEE 802.1Q or IEEE 802.1p) to allow the network components to handle packets with a certain priority in a preferred way.

However, there is one main problem concerning these concepts: if there are more packets arriving at a switch than it can handle, some packets still get discarded due to buffer overflows. This could affect UDP streams because there is no flow control mechanism like TCP streams have. Therefore, a quality of service concept has to be developed based on traffic shaping, that avoids congestions at any point inside the smart home network.

AVB (audio/video bridging [7]) is one concept, to expand the behavior of standard Ethernet. The main idea is to use a similar mechanism as in the case of the RSVP (resource reservation protocol). Before establishing a new connection, every switch for this connection gets a request and checks whether or not the necessary resources are available. This is a suitable solution for some cases, but has also some disadvantages: special AVB switches are required and there is no scheme implemented, that adapts the different data streams, if the requested resources are not obtainable. Finally, the applications must support these requests.

Therefore we think, the access to the network must be managed based on the applications, the destination of each communication session and the current status on each link of the network for these data streams. [8] demonstrates how traffic shaping could be applied, but the presented solution is designed for virtual machines and the network topology is not taken into account. Besides, there are a lot of other publications, e.g. [9, 10], but after all we have not yet identified one concept that fulfills all our requirements:

- guaranteed and/or best effort data rate for individual applications
- consideration of the network topology
- avoidance of network congestion for end-to-end communication
- integration of standard off-the-shelf switches
- no changes to the network stack
- no special requirements for the behavior of the applications

In the following sections we will present our solution, first the security architecture and finally the quality of service scheme for the SHS network scenario.

III. Contribution of our Work

The main contribution regarding the security architecture is the new combination of different approaches working cooperatively together to address the security aspects of the smart home scenario. This includes as starting point the collection of important threads and results, in combination with the role based access system, in a complete overview of the security problem. Our solution is designed in view of this analysis and evaluated with respect to the different hardware and software elements which are part of a smart home system. Furthermore, the QoS system realized by a middleware addresses the requirements pointed out in the previous subsection, whereas the most important requisites are a cost-sensitive installation and a framework without an

additional interface to the applications running on the HAM units. Finally, some alternative approaches regarding QoS will be separately discussed in section VI.

IV. Security Architecture

Regarding the problem, that there is no all in all security concept, we developed such a concept in the SHS research project. We propose a complete and comprehensive security system with features for each single application of the SHS system, by providing a new combination of commonly known security features (e.g. encryption, hashing) together with new, improved or adapted features (e.g. authentication, role-based access). This includes features for encrypting transferred and stored data, to authenticate each participant and for a role-based access-system to restrict access to all the data and functions of the system. We also performed threat modeling to identify the most common security threats to the system and developed solutions for these threats.

A. Threat Modeling

Threat modeling is a common method to identify and evaluate all potential threats of a system. The procedure is to identify the threats and visualize them in a threat matrix. The most dangerous of them are chosen to build threat trees to give an overview about the reason of the threat. Furthermore, all security assets and security leaks are identified and possible attack scenarios and corresponding countermeasures are shown.

Threats: Some of the identified threats of the provided system are:

- physical threats like vandalism, burglary, theft of devices
- theft of passwords
- intentional disclosure of administrator passwords
- hacking of accounts, passwords or ciphers
- phishing of information
- spoofing within authentication procedures
- intentional backdoors in external code
- denial-of-service attacks, remote control of devices
- computer viruses and the like
- misuse of administrative privileges
- denial of information

These threats are just the most common, of course there are more threats or attacks possible, but they are more unlikely or they do not harm that much. All of these threats were analyzed and rated, in order to compare threats. In our analysis, we identified phishing as the most likely and breaking a cipher as the most harmful threat. In the following we will exemplarily analyze the threat of breaking a cipher.
Hacking of a cipher has an enormous damage potential. In the worst case the adversary gets all information, which are sent over the network. This contains user names and passwords as well as all necessary authentication information. So it is conceivable that the attacker gets root permission to the system. In the worst case, which means that there is no reissuing of keys and no random numbers are used (depending on the cipher), this attack is repeatable at any time. Only highly skilled programmers could perform this attack and tools are only useful if the security architecture has some significant weaknesses. So the probability of this scenario has to be put on a medium level. Depending on the location of the attack, e.g. within a flat, at a NAT gateway or at a HAM, some single user might be affected up to all users and the provider. This attacking scenarios is usually discoverable by the leak of sensitive information. After a successful attack it is possible, that the users lose their trust in the system and in the worst case there is a possibility of legal consequences. Summarizing this, hacking a cipher is the most harmful threat with inestimable consequences. There are different vulnerabilities to perform this attack. The key length has to be chosen depending on the available resources and is hence not necessarily optimal to security. Another weakness is the key management, as in some cases it is possible that unauthorized persons could find out the keys. The most common way to break a cipher is the brute force attack, where every possible key is sequentially checked. An improvement is the dictionary attack. Other, more sophisticated, attacks are: man-in-the-middle attack, linear and differential cryptanalysis or other algebraic attacks. The most useful countermeasures are extending the key length (regarding the resources), the use of a key management system, like DHKE.

Security Assets – A main part of our research was to identify all security assets of the given building automation system. Assets define all system features, processed data and system functions which have to be protected against attacks. Those security assets are:

- confidentiality – all personal data in the system has to be confidential, i.e. data has to protected against unauthorized access and it has to be assured, that only the designated receiver can read the data.
- authenticity – it has to be assured that received data are originated by the claimed sender, i.e. the sender's authenticity has to be ensured.
- accountability – it must be possible to identify the responsible entity for each incident.
- integrity – unintended and intentional data altering have to be recognizable or preventable. Therefor it is necessary to identify the originator of data uniquely.
- availability – the system's inherent services and functions have to be available and have to work correctly.
- controlled access – only authorized entities are allowed to access services, functions and data.
- anonymity (pseudonymity) – personal data has to be pseudonymized. This means, that it is not possible to associate personal data to a single user, even if there is an unauthorized access.
- impossibility of finding linkage of intercepted data – all data, processed in the system, have to be encrypted in a way, that it is not possible to determine connections between the data and the system status. E.g. it should not be possible to create a presence profile based on intercepted radiator usage data.
- robustness – the system has to be robust against faults,

that means that the system has to work properly even if some instances have malfunctions.
- physical safety of devices – it is also important to ensure the physical safety of all devices, because all functionalities of the system depends on the correct behavior of the devices. However the physical safety is no part of the security architecture. For example the physical safety can be improved by using backups of the devices and servers.

B. Encryption Features

The proposed security architecture provides a combination of features for encrypting transferred and stored data, management of key exchange and to ensure message authentication, while being liable to severe restrictions of computing power, because most of the used devices are embedded systems with low resources. There is no security architecture, which combines security features for all kind of devices and all parts of a home automation system. Due to the ressource restrictions we can use neither asymmetric ciphers nor a complete public key infrastructure. We provide two different ciphers, which can be used within the system. Those ciphers are AES128 (Advanced Encryption Standard with 128 bit key length, see [11]) and RC4 (Ron's Code Nr. 4, see [12]). We recommend the use of RC4, because it is more secure and faster than AES128, but AES128 is a more widely spread standard. Of course there are many other encryption standards, but they all have crucial disadvantages like lack of security, high performance needs or they are not supported by most manufacturers.

Symmetric ciphers work with one key for both participants (sender and receiver). The main problem is how to provide this key to both parties. It is insecure to send the key in plain text over an insecure channel and it is impracticable to commit the keys personally. So there is a need for a key exchange management. We provide a common procedure for secure key exchange, the Diffie-Hellman Key Exchange (DHKE, see [13]). The DHKE establishes a shared secret, which can be used for secret communication.

The security of the DHKE is based on the discrete logarithm problem, which makes it hard to compute g^{ab} from given g^a, g^b. This key exchange is used to provide keys between parties, which communicate bidirectionally. This comprises user, operators, provider and all devices, that are able to communicate bidirectionally. To provide keys to unidirectionally communicating devices, the key is stored at the device during the manufacturing process and, after putting into operation manually, provided to other parties. In order to provide as much security as possible, a periodic key renewal is necessary. This is only applicable with bidirectionally communicating devices by using the key exchange method again.

As mentioned above we use AES-128 as encryption method, so we need symmetric keys of 128 bit length. Referring to [14] and [15] we need the public DH-parameters p (prime number) and g (primitive root) as well as the private DH-parameters a and b (private random numbers). The requirements to this parameters are shown in table I.

In [15] it is shown how to extract a 128 bit shared key. A symmetric key of 128 bit length is equivalent in strength to a 3072 bit asymmetric key, as claimed by RSA Security in 2003 (see [16]). An asymmetric key length of 3072 bit should be used if security is required beyond the year 2030.

Due to known problems of DHKE, e.g. the possibility of a man-in-the-middle attack (a man in the middle masquerades himself as Alice and Bob and performs two distinct DHKE, so he is able to decrypt and re-encrypt messages), it is necessary to provide advanced versions of the DHKE. A possible countermeasure for man-in-the-middle attacks is the use of an authenticated DHKE, or station-to-station protocol (STS, see [17]). The STS-protocol is based on the classic DHKE and its security is also based on the discrete logarithm problem. As distinct from DHKE, the STS-protocol uses an asymmetric key pair for each party to sign the key exchange process. This advancement results in a mutual authentication of each other, that means the originator of a message within the key exchange is the claimed one and there is no man in the middle. The disadvantage of the STS-protocol is the additional computational cost. Therefore, we provide both methods, the classic DHKE for devices with high resource restrictions and the STS-protocol for devices with more available resources .

Besides encryption and key exchange, we provide a feature to ensure message integrity. Therefore, we use special message authentication codes, so called cryptographic hash algorithms. We provide two different hash algorithms, the widely known SHA-1 (Secure Hash Algorithm Nr. 1, see [11]) and the RIPEMD128 algorithm (RACE Integrity Primitives Evaluation Message Digest, see [18]). Both algorithms generate a unique 128 bit hash based on the message. Each message can be identified by this hash. Comparing the hash of a message m, denoted by $h(m)$, which is sent and encrypted within the message, with a self computed hash of the received message m', $h(m')$, you can detect altering of a message, by $h(m) \neq h(m')$, which ensures the message integrity.

As mentioned in section "Conclusion and Future Work" of our previous work [19] there was an ongoing NIST (National Institute for Standardization and Technology) competition for the next secure hash algorithm. Just a few weeks ago, on Oktober 3rd, the NIST pronounced the hash algorithm KECCAK (see [20]) to be the next secure hash algorithm, called SHA-3 (see [21]). SHA-3 is not meant to replace the common SHA-2, since no significant attacks on SHA-2 are known. Due to given theoretical attacks on SHA-1, there was a need for an alternative, different hash function. Keccak is built on a so called sponge function. A sponge function has an finite internal state und uses an input stream of any length and produces an output stream of any desired length. SHA-3 is a family of hash function with the possible state sizes of $\{25, 50, 100, 200, 400, 800, 1600\}$ bit and possible hash sizes

TABLE I
REQUIREMENTS TO THE DHKE-PARAMETERS

Value	Size
p	min. 512 bit (recommended 1024 bit)
g	$0 < g < p$
a	$0 \leq a \leq p-1$
b	$0 \leq b \leq p-1$

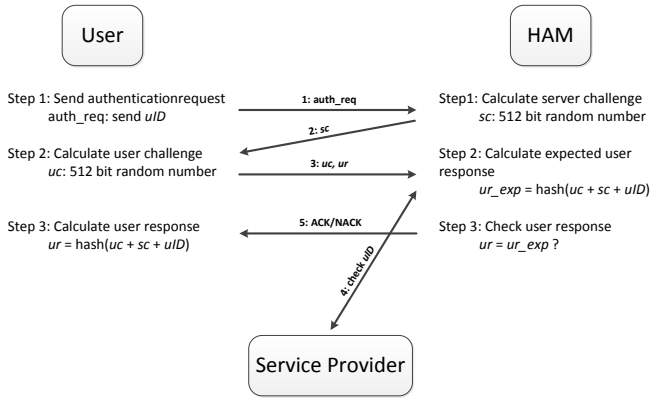

Fig. 2. User Authentication Process.

of $\{224, 256, 384, 512\}$ bit.
Nevertheless we can not recommend the use of SHA-3 without testing it in the context of embedded systems. Keccak is a very simple and fast hash algorithm based on a different architecture than SHA-2. Even so an implementation for micro controller is needed and hast to be tested, before we can recommend a use within the building automation system.

C. Authentication

Authentication is the process of verifying a claim made by a subject that it should be allowed to act on behalf of a given entity (person, computer, process, etc.). There are many different ways generally known for authentication, e.g. two-factor authentication, login / password, ownership authentication or knowledge authentication. For authentication we propose an adapted challenge-response protocol. Challenge-response authentication is a family of protocols in which one party presents a question (”challenge”) and another party must provide a valid answer (”response”) to be authenticated. Since we support many different entities, we need different types of knowledge for every entity type. Electronic devices possess a unique identity number, which can be used for authentication. A user receives such a number during the registration process.

To clarify this authentication methods, we will describe the authentication process of an user exemplarily. Every user of the system needs to be registered by a service provider. Within this registration process the user is provided with a unique identifier. This identifier is used to authenticate the user at his first participation in the system. After this first authentication, the user chooses a nickname and a password for every further authentication due to usability reasons. In the following, we will describe this first authentication process.

The authentication starts after receiving the unique identifier. The user wants to take part in the system and sends an authentication request to the system. As shown in figure 2, the user and the system perform a challenge-response process. Due to this process, the system and only the system is able to check whether the user is allowed to participate in the system or not. If the process is exited successfully, the user chooses a unique nickname and a password for any further authentication and the system only needs to check the combination of nickname and password.

D. Role-Based-Access-System

A home automation system, like SHS, has a number of functions and a variety of different and partly personal data. Required by law, the provider of such a system has to secure the personal data itself as well as proper handling of the data. That means for example, that only eligible persons for an assigned purpose are allowed to access this data. Because of the nature of a home automation system, there are some functions whose wrong usage can affect dependability. For this reason, the restriction of those functions is essential to ensure functionality at any time.

To provide this feature, we developed a role-based access system for the SHS scenario. First of all, we identified all participating entities, i.e. all kinds of persons or electronic devices which take part in the system. After that, we defined some standard roles and possible profiles and assigned the access authority to the specific data and functions:

- administrator - non-personalized user profile, personalized user profile (e.g. flat administrator, parents, ...)
- limited user - limited user profile (limitations individually determinable by flat administrator, e.g. profile: children,...)
- maintenance user - non-personalized profile with limitations for the purpose of maintenance (remote profile, on site profile,...)
- guest user - non-personalized limited profile with optional non-critical authorizations
- system provider - provider of the SHS system
- property provider - provider of the property, lessor
- service provider - external service provider, who offers services to normal users

We further identified the complete system functions/data and for all of them we assigned useful authorizations for every role. There are roles, like the administrator, who has authorization to all functions and data. Other roles, like a maintenance user, own only task-specific authorizations with respect to users privacy. Every system function and every data has an access control and only authorized users are able to get access. For every access, the system checks the user profile attributes whether the access is allowed or not. Within the registration process of a new user, there is a form where the registrar has to check which parts of system have to be accessible by the new user. In table II we will show the role-based-access-rights for some selected data and functions of a single facility service of the SHS-system. The shown service, “wireless reading of consumption data”, is an important and sensitive functionality of the SHS-system, so a restriction of access right is absolutely necessary.

E. Simulation Results

All provided algorithms work on embedded systems, which are supplied with battery and have only low resources. So it is necessary that each algorithm uses only a small amount of energy and time. So we measured duration and energy consumption of all cryptographic algorithms. The computations

TABLE II
ACCESS RIGHTS FOR SELECTED DATA AND FUNCTIONS OF "WIRELESS READING OF CONSUMPTION DATA."

	Role	Yes	No
Consumption data	Admin (Inst.)	x	
	Admin (Flat)	x	
	limited user		x
	maint. user		x
	guest user		x
	serv./prop. prov.	x	
	serv. prov		x

	Role	Yes	No
Transmission of data	Admin (Inst.)	x	
	Admin (Flat)		x
	limited user		x
	maint. user	x	
	guest user		x
	serv./prop. prov.	x	
	serv. prov		x

were processed on two different micro-controllers, the HCS08 and the MSP430.

HCS08 - all computations were processed by 8 MHz of clock frequency, a voltage of 3 V and a maximum current of 5 mA. Due to compiler license restrictions, RIPEMD128 was not tested on this device. The measurement results are shown in table III.

MSP430 - the computations were processed by a clock frequency of 25 MHz, a maximum of 3.6 V and a maximum current of 8.9 mA. The results are shown in table IV.

The energetic consideration of the implemented algorithms shows, that the Diffie-Hellman key exchange consumes the most energy. For this reason, we recommend to perform the key exchange only once during the first authentication. Every further key should be transferred via the established secure channel. As an energetically convenient cipher, we recommend AES128. Furthermore, it is supported by almost every device. We recommend RIPEMD128 as an energetic-optimal hash algorithm, because it is obviously better than SHA-1.

The following scenario within a home automation system demonstrates how important a security system is. Let us assume a radiator remotely controlled via Internet, i.e. the user wants to turn on the radiator thirty minutes before he arrives at the flat. He uses his smart phone to connect to the system remotely and uses a system function to turn on the radiator. In this scenario, there are many security needs. The remote connection has to be secured, the remote device has to authenticate itself, the accessing user has to be authorized and it has to be checked if the user has the right to access. If one of those needs is not satisfied it is possible for a malicious person to turn on the radiator whenever he wants to. Furthermore, for an intruder it would be possible to detect if the user is not at home, which means a high burglary risk. The proposed security architecture satisfies all of the named needs. We provide a secure Internet connection via SSL and the named encryption algorithms, our system is able to authenticate the accessing device and user and we can refuse the connection if an unauthorized access occurs.

TABLE III
ANALYSIS OF THE HCS08 MICRO-CONTROLLER

Algorithm	Duration [ms]	Enery use
DHKE	5220	87.5 mWs
RC4	14	210 μWs
AES128	5.7	85.5 μWs
SHA1	191	2.87 mWs
RIPEMD128	-	-

TABLE IV
ANALYSIS OF THE MSP430 MICRO-CONTROLLER

Algorithm	Duration [ms]	Enery use
DHKE	464	14.9 mWs
RC4	4.98	159 μWs
AES128	2.00	64.1 μWs
SHA1	6.57	211 mWs
RIPEMD128	0.827	26.5 μWs

V. QUALITY OF SERVICE SYSTEM

A. Theoretical Functionality

The fundamental idea of our quality of service solution is to control the access to the SHS network on each HAM unit and differ thereby between the applications based on a predefined priority scheme for each service. This means, that we allow each application to use only a defined data rate for communication. Furthermore, an adaptation of these settings is continuously made based on the state of the network. To perform this evaluation, first the network topology must be known and second, the current behavior of the applications must be obtained. For the first task, there exist diverse techniques to get this information automatically, but currently this is not a part of our application, we simply work with the predefined information of the network topology.

The second task is to measure and to shape the traffic caused by the services on the HAM unit. Both parts are highly related to the used operation system. To monitor the traffic, a packet analyzer, developed with the help of the "`pcap`" library, is used. This software offers the possibility to implement our system on Linux and on Windows machines, because this library is based on a portable framework. The shaping of the outgoing traffic is more challenging, but from a general point of view, Linux as well as Windows have a mechanism, that allows to take control of the data rate on the network interface card. The mechanism can be divided into two parts: a filter and a queue. The filter is used to assign specific packets to a queue, whereby several attributes could be used, e.g. a destination port range, a process ID of the sending process or the 802.1p flag settings of the packet. Each filter is assigned to a queue, but it is also possible to connect several filters to the same queue. If necessary, a serving strategy of the queue, like HTB (hierarchical token buffer) could be used, but in our case, a simple FIFO strategy is sufficient. The queue schedules the transmission of the packets, so that the defined data rate is guaranteed.

Our complete quality of service system works as follows: on each HAM unit a middleware is installed, that monitors and controls the outgoing network traffic with the help of the instruments recently described. A powerful HAM unit or

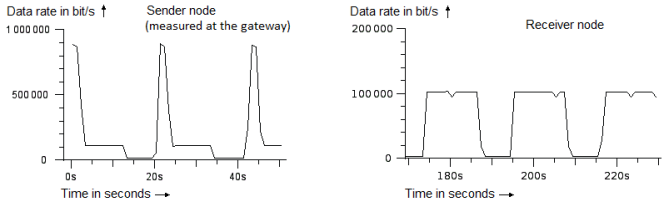

Fig. 3. Shaped traffic caused by multimedia device.

an additional control server is used as control manager of the network. The middleware on each HAM unit reports the communication status frequently in a certain time interval, e.g. 200 ms, to the control server. With this information, the server checks the network status on each link and sends adaptation messages to the middlewares, if one or more applications cause more traffic than suitable for the network. The adaptation process guarantees, that the high priority services of the SHS system can use their desired data rate for communication and prevents congestion situations inside the network.

B. Simulation and Evaluation

To test the quality of service system, we used a virtual network to check the functionality of the system and as well a real network to get reliable measurement data to prove the correct system behavior.

As mention in the introduction, the HAM unit is not only used as gateway for the sensor network, it is also used by some multimedia devices like a VoIP phone or a smart phone to allow them to communicate with each other and to give them access to the Internet via the installed SHS network. Therefore, by the virtual setup, we first checked the behavior of such devices and how the traffic shaping could be applied to control the traffic caused by such devices. Because the HAM unit acts as gateway in this case, the only way to assign this traffic to a filter is to use the second network interface as specific attribute for this packet and the MAC-address of the devices, to handle them individually.

Fig. 3 presents the measured results. The axis of abscissas shows the time in seconds, but the time axises of the two plots are not synchronized and the axis of ordinates is scaled in bits per second. The multimedia device sends three data packets in a row separated by a short time interval. The adaptation of the traffic class due to the reached data rate limit is not visualized in the diagrams.

The left plot shows the data received on the gateway sent by the multimedia device and the right plot shows the data received at the addressed destination. It illustrates that the traffic is limited to 100 kbit/s which was the default setting by our setup for this traffic class. Noticeable is the fact, that the gateway gets a short packet burst from the multimedia device at the startup, but the received traffic at the destination shows that the shaping works well when the gateway forwards the traffic to the SHS network.

Next, we used a real network for the evaluation of the system. To reduce the complexity, only two PCs, acting as HAM unit, are sending data to one destination and according

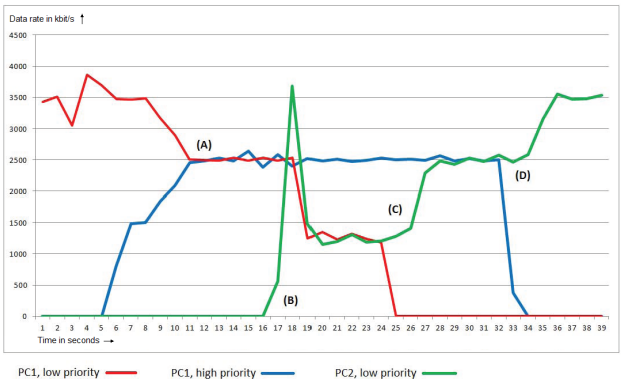

Fig. 4. Shaped traffic of some SHS services.

to that, there is one unique bottleneck link inside the network. Fig. 4 illustrates the traffic on that link. To eliminate the influence of the network devices and the system performance of each unit, we modeled each link inside the network to support only a maximum data rate of 5 Mbit/s. Finally we used only two priority classes and reduced the system reaction time to one second, which means that the middleware sends the current status each second to the control server. As above, the abscissa represents the time in seconds, but the data is reduced to the situations, where some changes happened. The ordinate dimension is in kbit/s.

Initially, PC1 sends a data stream with low priority and a data rate of 3.5 Mbit/s. Next, after a few seconds, this PC initializes a data stream with 2.5 Mbit/s but high priority. Due to the adaptation strategy, both streams are reduced to 2.5 Mbit/s (point A), because the link supports only 5 Mbit/s, but any other user defined partitioning would also be possible. This behavior is described in the system configuration, which could be changed by administrator.

After a few seconds, PC2 starts a data stream with low priority and a desired data rate of 3.5 Mbit/s (point B). In this case the adaptation of the data streams is different because we have two data streams coming from different PCs with different priority at the same time on the link. The reaction is, that both data streams with low priority in summary and the high priority data stream will get an equal data rate. This means, that the high priority data stream of PC1 is unchanged but the two low priority data streams are reduced to 2.5 Mbit/s in total.

Next, after the situation is stable, the low priority data stream from PC1 is stopped (point C) and so the low priority data stream of PC2 reaches the maximum of 2.5 Mbit/s, because there is still the high priority data stream of PC1. Finally this high priority stream is canceled (point D) and due to that, the data rate of the last stream inside the network can increase the date rate to the desired value of 3.5 Mbit/s.

VI. Further Considerations for Ethernet

As pointed out in the previous section, our proposed QoS system is based on an admission control scheme with a continuous evaluation and adaption of the network QoS settings made by a central control server. Nevertheless, this approach

solves the addressed problem under some practical constraints and can be realized with currently available hardware, it also introduces two critical problems. First, the single point of failure of the control server and second, the scaling problem conditional to these control servers if the size of the network is increased.

Due to the fact that each node of the network managed by the control server could also be a gateway to other networks or subnetworks, it is possible to split large networks into smaller sections and apply a control server to each of these network sections. This would mitigate the scaling problem and as well the single point of failure aspect. However, we still have to rely on these control servers, either for the complete network or at least for each section of the network. Therefore, a better alternative is to use distributed mechanisms to overcome these problems.

A. Distributed Approaches

The challenge of distributed algorithms is to reach a global objective for a large system consisting of several elements by controlling the system behavior only at each element. For example, the shortest path problem could be globally solved by the Dijkstra or Bellman-Ford algorithm but this is also a typical example for the ant colony optimization approach [22] and demonstrates how a simple idea could be used to solve problems based on a distributed technique.

In the case of an Ethernet network, the problem is more complex and therefore it is difficult to find adequate solutions solving the quality of service problem with a decentralized scheme. Nevertheless, many approaches have been investigated and collected under the term 'data center bridging' (DCB) based on several IEEE projects, see e.g. [23].

- congestion notification, IEEE 802.1Qau
- priority-based flow control, IEEE 802.1Qbb
- enhanced transmission control, IEEE 802.1Qaz

And the IEEE 802.1aq shortest path bridging standard, but we will discuss this together with an alternative in the next subsection in more detail.

Using these techniques, it should be possible to improve the performance and effectiveness of Ethernet networks and to integrate some QoS-aware behavior. The standards are mainly completed, but the corresponding hardware supporting these features is currently not available as well as comprehensive simulation studies showing how powerful all these ideas can work together related to the requirements of a QoS-aware network, whereas some other publications have already proposed some modification of these ideas to improve the standard.

The IEEE 802.1Qau congestion notification standard addresses the already mentioned overflow problem which occurs if a switch receives more data packets than it can transmit. As known, a point-to-point based congestion handling is not selective enough and could dramatically decrease the network performance especially in the case of large networks [24]. This standards attempts to overcome the problem by extracting the causing node of the congestion at the edge of the network. Each switch of the network detecting a congestion situation generates a congestion notification message which is sent over other switches to the causing node. Based on the received congestion notification, a rate limiter adjusts the injection rate for the services whereas the signaling contains enough information to selectively decrease only traffic, that is responsible for the occurred congestion situation. Evaluations and improvements of this standard can be found in [25] or [26].

Besides the Xon/Xoff signaling (PAUSE frame), the IEEE 802.1Qbb standards defines an enhanced mechanism of this idea. Similar to the situation described in the last paragraph, the Xon/Xoff signaling controls the incoming traffic to a switch to prevent buffer overflows. However, this regulation affects the complete traffic without evaluating the priority of the data packets. Because this is also part of the network interface card, the nodes of the network are affected by this mechanism, too. A more detailed discussion and performance evaluation can be found in [27]. The challenge how the controlling based on these priority classes should be done is addressed by the IEEE 802.1Qaz standard.

All these techniques are able to improve the performance, efficiency and the QoS-aware behavior of Ethernet networks. But it still must be evaluated how well these standards are able to enhance the network functionality with regard to specific requirements of different use cases, especially because these standards are not able to provide hard QoS as AVB ([7], II-B) does.

B. Bridging Strategies

The standards described in the section above are responsible for link control like traffic engineering, congestion management and the handling of traffic classes. Here, we will discuss a more fundamental aspect of an Ethernet network, the layer two topology. As presented in [28], Ethernet networks are typically based on the spanning tree protocol or some derivations of it. The main purpose for these protocols was to simplify the forwarding strategy for switches. Due to the deactivation of redundant paths in an Ethernet network, each switch could be sure, that sending out data packets with a destination MAC-address at that port where a packets was received with the corresponding source MAC-address before, is sufficient. The problems of circling data packets or packet duplicates did not have to be considered, either. Besides these advantages, the reduction of the network topology to a spanning tree goes around with a negative effect, too: redundancy is the basis for high performance, reliability and effectiveness and therefore not applicable in those networks.

Nevertheless, the IEEE 802.1aq shortest path bridging standard and TRILL (transparent interconnection of lots of links, RFC 6325) propose a bridging strategy for Ethernet networks where the setup of a unique spanning tree is no longer necessary and where the redundant paths are used to improve the network. The goal is to fully utilize equal cost paths in a mesh network topology to open the area where Ethernet could be applied, especially in view of data center networks and metropolitan area networks. Compared to the classical hierarchical separation of networks into core/aggregation/access

layer, these technologies permit the chance to unify the access and aggregation network technology.

Both techniques, shortest path bridging and transparent interconnection of lots of links, have been evaluated based on various conditions and even some improvements have been discussed [29–31]. However, as we think, the challenge here is to define a suitable and reproducible network scenario allowing to fairly evaluate the performance of both techniques. Furthermore, the evaluation and comparison must be based on exactly defined and convincing performance metrics like throughput, adaption time, link utilization or how good specific requirements are fulfilled. To perform an evaluation of a network or even more a comparison of different network techniques, it is very important to spend effort on the definition of usable metrics for this case. In our view, this was not the main focus of many publications on this topic, hence, it is hard to compare these results. Therefore, our future work is to define these metrics to determine under which conditions IEEE802.1aq and TRILL perform best.

VII. Conclusion and Future Work

In this paper we provided a complete communication architecture for the smart home scenario which offers both, an adequate security system and a quality of service scheme. The comprehensive security architecture addresses all needs of modern building automation systems. We performed threat modeling and identified all possible threats and all security assets of the system. We provide security features and functions for all needs, comprising encryption features, hash algorithms, authentication methods and a role-based-access-system. The proposed security architecture satisfies all actual legal requirements regarding the German federal data security law. In the near future, updates of this law in relation to smart metering systems are expectable. Nevertheless, the proposed architecture will also fulfill these requirements, but the actual certification has to be considered. Moreover, the evaluation of the quality of service strategy demonstrated, that the main parts of that solution can cooperate to avoid network congestion inside the home network. As described, there are interesting alternative approaches for Ethernet and our main focus for the future work is to compare and evaluate this techniques with respect to the QoS aspects of the SHS scenario.

Acknowledgment

The work described in this paper has been carried out in the "SHS: Home" research project funded by the AiF (Arbeitsgemeinschaft industrieller Forschungsvereinigungen "Otto von Guericke" e.V.) Projekt GmbH, the project executing organization for the German Federal Ministry of Economy and Technology.

References

[1] Smart Home Services Research Project. (2011). [Online]. Available: http://www.smart-home-services.de/

[2] ACX GmbH. (2011) ViciOne Home and Building Automation. [Online]. Available: http://www.acx-gmbh.de/de/home-building-automation/index.html

[3] M. A. Zamora-Izquierdo, J. Santa, and A. F. Gomez-Skarmeta, "An Integral and Networked Home Automation Solution for Indoor Ambient Intelligence," *IEEE Pervasive Computing*, vol. 9, pp. 66–77, October 2010. [Online]. Available: http://dx.doi.org/10.1109/MPRV.2010.20

[4] Smart Home der Bundeswehr Universitaet Muenchen. (2011). [Online]. Available: http://www.unibw.de/eit8_2/forschung/projekte/shfilm/

[5] Smarter Wohnen ®NRW, Fraunhofer IMS, Fraunhofer ISST, HGW. (2011). [Online]. Available: http://www.smarterwohnennrw.de

[6] Service Centric Home. (2011). [Online]. Available: http://www.sercho.de

[7] IEEE 802.1 Audio/Video Bridging Task Group Home Page. (2011). [Online]. Available: http://www.ieee802.org/1/pages/avbridges.html

[8] Bannazadeh H. and Leon-Garcia A., "A Distributed Ethernet Traffic Shaping System," *Local and Metropolitan Area Networks (LANMAN), 2010 17th IEEE Workshop on*, May 2010.

[9] Y. Zhang, R. Yu, S. Xie, W. Yao, Y. Xiao, and M. Guizani, "Home M2M Networks: Architectures, Standards, and QoS Improvement," *Communications Magazine, IEEE*, vol. 49, no. 4, April 2011.

[10] G. McAlpine, "Congestion Control for Switched Ethernet," *High Performance Interconnects for Distributed Computing*, 2005.

[11] N. Ferguson and B. Schneier, "Practical Cryptography," *Wiley Publishing, Indianapolis, ISBN 0-471-22357-3*, 2003.

[12] N. W. Group, "A Stream Cipher Encryption Algorithm 'Arcfour'," *Internet Engineering Task Force*, 1997.

[13] W. Diffie and M. E. Hellman, "New Directions in Cryptography," *In IEEE Transactions on Information Theory. 22, Nr. 6*, 1976.

[14] RSA Security. (1991) Public Key Cryptography Standards Number 3: Diffie Hellman Key Agreement Standard. [Online]. Available: http://www.rsa.com/rsalabs/node.asp?id=2126

[15] N. W. Group, "RFC 2631: Diffie-Hellman Key Agreement Method," *Internet Engineering Task Force*, 1999.

[16] B. Kaliski, RSA Security. (2003) TWIRL and RSA Key Size. [Online]. Available: http://www.rsa.com/rsalabs/node.asp?id=2004

[17] W. Diffie, P. C. V. Oorschot, and M. J. Wiener, "Authentication and Authenticated Key Exchanges," *Designs, Codes and Cryptography*, vol. 2, no. 2, pp. 107 – 125, 1992.

[18] H. D. B. Preneel, A. Bosselaers, "The Cryptographic Hash Function RIPEMD-160," *CryptoBytes, Vol. 3, Nr. 2*, 1997.

[19] M. Hager, S. Schellenberg, J. Seitz, S. Mann, and G. Schorcht, "Secure and QoS-aware Communications for Smart Home Services," in *Telecommunications and Signal Processing (TSP), 2012 35th International Conference on*, july 2012.

[20] G. Bertoni, J. Daemen, M. Peeters, and G. V. Assche, "The keccak reference," Submission to NIST (Round 3), 2011. [Online]. Available: http://keccak.noekeon.org/Keccak-reference-3.0.pdf

[21] N. I. for Standards and Technology, "Winner of the cryptographic hash algorithm competition for sha-3," 2012. [Online]. Available: http://www.nist.gov/itl/csd/sha-100212.cfm

[22] Jayadeva, S. Shah, R. Kothari, and S. Chandra, "Debugging ants: How ants find the shortest route," in *Information, Communications and Signal Processing (ICICS) 2011 8th International Conference on*, dec. 2011.

[23] S. Reinemo, T. Skeie, and M. Wadekar, "Ethernet for high-performance data centers: On the new ieee datacenter bridging standards," *Micro, IEEE*, vol. 30, no. 4, pp. 42 –51, july-aug. 2010.

[24] W. Noureddine, F. Tobagi, W. Noureddine, and F. Tobagi, "Selective back-pressure in switched ethernet lans," in *Proceedings of IEEE GLOBECOM*, 1999, pp. 1256–1263.

[25] M. e. a. Alizadeh, "Data center transport mechanisms: Congestion control theory and ieee standardization," in *Communication, Control, and Computing, 2008 46th Annual Allerton Conference on*, sept. 2008.

[26] W. Jiang, F. Ren, C. Lin, and I. Stojmenovic, "Analysis of backward congestion notification with delay for enhanced ethernet networks," in *INFOCOM, 2012 Proceedings IEEE*, march 2012, pp. 2961 –2965.

[27] M. Hagen and R. Zarick, "Performance evaluation of dcb's priority-based flow control," in *Network Computing and Applications (NCA), 2011 10th IEEE International Symposium on*, aug. 2011, pp. 328 –333.

[28] R. Sofia, "A survey of advanced ethernet forwarding approaches," *Communications Surveys Tutorials, IEEE*, vol. 11, no. 1, quarter 2009.

[29] R. Perlman, "Challenges and Opportunities in the Design of TRILL: A Routed Layer 2 Technology," in *GLOBECOM Workshops, IEEE*, 2009.

[30] K. Miyazaki, K. Nishimura, J. Tanaka, and S. Kotabe, "First-Come First-Served Routing for the Data Center Network: Low Latency Loop-Free Routing," in *World Telecommunications Congress (WTC),*, march 2012.

[31] D. Allan, J. Farkas, and S. Mansfield, "Intelligent load balancing for shortest path bridging," *Communications Magazine, IEEE*, july 2012.