Dynamic Key Distribution for Secure Group Communications in Constrained Environments

Tobias Guggemos
MNM-Team, Ludwig-Maximilians-Universität München, Munich, Germany
guggemos@nm.ifi.lmu.de

Abstract

Group communication – especially in form of multicast – is a famous communication pattern in constrained networks, e.g. in the Internet of Things (IoT), Wireless Sensor Networks (WSN) or Device to Device (D2D) communication. However, it comes with mandatory management overhead during the life-cycle of a group, which is usually favored due to the potential energy savings ones the connection is set up. The management paradigm worsens, if the connection within and the management of the group has to be secure and in turn requires security management. Security and cryptography, however, need special attention when used in constrained environments. The proposed thesis will connect group management, group communication and security management and apply them to constrained environments.

Introduction / Motivation

Group communication has been discussed for decades, mostly within computer networking and social messengers. Nowadays, most smartphone messengers offer the formation of groups in order to achieve discussion of several people on a certain topic or interest. Groups have members and administrators, the communication itself is a 1:n communication pattern, where one device is sending data to a group of receivers, the so called multicast. In classical computer networks, multicast is mostly used for streaming applications. Clients subscribe to and the server sends data to a specific multicast address while the network takes care of the distribution.

Other forms of group communication are the n:1 communication pattern, where a group of people sends data to single receiver(s) outside the group. A common example for this pattern are *receiver initiated MAC protocols* (Sun et al., 2008). The specification of n:m communication pattern is self-explanatory, however, please note that 1:1 communication might be a valid form of group communication as well.

Scenarios with networks of constrained devices (like embedded systems) and network technologies (like Internet of Things) can benefit from dynamic formation of communication groups. First, this form of communication often saves bandwidth and in turn energy, increasing the life time of battery driven devices. Second, the existence of a communication group eases distribution of data as the interested receiver registers beforehand and does not have to be discovered ad-hoc, examples being the distribution of control information (e.g. in Smart Homes/Cities), but also firmware updates for a certain group of devices.

The goal of this PhD thesis is to benefit from the advantages of group communications in constrained systems while preserving security. Thus, it will develop a system to evaluate the efficiency of secure group communication and the inherent key management solutions, covering the life-cycle of a communication group. The methodology being used will present models covering the key management during the different group management actions. The system will be developed according to these models in order to ensure its completeness and to produce reproducible results for the research community. Evaluated solutions will either be optimized to achieve better efficiency or shown impracticable for specific system or scenario classifications. With this results at hand, recommendation on scenario specific configuration for key management can be developed.

1 RESEARCH PROBLEM

A major difficulty of securing communication in constrained environments is the distribution of keys, which is the main aspect of this thesis and mainly touches the research areas of *Security Management* (Section 1.4) and *Cryptography* (Section 1.5). In order to understand the additional challenges for constrained group communication, there are three other related research areas, which leads to the problem

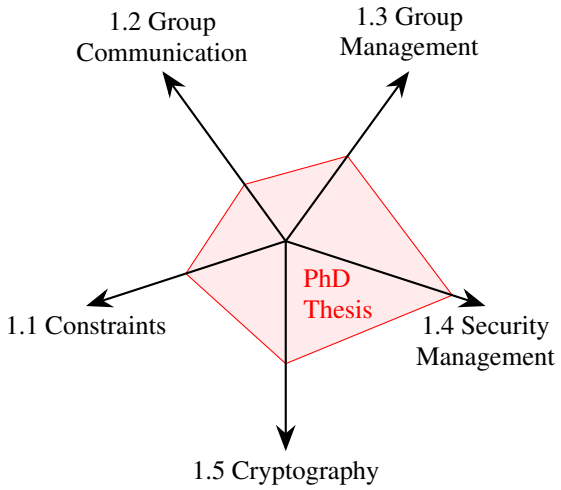

Figure 1: Connected research areas and their relation to the presented PhD thesis.

space in Figure 1. The figure highlights the expected influence of each of the areas to this PhD thesis and the following subsections will briefly introduce each of them.

1.1 Constrained Environments

The constraints considered are *system limitation*, including *device limitations* (CPU, RAM, ROM) of the used microcontroller and its attached hardware limitations for *power*, and *networking*. *Scenario limitation*, such as maximum execution time and minimum device lifetime are also considered.

1.1.1 System limitations

System limitations are part of ongoing research and standardization, resulting in the description of RFC 7228 (Bormann et al., 2014) and its proposed successor RFC 7228bis (Bormann et al., 2017). Both documents define classes for the different aspects:

Device Classes currently range from Class 0 to Class 19, although only up to Class 13 is of interest for this thesis (Class 14 - 19 classify smartphones, desktop PCs and servers). The classification ranges from $< 10KiB$ up to $1MiB$ of RAM and $< 100KiB$ up to $2MiB$ of Flash (Class 0-Class 2) and increases toward Class 10 with about $4-8MiB$ of RAM up to Class 13 with $0.5-1GiB$ of RAM without significant limitation for Flash memory.

Power Classes differentiate between the maximum average power available during the lifetime (in Watt) and the total electricity available until the device runs out of energy (in Joule). Both require different strategies in order to exploit the provided power to the fullest.

For the available power, the RFCs define three classes of devices, which are usually powered off (Class P0), always on low power (Class P1) and always on and connected (Class P9).

For the available energy, the RFCs define devices being limited in the energy for a single event (Class E0), limited for a specific period (Class E1), limited for the whole lifetime (Class E3) and not limited at all (Class E9).

Network classes mainly distinguish between the available MTU size and the bit rate of the physical layer. Both factors are typical for but not limited to wireless communication. Even though the bit rate is important for choosing a suitable network technology in a given scenario, the MTU size turns out to be the major source of limitation. It is the relevant factor for packet fragmentation, which is avoided wherever possible. In constrained environments, where sending frames on the physical layer is very expensive, packet compression turns out to be the weapon of choice (Kushalnagar et al., 2007). Sending an extra bit is as energy consuming as 10-100 CPU cycles and sending an extra radio frame is even worse. In unconstrained environments, fragmentation is usually tried to be avoided in order to preserve interoperability.

The network classes for MTU start from as low as $3-12bytes$ (Class S0) and $12-127bytes$ (Class S1), where compression is almost unavoidable in order to prevent fragmentation. The classes continue from $128-1279bytes$ (Class S2) up to $>= 1280$ (Class S3) where fragmentation turns out to be negligible.

1.1.2 Scenario limitations

Scenario limitations describe a set of systems with a given set of *system constraints* having to meet *minimum lifetime* of a system or a *maximum execution time* of one single task within the scenario.

minimum device lifetime A scenario with a *minimum device lifetime*, will highly affect the choice of battery and the chosen energy strategy. This may as well lead to a specific choice of network technology, which on the other side could be driven by the physical setting of the device where only a certain low-power network technology might be available.

maximum execution time A famous scenario where *maximum execution time* applies, is the one of an

industrial lightening system, where thousands of light bulbs need to be turned on within a certain time (e.g. 200 ms). In an extreme case, this may change during the life-time of the device which leads to an update of the energy strategy.

Summary of Challenges:

I. device strategies for energy / time optimization

II. scenario strategies for energy / time optimization

III. network overhead needs to be reduced

IV. network technologies with very low MTU

1.2 Group Communication

Most of the examples for group communication have in common that they favor some management effort in order to simplify the actual communication/distribution of data. This is, however, controversial for typical traffic in the internet, where management tends to be more expensive, than data distribution. It happens that this makes group communication a minority within today's internet traffic.

This cost paradigm changes in scenarios with constrained resources, where managing a communication channel might cost much less money than sending a technician to replace a device because it ran out of battery, caused by too much traffic. It is shown in (Silva et al., 2008) that group communication in form of multicast saves energy but also allows the minimization of the execution time as in the example for an industrial lightening system. In that case, multicast allows to send only one packet instead of thousands and, thus, significantly reduces the execution time of the system.

With the arrival of IoT, these scenarios may even distribute over different administrative domains (e.g. connecting devices of two independent smart homes), further worsen the management overhead.

Summary of Challenges:

I. minimizing management of multicast

II. group communication within different administrative domains

1.3 Group Communication Management

Misapplied, the management of a group channel can pervert the advantages of group communication and may even lead to higher energy consumption as shown in (Djamaa et al., 2014). When connecting different administrative domains over a public network – which is a common use case for IoT – this worsens as it is impossible to ensure that every router in the public network is capable or willing to forward multicast packets. Several approaches, such as path discovery, exist in order to overcome this issue but it leads to bare acceptance of multicast in typical internet traffic.

In wireless sensor networks (WSN) it is easier to solve the routing issue, mainly because ad-hoc routing was a very widely discussed topic 10 years ago. The movement resulted in several quasi-standard routing protocols for different scenarios, of which some include MAC layer multicasting. However, when leaving the local domain of WSN, the management issues demand the necessity of efficient management channels remains.

There are additional management issues, when considering not only the *communication*, but also the other phases of the life cycle of the group. Most commonly a group has four group relevant actions, being *create / delete group*, member *joining* or *leaving* the group, which needs to be performed and managed as efficient as possible in order not to overburden devices or networks.

Summary of Challenges:

I. cover the whole group life cycle

II. efficient management channels

1.4 Security Management

During the actual communication, the three security properties of *confidentiality*, *integrity* and *authenticity* turn out to be most valuable. Although, all of them can be solved by applying cryptographic functions, there are many issues to be solved in order to apply them in a secure and trustful manner. This is especially true for the management of cryptographic (group) keys.

1.4.1 Group Key Management

Group Key Management (GKM) is highly driven by the security aspects during the actual group communication:

I. Confidentiality requires the parties to agree on a symmetric encryption key, which is often done with the Diffie-Hellman key exchange. Confidentiality can also be ensured with asymmetric cryptography, a technique which is often applied in e-mail and mobile messenger communication. However, for group communication the distribution of keys – let it be symmetric or asymmetric – is a difficult task to be solved. The

most common symmetric approach has a central key server (sometimes called trusted third party), which distributes a key to the participants of the group. There has been and there is still various research, investigating in more efficient key distribution schemes, such as logical key hierarchies (LKH). Additionally, there are decentralized and distributed key distribution approaches available, a recent one has been proposed for mobile messaging (Omara et al., 2018).

II. Integrity of messages is usually achieved by a combination of a shared key and a message authentication code (MAC), which is called Key-Hashed MAC (HMAC). It comes with the same challenges as confidentiality for key distribution. If an integrity key is shared by all members in the group, a message can be altered by any group member. This allows integrity within the group, meaning that a receiver can ensure that the message was not altered outside the group. Additional security can be applied by individual sender keys, so that the message cannot be altered, even by valid group members, and thus enabling sender integrity.

III. Authenticity is achieved by asymmetric cryptographic keys, as it offers the necessary fusion with the sender's identity – usually in form of certificates. The difficulties lie in the longer size of asymmetric keys and a trustful mapping between the identity and public key.

1.4.2 Trust Management

Trust Management is a highly controversial topic, especially in the world of IoT where objects, which are physically vulnerable are interconnected, and need to be considered violated at any time. Yan et al. surveyed trust management in this specific area and laid one focus on the trust of the physical system (Yan et al., 2014). Multiple ideas exist to enhance physical security (e.g. Trusted Platform Modules), but the trust problem remains. However, this could be overcome with techniques of trust management and dynamic access control for a communication group. If trust can be built before any of the mentioned group actions is performed (join, leave, etc.), it can also be revoked within the group if a member is compromised. This in turn requires key management (see above), enabling revocation of identities and their corresponding keys.

Additionally, trust requires access control to the communication group, allowing restricting, granting and revoking rights to specific members.

Summary of Challenges:

I. efficient symmetric key distribution protocols

II. efficient key hierarchies (symmetric and asymmetric)

III. efficient public key infrastructure

IV. efficient public key revocation

V. access management

VI. identity management

1.5 Constrained device cryptography

All constraints in Section 1.1 can have significant and independent impact to the maximum achievable level of security. In combination they can even worsen the security. The available RAM can significantly reduce the maximum length of keys for confidentiality, integrity and authenticity.

The choice of network technology or the form of energy supply might be driven by the scenario and cannot be altered significantly. Imagine a scenario with a minimum device lifetime of many years and a very low-powered network link (e.g. LoRa (see RFC 8376 (Farrell, 2018)) with 50 bytes MTU). Applying strong authentication algorithm (e.g. RSA on top of X.509 certificates) with unoptimized secure protocols will result in high packet fragmentation rates and many frames on the physical link. As this is usually the most energy-expensive task, it directly influences the lifetime of the battery for energy supply and, thus, the lifetime of the device.

Many encryption and integrity algorithms are supported by hardware acceleration (e.g. AES), but efficient authentication algorithms remain a difficult task on constrained devices. They not only require more computation time, they also result in higher network and management overhead (see previous subsection) and tend to be more affected by the challenges raised by the potential arrival of quantum computers. A very famous example for these challenges is the algorithm of *Shor* (Shor, 1994), which will brake RSA and ECDSA, the latter being very famous in constrained devices because of its efficiency and shorter key lengths compared to RSA.

Summary of Challenges:

I. efficient asymmetric cryptographic algorithms

II. minimized security protocols

III. Post Quantum Security

2 OUTLINE OF OBJECTIVES

In order to achieve better efficiency when distributing group keys in constrained environments, this thesis will investigate 1.) efficient security solutions for constrained devices, 2.) improving the key management for group communication and finally 3.) building a scalable and interoperable framework for distributing group keys. Each of these goals will be briefly discussed in the following.

2.1 Evaluating efficient security solutions

There is a variety of research for efficient security solutions, in particular in form of new asymmetric cryptographic algorithms, network protocols and certificate formats (including certificate revocation). This work will not design yet another solution, but evaluate the most promising solutions within the context of constrained devices and group communication in particular. This is of special importance, as many of the solutions are not evaluated on current hardware and state of the art network technologies, or not even available as open source. The goal is a framework, which can be used to evaluate existing and new solutions with a special focus on their suitability in highly dynamic environments.

An additional task will include the specific evaluation of algorithms proposed in the NIST call for *Post-Quantum Cryptography Standardization*[1].

2.2 Security Management

With the framework mentioned above, the work will investigate in how to use existing security solutions for efficient distribution of symmetric or asymmetric keys, but also their revocation. Identities necessary for authenticity, tend to be (asymmetric) cryptographic keys, making this similar to certificate revocation. However, instead of being used for frequent communication within the group, it is used to achieve trust within the group, leading to stronger requirements on its (physical) security.

The goal is to develop a metric for comparing distribution schemes for given scenarios.

2.3 Scalability and Interoperability

The last goal is to design and implement an architecture, which is able to dynamically establish communication groups, fitting defined security requirements and evaluate the above goals. A special interest will point on the scalability and interoperability, but also on the level of distribution between different administrative domains. The solution should not be limited to local or broadcast domains but should dynamically scale over globally distributed domains.

[1] https://csrc.nist.gov/projects/post-quantum-cryptography

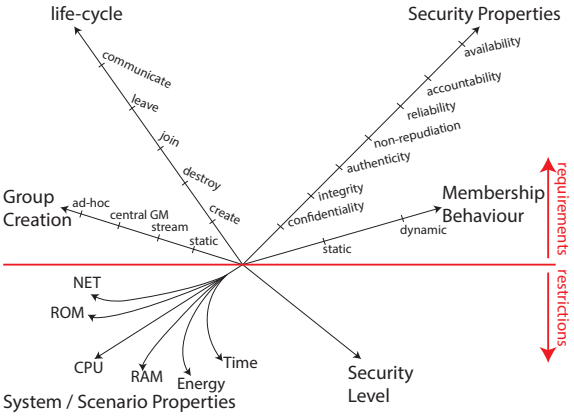

Figure 2: Requirements for security management and restriction, which are incorporated in the PhD thesis.

2.4 Summary

The key aspects of this thesis, *Security Management* and *Cryptography*, are influenced by certain requirements and restriction, as outlined in Figure 2. The red line in the diagram marks the differentiation between these two aspects.

Requirements Above the red line, the diagram is used to describe the requirements for a certain scenario in order find a viable solution for the aspects of security management. As already mentioned, groups underlay certain actions during their *life-cycle*. The management of each of these phases depend on 1.) *Group Creation* and 2.) *Membership Behavior*, directly influencing the security management. Additionally, the *Security Properties* describe which aspects of security need to be considered during a certain phase of the group management.

Restrictions Below the red line the diagram is used to describe the conditions, under which the requirements have to be met. They mainly consist of 1.) *constraints* of a certain scenario (see Section 1.1) and 2.) the desired *Security Level*. Constraints and Security are directly influencing one another and describe which cryptographic functions and keys can be used. Th constraints and the required security level influence the possible / necessary options for key management protocols.

3 STATE OF THE ART

The work at hand proposes an infrastructure, allowing for dynamic key management of communication group. Especially in the area of IoT, this is a widely discussed topic, but dynamic approaches are rare.

3.1 Group Management

Named Data Networks (NDN) (Shang et al., 2017) is one such approach, abstracting the typical protocol stack (IP, TCP/UDP, DNS) and naming the data instead of the systems generating or consuming the data. It can be seen as a follow-up of the idea of Information Centric Networking (ICN) (Ahlgren et al., 2012) making the communication infrastructure more robust against mobility of devices, changes of addresses (e.g. IP-address) or names (e.g. DNS-names). Both offer dynamic formation of groups being interested in certain data / information, but the security management behaves static during the setup of the devices. Device-to-device (D2D) is another approach, where the data is not routed over central services, but through a decentralized network (e.g. border routers, mobile access points, etc.). D2D offers a solution for dynamic communication groups and efficient networking, but as outlined by (Haus et al., 2017) we have yet to see suitable solutions for security management, especially when talking about the constraints of some of the devices.

3.2 Security Management

Group key distribution itself is an extensively studied area and resulted in a couple of standardization activities. (Rafaeli and Hutchison, 2003) survey a set of approaches for secure group key distribution (GKD). According to their analysis, there are three different types of GKDs: centralized, decentralized and distributed GKD protocols. Most of them are rather *Cryptographic Key Schemes* than networking protocols, some of which are distributed within *Group Key Management Protocols*. Besides a practical evaluation of G-IKEv2 for group key management, the work in (gentschen Felde et al., 2017) gives a comparison of the most recent proposals for distributing keys in constrained environments, however, the solutions are still experimental and require further evaluation. There is different work establishing group keys on different layers of the OSI model (Singh et al., 2015; Tiloca et al., 2017), but an analysis and solution covering the whole life cycle is still missing.

There is recent research activity in group key management protocols for mobile messengers (Omara et al., 2018). In contrast to the work of this thesis, it is more focused on usability but offers strong security proofs, which will need to be adapted to constrained scenarios.

3.3 Cryptography

Cryptography in general and for embedded devices in particular is widely discussed among different research communities. There are studies on 1.) lightweight cryptographic schemes (often based on elliptic curve cryptography), 2.) optimizations for security protocols (such as TLS or IPsec), 3.) accelerating cryptographic functions or secure storage and generation of key material and 4.) new mathematical primitives. The latter recently gained attention due to the previously mentioned NIST call for *Post-Quantum Cryptography Standardization*.

All of these topics offer solutions for some parts of the described problem space, but an integrated solution is missing. Especially the rapid progress in quantum computing requires attention, as some constrained devices with life-time of 10+ years may still be deployed when the first quantum computers appear.

The contributions of the work at hand can help to overcome this issue, as it will provide solutions how any compromised key of a compromised algorithm can be replaced, even on devices where physical accessibility may not be given.

4 METHODOLOGY

Any given action in the group can require the distribution of keys, especially when members join or leave the group and security goals such as *forward* or *backward* secrecy need to be met. This work will first establish role, communication and information models for the different parts of the life-cycle. With these models at hand, a system instantiating the models is developed and used to evaluate existing and new group key distribution solutions in constrained environments.

4.1 Role-, Communication- and Information Model

The models were built by analyzing the group actions *create*, *destroy*, *join* and *leave*. Additionally, the actions of sending a message within the group was analyzed and it was found that in order to achieve trust

within the system (and in turn in the group) additional action called *registration* is necessary. This action registers a member in the system and registers its cryptographic material at a trust anchor.

Please note, that the author is fully aware that this additional action does not solve the issue of trust in general and results in a *chicken-egg-problem* in the system. However, this is true for any other system such as PKI or DNSSEC, which often combine similar actions and roles for registration. In fact, the following models and actions were identified by analyzing state-of-the-art systems, such as *X.509*, *DNSSEC* and *PGP* when performed within a group keying management system such as *GKMP*, *GDOI* or *Kerberos*.

In the following, the identified models are briefly discussed and shown in Figure 3. However, the entire model will be part of the PhD thesis itself.

4.1.1 Role Model

The analysis showed the following roles are necessary during the different group actions:

- **Group Admin** is registered to the system, performing group actions *create* and *destroy*.
- **Client / Sender** is registered to the system, performing *join* and *leave* requests and sends messages.
- **Group** is the role for all members of the group.
- **Identity Manager (IM)** for assigning identities and ensuring their reliability and uniqueness.
- **Key Manager (KM)** for generating cryptographic material for authentication, usually in form of asymmetric key pairs. The instance of this role can either be part of or attached to the client (e.g. a TPM), or an external service. The generated key(s) are generated for the Identity. The same or another instance of this role is in charge of generating communication keys, distributing them to the group and re-key on certain actions if required.
- **Trust Anchor (TA)** connects the Identity (generated by the IM) with the (public) key (generated by the KM). Analyzing the currently used systems for trust management (e.g. X.509) showed that the group life-cycle should start with a so-called *registration* phase, which leads to an entry of the new client within the TA. Once registered, the TA can be consulted by *any role* within the system to proof authenticity (AuthN).
- **Group Manager (GM)** is in charge of managing groups with corresponding group ids/addresses and their members. It also offers a service for exploring existing groups.
- **Access Manager (AM)** is in charge of managing if a client is authorized (AuthZ) for specific group actions.

4.1.2 Information Model

The cryptographic information being exchanged prior and during the group communication is as follows:

- **Identity** the identity of the role initiating an action, therefore either the User or the client performing a group action or the sender sending a message. Valid Ids are managed by the IM.
- **Private Key** the cryptographic private key of the Id generated.
- **Public Key** the cryptographic public key of the Id generated.
- **System Certificate** the combination of Id and Public Key, which is registered at the TA.
- **Cryptographic Primitives** the information about the algorithm being used for the different cryptographic keys (e.g. *RSA* for authentication or *AES* for confidentiality).
- **Current Communication Keys** the cryptographic keys used for securing the communication.
- **New Communication Keys** keys used by the group after *join* or *leave*
- **Old Communication Keys** keys used by the group before *join* or *leave*
- **Group Id** the identity or address of the group.
- **Group Members** mapping of Ids to group id, stored at the GM
- **Access Control List** mapping of identities to a security policy for a specific group action, stored at the AM.

4.1.3 Communication Model

With the roles identified in the previous subsection, the following communication paths are necessary within the system.

- **Identity Request** client/admin requests an Identity from the IM, who returns a system unique Id.
- **Key Generation Request** client requests an authentication key-pair with its Id to the KM.
- **System Certificate Registration** after generating the key-pair, the KM requests the registration of the corresponding Id and public key at the TA.
- **Verify Id** KM or TA requests the IM to verify a given Id.

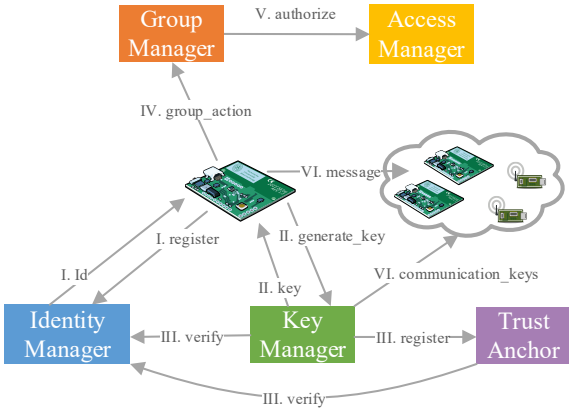

Figure 3: Roles and basic communication paths

- **Verify AuthN** any member of the system can verify a signature signed with a system certificate by requesting the TA.
- **Verify AuthZ** GM requests from the AM if an Id is authorized to perform a given group action.
- **Group Action** client/admin triggers a group action including a signature signed with its private key and Id.
- **Re-key** GM triggers the KM to perform a re-key of the communication keys of the group.

4.2 Evaluation

In order to provide a valuable evaluation for constrained systems, first a test infrastructure will be described and set up, which will be used for practical measurements. The security mechanism will additionally be evaluated with formal security proofs.

4.2.1 Infrastructure

The infrastructure, which will be set up, is very closely related to the well-known evaluation platform called IoT-Lab[2]. The major difference to the IoT-Lab lies in the usage of different microcontrollers in combination with different networking technologies.

The IoT-Lab currently supports three different microcontrollers based on ATMEGA MSP430, ARM Cortex M3 and ARM Cortex-A8. Additionally, it supports two networking technologies, one being based on the IEEE 802.15.4 standard and the other one being LoRa. The platform proposed in this paper will supplement the platform with ARM Cortex M0 microcontrollers and the additional networking technologies IEEE 802.3 (Ethernet), IEEE 802.11 (WiFi) and IEEE 802.15.1 (Bluetooth). Furthermore, it will be supplemented with an additional configuration software, allowing the easy setup of communication groups within the infrastructure. The communication groups will support Broad- and Multicast on the Mac- and IP-Layer. The hardware is selected to support a multitude of state-of-the-art embedded operating system, but a special focus will be put on the development with RIOT-OS (Baccelli et al., 2013).

First and foremost, the evaluation will provide measurements for execution time, memory footprint and energy consumption. Additionally, the scalability will be evaluated by increasing the testbed.

[2] https://www.iot-lab.info

4.2.2 Formal Proof of Security

Formal correctness of security protocols is common practice nowadays. However, these proofs usually only consider the protocol itself and not the systems implementing them. The main reasons for missing formal definitions are the variety of systems using such protocols and the potential complexity of the definition itself.

With constrained systems, the device classification could be used for a high-level formal description of systems. Embedded firmware is less complex than regular operating systems, making a formal definition more valuable. The thesis at hand is going to evaluate security of different networking protocols using the aforementioned terminology for constrained systems under a certain security goal with formal models.

5 EXPECTED OUTCOME

The thesis is going to instantiate the necessary key management actions during a group's life cycle with different networking protocols securing the process. This allows the evaluation of different protocols / technologies in each of the steps by formal and practical analysis. With this analysis at hand, optimizations on the different aspect are expected to provide valuable results for research, especially in the following aspects:

I. Communication Protocols are numerous in IoT-scenarios, but many of them lack security features because of restriction in packet sizes, etc.

Outcome: Optimizing state-of-the-art protocols offering *confidentiality*, *integrity* and *authenticity* during the communication, so that they can be used by application developers without having to deal with the security details. Special focus will be put on the protocols *IPsec/ESP*, *TLS* and *DTLS*.

II. Group Key Management Protocols are often inefficient, as the Key Manager is a very critical role for the security of the system. In order to provide secure, but efficient solutions for constrained environments the key management protocols should not generate unnecessary overhead. Additionally, it needs to allow efficient key distribution, e.g. in form of key hierarchies for all security aspects of the communication.

Outcome: Embedding efficient key distribution in low-overhead key management protocols.

III. Trust needs to be built before the actual communication happens. However, once established, the trust should not come with high requirements for networking and storage capabilities of the devices, e.g. in form of difficult key infrastructures (such as X.509). Identity Based Signatures (IBS) is a technique, which offers the minimization of overhead during the communication if strong trust relationships are built before the communication.

Outcome: A solution how pre-build trust can be used to improve the efficiency of the system, e.g. by using and optimizing IBS schemes. Additionally, these solutions are going to be embedded in the previously evaluated *Communication Protocols* and *Group Key Management Protocols*.

IV. Provable Security the constraints of the considered system may allow to prove security by using the terminology provided by (Bormann et al., 2017).

Outcome: A methodology to evaluate constrained system security on a „per-scenario bases".

6 STAGE OF RESEARCH

Based on the expected outcome shown in Section 5, the current state of research and the next steps are as follows:

I. Communication Protocols: Work has been published regarding the efficiency of cryptographic algorithm combined with TLS and IPsec for constrained devices (Migault et al., 2015). Based on that, recommendations and a new compression mode for IPsec (called „Diet-ESP" or „ESP Header Compression, EHC") was published in the research community(Migault et al., 2017) and the latter was proposed to the standardization body of the *IETF*. This goes together with another optimization called *Implicit IV*. The IETF WG in charge for IPsec recently adopted *Implicit IV*– which will be published as an RFC this year – and accepted ESP Header compression as a working item for the charter. Additionally, an evaluation of secure group communication protocols has been published (Guggemos et al., 2017) different authentication protocol are currently being implemented for publication in the open-source community.

Next Steps are to include new authentication mechanism into the existing protocols and evaluate their efficiency.

II. Group Key Management Protocols (GKMP): There are three active research tasks regarding this aspect. First, a survey on key management protocols has been started and a minimization for one of such protocols (namely Group-IKEv2) has been published (gentschen Felde et al., 2017). This effort is considered as part of the standardization of a new, IKEv2-based, GKMP currently being proposed within the IETF. Second, efforts on a key distribution scheme being more efficient than the widely used *Logical Key Hierarchy (LKH)* are about to be finished and will be published soon (the corresponding paper is work in progress). At last, a laboratory for researching efficient group management is going to be finished soon[3].

Next Steps are about the efficiency of the protocols for the potential use case of updating firmware on constrained devices.

III. Trust: Work evaluating IBS has started and first results will be published soon. The first focus was on practical advantages and disadvantages compared to classical solutions such as X.509. With this at hand, there is ongoing effort in researching hierarchical IBS schemes in constrained group scenarios, focusing on its efficiency for constrained networks.

Next Steps are a practical solution on how the key hierarchy has to be managed and distributed.

REFERENCES

Ahlgren, B., Dannewitz, C., Imbrenda, C., Kutscher, D., and Ohlman, B. (2012). A survey of information-centric networking.

Baccelli, E., Hahm, O., Gunes, M., Wahlisch, M., and Schmidt, T. (2013). Riot os: Towards an os for the internet of things. In *2013 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pages 79–80, Piscataway, NJ. IEEE.

[3] http://mnm-team.org/projects/embedded

Bormann, C., Ersue, M., and Keranen, A. (2014). Terminology for constrained-node networks. RFC7228.

Bormann, C., Ersue, M., Kernen, A., and Gomez, C. (2017). Terminology for Constrained-Node Networks. Internet-Draft draft-bormann-lwig-7228bis-02, Internet Engineering Task Force. Work in Progress.

Djamaa, B., Richardson, M., Aouf, N., and Walters, B. (2014). Unicast/multicast performance in single-hop duty-cycled 6LoWPAN networks. In *9th International Symposium on Communication Systems, Networks & Digital Signal Processing (CSNDSP), 2014*, pages 140–145, Piscataway, NJ. IEEE.

Farrell, S. (2018). Low-Power Wide Area Network (LPWAN) Overview. RFC 8376.

gentschen Felde, N., Guggemos, T., Heider, T., and Kranzlmüller, D. (2017). Secure group key distribution in constrained environments with ikev2: (under review). In *2017 IEEE Conference on Dependable and Secure Computing*, Taipei, Taiwan. IEEE.

Guggemos, T., Felde, N. g., and Kranzlmüller, D. (2017). Secure Group Communication in Constrained Networks - A Gap Analysis. In *The 1st 2017 GLOBAL IoT SUMMIT (GIoTS'17)*, Geneva, Switzerland. IEEE.

Haus, M., Waqas, M., Ding, A. Y., Li, Y., Tarkoma, S., and Ott, J. (2017). Security and privacy in device-to-device (d2d) communication: A review.

Kushalnagar, N., Montenegro, G., and Schumacher, C. (2007). Ipv6 over low-power wireless personal area networks (6lowpans): Overview, assumptions, problem statement, and goals. RFC4919.

Migault, D., Guggemos, T., Killian, S., Laurent, M., Pujolle, G., and Wary, J. P. (2017). Diet-ESP: IP layer security for IoT.

Migault, D., Palomares, D., Guggemos, T., Wally, A., Laurent, M., and Wary, J. P. (2015). Recommendations for IPsec Configuration on Homenet and M2M Devices. In *Proceedings of the 11th ACM Symposium on QoS and Security for Wireless and Mobile Networks*, Q2SWinet '15, pages 9–17, New York, NY, USA. ACM.

Omara, E., benjamin.beurdouche@inria.fr, Rescorla, E., Inguva, S., Kwon, A., and Duric, A. (2018). Messaging Layer Security Architecture. Internet-Draft draft-omara-mls-architecture-01, Internet Engineering Task Force. Work in Progress.

Rafaeli, S. and Hutchison, D. (2003). A survey of key management for secure group communication.

Shang, W., Wang, Z., Afanasyev, A., Burke, J., and Zhang, L. (2017). Breaking out of the cloud. In IEEE/ACM, editor, *2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation*, pages 3–13, Piscataway, NJ. IEEE.

Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. In Goldwasser, S., editor, *Foundations of Computer Science, 35th Symposium on (FOCS '94*, pages 124–134, [Place of publication not identified]. IEEE Computer Society Press.

Silva, R., Silva, J. S., Simek, M., and Boavida, F. (2008). Why should multicast be used in WSNs. In Qu, G., editor, *IEEE International Symposium on Wireless Communication Systems 2008*, pages 598–602, Piscataway, NJ. IEEE.

Singh, M., Rajan, M. A., Shivraj, V. L., and Balamuralidhar, P. (2015). Secure mqtt for internet of things (iot). In Tomar, G. S., editor, *2015 Fifth International Conference on Communication Systems and Network Technologies (CSNT)*, pages 746–751, Piscataway, NJ and Piscataway, NJ. IEEE.

Sun, Y., Gurewitz, O., and Johnson, D. B. (2008). RI-MAC: a receiver-initiated asynchronous duty cycle MAC protocol for dynamic traffic loads in wireless sensor networks. In Abdelzaher, T., Martonosi, M., and Wolisz, A., editors, *SenSys '08*, page 1, New York (NY). A.C.M.

Tiloca, M., Nikitin, K., and Raza, S. (2017). Axiom.

Yan, Z., Zhang, P., and Vasilakos, A. V. (2014). A survey on trust management for Internet of Things.