NTNU

Norwegian University of
Science and Technology

An Inter-Domain Key Management Scheme for ZigBee Networks

Ivar Tønseth

Master of Science in Communication Technology
Submission date: December 2010
Supervisor: Danilo Gligoroski, ITEM

Norwegian University of Science and Technology
Department of Telematics

Problem Description

Design a device registration and authentication model in a multi-domain ZigBee network. In general, Zigbee considers a closed domain, with one coordinator, a couple of routers and several devices. This architecture does not allow for a multi-domain operation of devices in separate domains. The task is to extend the network architecture of ZigBee to inter-domain environment, find issues in the key management and design an extended key management scheme.

Assignment given: 18. June 2010
Supervisor: Danilo Gligoroski, ITEM

Preface

This thesis summarizes the work I have undertaken during the 10th and final semester of the Master's program at the Department of Electronics and Telecommunications, Norwegian University of Science and Technology (NTNU). The project was initiated and approved by professor Danilo Gligoroski at NTNU. Three months have been spent at the Seoul National University (SNU) in Korea where professor Yanghee Choi and Dr JongMin Jeong have contributed as supervisors.

It has been very rewarding for me to write this thesis, and I have acquired insight into the area of key management and wireless networks. I would in particular like to thank my supervisor in Seoul, JeongMin Jeong, for assisting me with his great knowledge of key-management in wireless systems.

I would also like to thank both Danilo Gligoroski and Yanghee Choi for valuable input during the process of writing this thesis.

Seoul/Oslo, July/December 2010

Ivar Tønseth

Abstract

Wireless networks are increasingly penetrating new range of applications, from industry controllers, to houshold appliances. The wireless standard, IEEE 802.15.4/ZigBee, combines simple operation with low power consumption. This type of network is increasingly utilized as a mechanism to monitor, survey, sense and track.

This thesis presents a multi-domain device registration and authentication model built on key pre-distribution mechanisms in order to enable nodes from different operational managements to interact. Little research has been done in the area of inter-domain communication in sensor networks. Even so, this may be an important feature to sensor networks which can open up for new services.

Two novel suggestions for a multi-domain model are presented; hierarchical inter-domain random pool (HIDRP), and interactive inter-domain random pool (IIDRP). The HIDRP scheme relies on a single global key-pool containing all keys which will be used by sub-domains, thereby acting as the equivalent of a root CA. The IIDRP scheme on the other hand, is based on the assumption of domains containing keys derived separatly without correlation. Devices from foreign domains will accordingly have no common key-material to which key-establishment can successfully be acomplished. Sharing common keying material happens by the exchange of keys between the coordinator nodes in each domain. The nodes will then be able to derive a shared secret key to enable authentication.

Since there are no protocols for inter-domain communication in the ZigBee protocol, the first step will be to provide architectural changes that will enable this function. Furthermore, a procedure to share network keys or link-keys for devices in different domains will have to be designed.

In the HIDRP scheme, the numerical analysis was performed to evaluate the key connectivity in relation to the size of keys involved in the distribution. The analysis showed that as the global key pool size increased, the link

connectivity decreased. Furthermore, no correlation was shown between key connectivity and the size of the local key pool. Only the size of the global key pool and the key ring affected the link connectivity.

In the IIDRP scheme, numerical simulation was performed in order to measure the round-trip-time (RTT) for link-key aquisition in a foreign domain. The results showd that as the number of hops increased between the node and the sink, so did the RTT.

Contents

List of Figures

Abbreviations

CSMA/CA Carrier Sense Multiple Access with Collision Avoidance

IEEE Institute of Electrical and Electronics Engineers

LR-WPAN Low-Rate Wireless Personal Area Network

MAC Medium Access Layer

PHY Physical Layer

FFD Fully Function Device

RFD Reduced Function Device

WLAN Wireless Local Area Network (IEEE 802.11 a/b/c)

GKP Global Key Pool

LKP Lokal Key Pool

KR Key Ring

Definitions

Link-key Symmetric key shared exclusively between two neighbour devices, obtained if both devices share same key.

Path-key Symmetric key shared exclusively between a device and its target device, obtained

Shared-key discovery Act of establishing a shared secret key between two nodes based on their share common key

Sink node The coordinator node occupied by one node in a domain

Path-key establishment Act of establishing an alternative route through established links

Re-keying The act of renewing a key upon compromization

Probabilistic key sharing Key distribution based on the probability of two nodes sharing at least one common key

Key-Ring Symmetric keys stored in a node used to establish a secure link to another node

Chapter 1

Introduction

1.1 Sensor Networks & Domains

Sensor networks are increasingly becoming more emerging, and new possibilities and technical innovations are made possible without the limitations imposed by the physical wire. Sensor networks are simple, robust and self-controlling. They are characterized by a range of sensor nodes running on battery power, often with low computational capabilities and memory. Due to the simple hardware architecture and efficient manufacturing procedures, sensor networks can perform various tasks and may prove to be an economically feasable solution to many services and applications. Today, sensor networks are used to perform monitoring, surveillance, sensing, tracking, and measuring operations[3].

The main focus in this thesis is the type of networks used by ZigBee, namely LR-WPANS (Low-Rate Wireless Personal Area Network). A LR-WPAN is characterized by low power-consumption, and low cost of deployment. The range is short, and it is optimalized to convey information over short distances[14]. According to the Task Group 4 under the IEEE 802 Working Group 15, the goal is to provide a standard which has the characteristics of ultra-low complexity, low-cost and extremely low-power for wireless

connectivity among inexpensive, fixed, portable and moving devices[8].

Sensor networks are in theory considered as a closed environment[9]. However, the evolution of the WPAN standard are seeking towards both mobile and stactic devices, allowing for a highly dynamic network. As such, devices should be able to drift from one location to another. Such a scenario might be troublesome with the architecture which forms the foundation of existing networks. In this context, devices in a WPAN may have to increase their functional operating space. In this way, devices in a WPAN or a ZigBee network will have the ability to extend their physical operational area to provide services beyond their home domain. Devices can thereby interconnect with other devices and applications not limited to their home domains operations. Such a feature could open up to new services where mobile nodes could interact and share information on a more diverse level than the static operations found by existing sensor networks. Today, the ZigBee protocol does not support devices to drift outside their home domain to interact with devices from other domains; inter-domain communication is not supported.

Extending the sensor network architecture to enable inter-domain communication will place some important restrictions on authentication. Imagine a sensor device loaded with sensitive information passing by a stationary node. The stationary node initiates a communication request but does not have the requried permissions. As a result, a key-agreement procedure is declined, and the sensitive information is not compromized. This scenario emphasizes the importance of proper authentication mechanisms in an inter-domain environment.

ZigBee enables device authentication mechanisms based on shared symmetric key. When a device enters a domain, a symmetric key is derived from preinstalled or out-of band obtained trust information[13]. Two devices will derive a shared symmetric key with each other based on the trust information given. As long as this process has been executed by all participating devices in a network, the domain is protected from unauthorized access by restricting access to only authorized devices sharing a symmetric key. This process has to be repeated between every device that enters a certain do-

main. With hundreds of devices in a network, the task of authentication becomes a burden. As such, this scheme does not scale well. Furthermore, devices that originate from different administrative domains will not be able to communicate.

There exists several different key management schemes for wireless sensor networks, such as random pool-based, matrix-based, polynomial-based, and location based[9]. These schemes are based on the act of pre-loading key material into the devices prior to deployment. The keys are first generated in a key pool, which are then randomly distributed in subset proportions onto the devices. These keys form the key ring of the node, and forms the basis of shared symmetric key aquisition between two nodes. The successfulness of this scheme relies on predicting the expected node-degree, such that the random graph that forms at key set up is as connected as possible[3]. Key pre-distribution is thus chosen as the key-management model which the propsed scheme introduced later in the thesis, is based upon.

1.2 Related work

Little resarch has been done in the area of multi-domain device registration and authentication in sensor networks. Most research I could find on the topic of inter-domain communication is related to routing protocols. Especially, there has been extensive research related to inter-domain authentication and routing in wired networks. This, however falls outside the scope of this thesis.

Routing protocols that tackle inter-domain challenges have been suggested. In [4], a inter-domain routing protocol (IDRM) is presented as a solution to the problem in mobile ad-hoc network. A solution to support the interoperation of networks governed by different administrative domains that employ different routing protocol designs, metrics and policies is given. This topic contrasts the main focus of the thesis, which is domains in which the key-delegation separates the two.

In [10], trust management in inter-domain scenarios are investigated. The

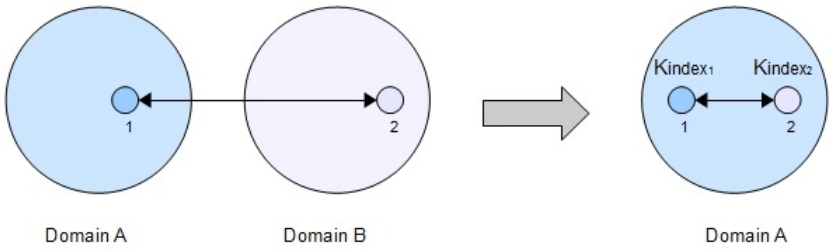

Figure 1.1: Problem description for open domains

paper introduces a design of an inter-domain PKI infrastructure in order to establish trust relationships for organizations to protect communication channels, or access to resources and internal data. However, relying on the pubic key infrastructure, this scheme deemes not to be applicable in WPAN networks.

1.2.1 Objectives

Figure 1.1 illustrates the problem of inter-domain authentication and device registration in current ZigBee networks. Node 2 from domain B is entering domain A, and wants to communicate with node 1 with home domain A. Because the key pool, KP, of domain A and B are different, there are no common key material in the key-ring, KR, of node 1 and 2. I.e., since
$KP_A \cap KP_B = \emptyset$,
$KR_1 \cap KR_2 = \emptyset$.
Consequently, both nodes will never succed in generating a link-key. This is the obstacle in multi-domain operations.

Thus, the purpose of this thesis is

- to give an overview of the IEEE 802.15.4/ZigBee protcol and general key distribution schemes

- to design a solution to device registration and authentication in a multi-domain environment
- to present the results of perfomance evaluation and numerical analysis of the design

1.2.2 Structure

This paper is organized as follows: Chapter 2 will give an introduction to ZigBee/802.15.4 networks, and an overview of general key management schemes. Chapter 3 gives the overall design structure of HIDRP and IIDRP with illustrative examples. Chapter 4 gives an evaluation and results of numerical analysis of the HIDRP scheme, and of the performance simulation of the IIDRP scheme. In chapter 5, a discussion is given based on the results. In chapter 6 conclusive comments are given which summarizes the thesis.

Chapter 2

Background

In this section some background theory and technological aspects that are useful for a better understanding of the analysis later in the thesis are presented.

2.1 IEEE 802.15.4/ZigBee

The IEEE 802.25.4 is a standard that defines the protocols and interconnections in a Wireless Personal Area Network (WPAN). The standard has been developed for the purpose of making a low power-consuming, reliable, low data-rate, near range data transfer protocol. ZigBee is the name for a standard that relies on the lower layers defined by the IEEE 802.15.4 standard. The ZigBee Alliance, the group of companies behind the standard, has targeted a low-cost and low-power consuming wireless communication standard. ZigBee technology is aimed towards consumer electronics, home and building automation, industrial controls, PC peripherals, medical sensor application, toys, and games[13].

The IEEE 802.15.4 standard defines two levels in the protocol hierarchy, namely the physical layer (PHY) and the medium access control layer (MAC). The purpose of only defining these two layers makes it easy for vendors

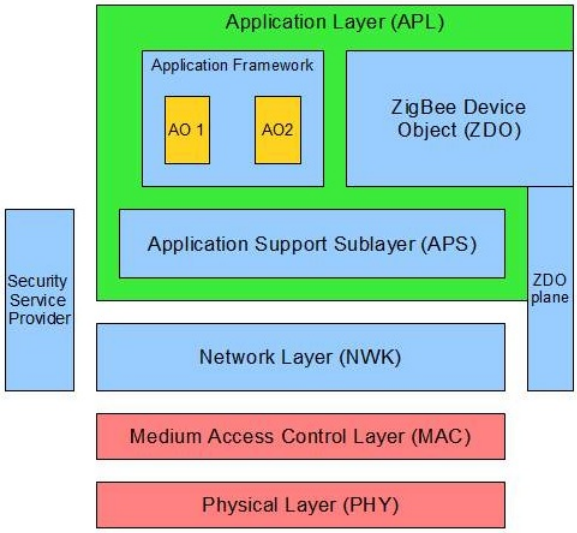

Figure 2.1: Protocol architecture of IEEE 802.15.4/ZigBee

to define a certain behaviour by customizing the upper layers. The main characteristics of the IEEE 802.15.4 protocol will still be the same. The ZigBee specification on the other hand, defines the two layers on top of the PHY and MAC layers, namely the network layer (NWK) and the application layer (APL). Figure 2.1 shows the protocol architecture of both ZigBee and the IEEE 802.15.4.

The layers depicted in Figure 2.1 are organized according to which layer that provides a service to another layer. The bottom layer will provide a service through a SAP (Service Access Point) interface to the layer directly above and so forth. The top layer, (Application Layer), will provide the end service to the user.

2.1.1 Physical Layer (PHY)

The physical layer is the lowest layer in the protocol stack, and hence and endpoint of transmission and reception of packets across the physical medium. It constitute the fundamental layer where data is transmitted as raw bits, in contrast to frames and packets formats provided by the higher-levels. The physical layer has a number of operational tasks. This includes activation and deactivation of the radio transceiver, energy detection, link quality indication, channel frequency selection, clear channel assessment for CSMA-CA (Carrier Sense Mulitple Access with Collision Avoidance), and data transmission and reception[7].

2.1.2 Medium Access Layer (MAC)

The MAC layer provides an interface between the APL and the PHY layer. The MAC layer handles a number of tasks such as channel access, providing reliable transmission mechanisms, and synchronization (between to peer MAC entities). Radio channel access is controlled using CSMA-CA. The layer generates beacons to support synchronization, and network beacons if the device is a coordinator. The MAC layer also supports device security, PAN association and disassociation, handling and maintaining the Guaranteed Time Slot (GTS) mechanism[7].

2.1.3 Network Layer (NWK)

The NWK layer is responsible for delivering data frames across the network to either the final destination node, or along the path through an intermediate node. Data frames are generated at this layer to convey application layer protocol data units to the destination. At this level there are three types of functional devices: ZC (ZigBee Coordinator), ZR (ZigBee Router), and ZED (ZigBee End Device). The layer performes a number of network management tasks, among them network discovery and formation, address

allocation, collecting routing information, route discovery, and network wide security. The layer is optimized to allow for low power devices to maximize their battery life [13]

2.1.4 Application Layer (APL)

The Application Layer (APL) consists of the application support sub-layer (APS), the ZDO (ZigBee Device Object), and the manufacturer-defined application objects. The APS layer form an interface between the NWK layer and the APL layer through a group of services that are used by the ZDO and the manufacturer-defined application objects. The application framework is where the application objects are hosted on ZigBee devices. 240 distinct objects can be defined, each with a unique endpoint address from 1 to 240. The ZDO is a base class of functionality providing an interface between the application objects, the device profile, and the APS. It is responsible for the APS layer, the NWK layer, and the Security Service Provider. Furthermore, it assembles configuration information from the end applications to determine and implement discovery, security management, network management, and binding management[13].

2.1.5 LR-WPAN topology

The NWK in the ZigBee protocol standard supports both star, tree and mesh topologies, as depicted in Figure 2.2. In a star topology, the coordinator is the central device responsible for initiating and maintaining the devices on the network. All devices with a direct link to the coordinator are called end devices. In mesh and tree topologies, the coordinator is responsible for starting the network and other key network parameters. Here, certain nodes can act as a router which will allow the network to expand the topology to form trees or a mesh networks. The communication flow can thereby happen in an ad-hoc manner, where router nodes forward data traffic. However, only the routers can rely traffic. An end device will not be able to forward traffic,

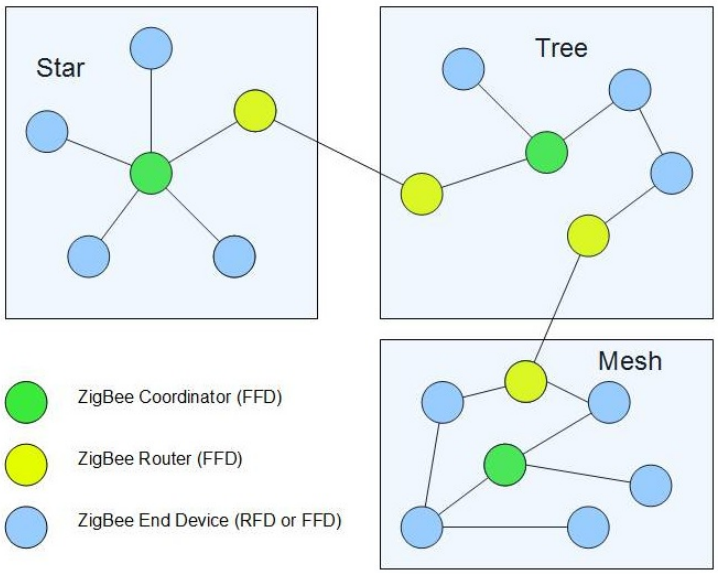

Figure 2.2: Network Topology

only receive. Thus, data flow in this type of network can be realized either as unicast (link-wise), or multicast (network-wise)[2].

A ZigBee device can be categorized into two different types according to its hardware configuration. The device can either be a fully functional device (FFD) or a reduced functional device (RDF). FFDs are devices with a hardware configuration which allows the device to perform advanced operations such as routing and control management. The coordinator device in a network is always a FFD. RFDs on the other hand has simpler hardware structure which limits its operational activity. These are end devices which can not act as a router[2].

2.1.6 Security mechanisms

There are several mechanisms in the ZigBee specification including key establishment, key transport, frame protection, and device management, which all

are part of the security services. The ZigBee security architecture includes security mechanisms at the NWK layer and the APS layer. In addition to security for their respective frames, the APS layer also provides establishment and maintenace of security relationships.

Two security modes are defined in the ZigBee specification; high security mode, and standard security mode. High security mode is designed for commercial applications where strict security policies are applied. In this mode the Trust Center will have to store a list of devices, master keys, link keys and network keys, which it needs to enforce the policies. Standard security mode is designed for lower-security residential applications. The Trust Center may maintain a list of devices, master keys, link keys and network keys with all the devices in the network. However, memory requirements for the Trust Center are lower in this mode than in high security mode[13]

ZigBee encryption is based on the 128-bit AES standard. Encryption is available at the network level or device level. At the network level encryption is done using the network key, while at the device level the encryption is achieved using the link keys between every pair of nodes[1].

2.1.7 Key Management

The security in ZigBee is upheld by a set of keys distributed in the network[13]. ZigBee utilizes symmteric key distribution which is applied when secure communication is required. Symmetric key, in contrast to PKI where pairs of a private and public keys are used, uses only one key in the prosess of encryption or verification. The keys, depending on type, can be deployed to several layers in the protocol stack. There are three main types of keys used in the ZigBee key management scheme. These are:
Link keys: Used to secure unicast data transfer between two application-layer peer entities. The key is 128-bit long, unique to every pair of communicating devices. A device can obtain a link key by key-transport, derive it by key-establishment, or be preinstalled in the device. The link key is used to generate specialized uncorrelated keys using a one-way function.

Network key: A unique 128-bit key shared by all devices in a ZigBee network. The network key is used to secure broadcast messages. The network key can either be acquired via key-transport or be pre-installed in the device. Two different types of network keys are available depending on the security requrements; standard security network key and high security network key. The practical implication of using either high security or standard security is how the network key will be distributed, and it may also control how network frame counters are initialized. The network key and the associated outgoing and incoming frame counters should be available to both NWK layer and APL layer.
Master keys: Used in the key-establishment protocol (SKKE) for acquiring link keys, and is the basis for long-term security between the two devices. The master key may be obtained from the Trust Center via key-transport, be pre-installed during manufacturing, or may be based on user-entered data (i.e. PIN).

Secure initalization and installation of these keys are vital on order to upheld security between two devices[13].

2.1.8 Key Establishment

The key establishment produces the *link-key* and it is undertaken at the Application Support Sublayer (APS)[13]. Initial trust information, such as the master key, must be installed in each device prior to running the key establishment protocol. The master key can also be provisioned in-band or out-of-band. Between two devices, one takes the role as an initiator device, the other one as a responder device. The initiator will then instansiate an APSME-ESTABLISH-KEY.request primitive at the higher layer. This command will prompt the initiation of the SKKE (Symmetric-key key establishment) protocol. Four frames are sent between the devices as part of the SKKE protocol. If no error conditions occur during the execution, both the responder and the initiator device shall consider the derived key as their newly shared link key.

2.1.9 Trust Center

In a ZigBee security domain, an entity is given the role as the *Trust Center*[13]. Only one device on the network serves as the Trust Center. This entity is responsible for allowing devices into the network, and the distribution of keys in order to fullfill trust management, network management, and end-to-end configuration management. The Trust Center role is ususally occupied by the coordinator device, and each secure network shall have only one Trust Center. Each devices communicates with its Trust Center based on either the master key or network key. In high-security networks, the master key and address of Trust Center is either pre-installed, or sent via in-band unsecure key transport. In low-security networks, a device communicates with its Trust Center using the current network key, which can be preconfigured or sent via an in-band unsecured key transport. If initial trust-information is not pre-loaded, the Trust Center role defaults to the ZigBee coordinator[13]. The Trust Center role is the equivalent to the sink node as reffered to later in the thesis.

2.2 Key distribution protocols

There are three types of general key agreement schemes commonly used in key management. These are *trusted-server* scheme, *public key* scheme, and *key pre-distribution* scheme[5].

The trusted-server scheme relies on a trusted server which arrange key agreement between pairs of nodes. However, key schemes based on a trusted third party render impractical for large scale sensor networks because of the unknown topology prior to deployment, communication range limitations, intermittent sensor-node operations, and network dynamics[6]. Furthermore, this type of key distribution is dependent on a trusted infrastructure, which may not exist in a sensor network[5]. Moreover, traffic load on selected nodes acting as a trusted-server will likely result in an unbalanced traffic load[5].

Public-key infrastructure (PKI) is commonly used in data security, but is considered to require extensive processing power which makes the system unpractical to be used solely as a key distribution system in sensor networks[11].

The third option of key distribution is *pre-distribution*. This scheme relies on key material being generated and loaded onto devices prior to deployment, and is considered the only practical option for the distribution of keys to sensor nodes of large-scale sensor networks [6]. Pre-distribution of keys is therefore chosen as the basic key-distribution scheme when designing a solution for multi-domain sensor networks.

There are however different pre-distribution schemes to be considered. A brief introduction follows on the most relevant schemes.

2.2.1 Key Pre-Distribution

Key Pre-distribution is the act of pre-loadings sensor with keying material prior to deployment. One solution is to generate pairwise keys based on a single *mission* key, carried by all nodes. This simplicity greatly reduces resillience; if one node is compromized, the security of the entire network will also be compromized[11].

Another solution is to implement *n - 1* unique secret pairwise keys in all *n* nodes in the nework. For a node, every key out of the *n - 1* will be matched with a specific node with the corresponding key. This scheme offers optimal resillience because one compromized node does not affect the security between other nodes. However, since memory capacity requirements increase with the increase in number of nodes, this scheme may not be suitable for a large sensor networks[11].

2.3 Random key-predistribution (RKPD) scheme

Eschenauer and Gligor [6] has proposed a random key-predistribution (RKPD) scheme which relies on *probabilistic* key sharing. The scheme relies on calculating the probability of obtaining a certain level of *network connectivity*. Network connectivity is the degree of connected nodes in a network, i.e. sensor nodes that have a communication path between them. The number of keys that needs to be stored in each sensor node is based on the required probability that any two nodes share at least one key[12]. Three steps that form the basic steps of the key distribution scheme are outlined and explained:

- **Key pre-distribution phase**
  Prior to deployment, a large pool of P keys (e.g. $2^{17} - 2^{20}$ keys) is generated off-line together with their corresponding key identifiers. Each node randomly picks k keys from P without replacement, which will then form the key-ring of the node. The key identifiers of the key ring, together with the associated sensor identifier are then stored on a trusted controller node.

- **Shared-key discovery phase**
  During network initialization, every node discover its neighbours (i.e. nodes within wireless range of each other) with which they share a key with. Nodes discover if a neighbour share a key with it by receiving a broadcasted list of the key identifiers of its neighbours key-ring. If a node shares a common key with its neighbour, they mutually authenticate to verify that the other node actually has posession of the key. All traffic between these two nodes will be secured by link encryption. This key will from now on be referred to as a *link-key*.

- **Path-key establishment phase**
  After the shared-key discovery phase, if a node does not share a common key with one of its neighbours, they do not share any common keying material. However, the nodes can still securely communicate by establishing a *path-key* to the nodes if they are connected by two or

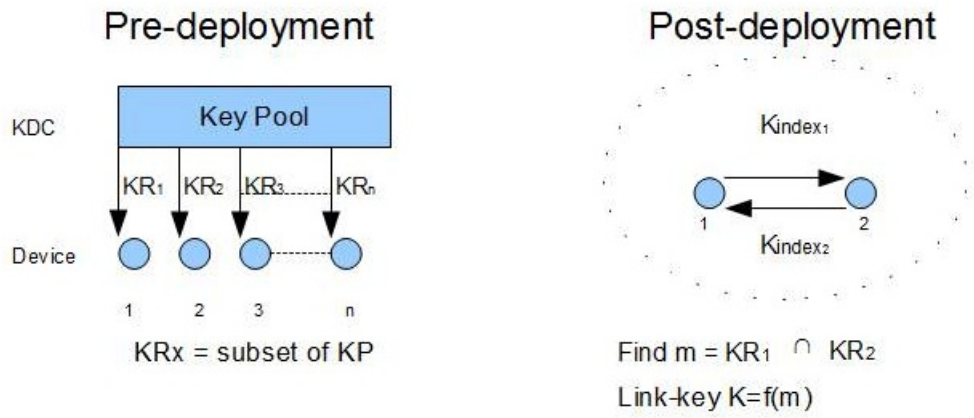

Figure 2.3: RKPD

more secure links. All communication between the nodes will be then passed along this path via secure links.

Figure 2.3 shows the pre-and post deployment phase of RKPD. In the pre-phase, a subset KR_i for node i is selected by the KDC, which is then stored in the node. In the post-phase, node 1 and 2 sends its KR index, K_{index} to each other. Subsequently, both nodes find $m = KR_1 \cap KR_2$, and then generate a link-key with a function of $f(m)$

Revocation

Upon node compromisation, the affected key ring should be revoked and replaced. The controller node broadcasts a signed and encrypted list of k key identifiers for the key ring to be revoked. After receiving the list, and verifies the signature, the node locates those identifiers in its key ring, and remove the corresponding key (if any). After revocation, some links may disappear and will have to be restored by running the shared-key discovery phase, and if necessary, the path-key establishment.

Chapter 3

Proposed Scheme

The RKPD scheme has some advantages wich make it suitable as key distribution scheme compared to for example PKI. The operation and management of the RKPD scheme is simple. Compared to the complexity of PKI (i.e. private/public key, CA), the RKPD scheme does not require extensive infrastructre. Secondly, RKPD is independent of location information. This means that knowledge of deployment topology is not required in order to guarantee an acceptable connectivity. Third, this scheme requires only a constant size of memory in order to store keying material regardless of the network size. Owing to its simplicity for the resource constraints in sensor networks, RKPD is an efficient solution for an open-domain environment as well.

In the following, a design to an open-domain environment for device registration and authenticated is presented. Two solutions are suggested, both leveraging on the RKPD scheme. These are hierarchical inter-domain random-pool (HIDRP) and interactive inter-domain random-pool (IIDRP).

The essence of HIDRP is the global key distribution center, KDC_{Root}, managing a single key pool for each device regardless of local domains. In the case of IIDRP, each node need to perform additional interactions to establish shared secret keys compared to the basic RKPD scheme.

Probability analysis for the first scheme and performance simulation for the latter scheme will be presented. The two schemes will be analysed and discussed with performance related to key connectivity and round-trip-time respectively, as important parameters.

In these scenarios, we assume that the local coordinator node (sink node) will be a node with fully functional capabilities. Both of the schemes are based on the RKPD scheme presented in chapter 2.

3.1 Hierarchical inter-domain random-pool

The hierachical inter-domain random-pool scheme uses a global key distribution center, KDC_{Root}, as the key authority. The KDC_{Root} generates a global key pool, (GKP), of size w keys, corresponding to the number of local KDC's, KDC_{Local}. If the number of sub-domains is large, the size of GKP, w, has to be correspondingly large. The GKP contain all keys that will be used by local sub-domains. The KDC_{Local} is the coordinator node, in charge of its own network domain. Figure 3.1 shows the overall schematics of the HIDRP scheme.

3.1.1 Pre-deployment phase

At pre-deployment phase, a local KDC, KDC_X, acquires a randomly selected subset of size r from GKP, which will form the key-pool, LKP_X. All nodes residing in LKP_X's domain will load a randomly selected subset of keys from KDC_X's key pool of size m. m will form the individual nodes key-ring. We assume that each KDC_X can establish a secure channel to the global KDC. Hence, each KDC_{Local} can maintain the LPK securely.

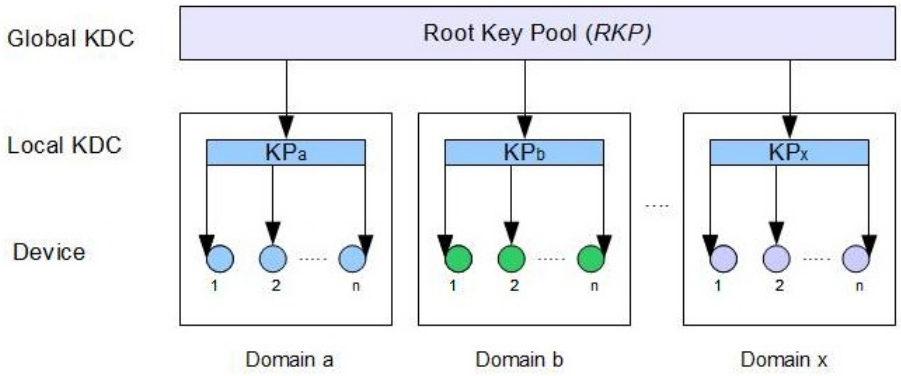

Figure 3.1: Hierarchical inter-domain random-pool

3.1.2 Key-discovery phase

The key-discovery operation is almost identical with the baisc RKPD. Key agreement and key discovery between devices whose domain is different will be executed according to the link-key discovery and the path-key discovery mechanisms in the RKPD scheme.

Because the key-ring of each device is derived from a single global key-pool, two devices originating in different domains can still share common keys. The success rate of obtaining a common key is naturally less than the basic RKPD scheme, where nodes share the same key-pool and key-ring size. This however will be analyzed in the following section.

3.2 Interactive inter-domain random-pool

IIDRP is a two-level architecture between a local key distribution center and end-devices, like the basic RKPD; there is no architectural change. In IIDRP, keys in each domain originated from the separate local key-pool have

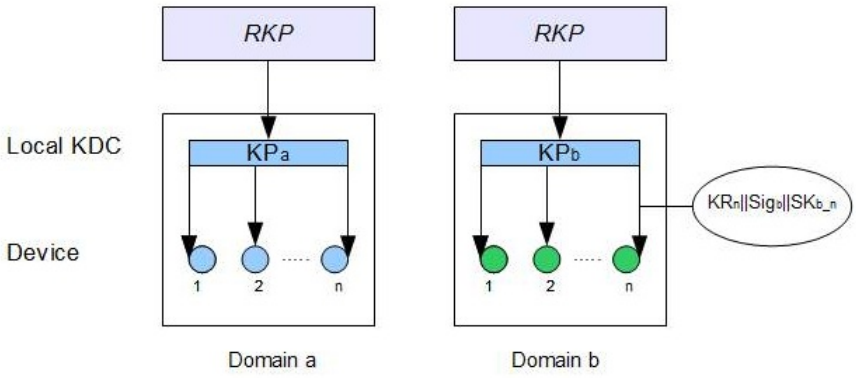

Figure 3.2: Interactive inter-domain random-pool

no correlation with key pools of other local key distribution centers. Two nodes in different domains engaged in interaction may therefore have no probability to successfully establish a link key without further interactive procedures. IIDRP is depicted in Figure 3.2. We assume every KDC_{Local} in a network has knowledge of the device ID and index of its key-ring in its own domain. Furthermore, we assume a secure wired channel between the KDC_{Local}'s.

3.2.1 Pre-deployment phase

Every node in a domain X randomly selects a key-ring of size m from LKP_X, which is exactly identical with the basic RKPD scheme. In addition to a key-ring, the nodes also receives the signature of KDC_X, Sig_a, and a symmetric key between KDC_x and each node, SK_a_n. This symmetric key will be used for securely receiving a new key-ring from a foreign KDC.

3.2.2 Key-discovery phase

Let us consider two nodes i and j, each belonging to different domains A and B respectively. Node i wants to interact with node j, and is currently within the range of node j. Node i realizes entering a foreign domain either by detecting domain broadcast beacons sent from KDC_B in the current domain, or from node j during communication initiation. Node i sends its node address to KDC_B, signature of its KDC, Sig_a, and domain name, either directly or via intermediate nodes if i is not in range of KDC_B. KDC_B then sends a message through the secure wired channel to KDC_A, requesting a confirmation of whether node i is registered with its address in domain A. If node i is a member of domain A, KDC_A replies to KDC_B with a confirmation message. This will prompt KDC_B to select a new key-ring from its key-pool, which is then sent to node i. We therefore have to assume storage capacity in every node sufficiently large to store an extra key-ring. After receiving a new key index from KDC_B, node i and j start a key negotiation process with its own key ring. This process is identical with the basic RKPD scheme.

Chapter 4

Evaluation

4.1 Numerical analysis of HIDRP

In hierarchical inter-domain random-pool, the main focus has been to investigate the key connectivity. In the following, a probability analysis is performed regarding the relation between size of both the global key-pool, local key-pool and key-ring, and how this impacts the key connectivity between two nodes from different domains.

4.1.1 Notation

- P_C : the probability that two nodes succeed in sharing a secure key
- w : size of GKP (Global Key Pool) which means GKP has w-number of keys
- r : size of Local KP (LKP)
- m : size of Key Ring (KR) for each node
- c : the number of common keys in two LKPs (say, LKP_A and LKP_B for domain A and B, respectively)
- d : the number of different keys in two LKPs, $d = r - c$
- $p_L(i)$: the probability that two LKPs have i different keys in their LKP.

This means two arbitrary LKPs share $r - i$ number of keys that are identical between two LKPs where $0 \leq i \leq r$.

- $p(i)$: the conditional probability that two nodes do not share any key under the condition of - $p_L(i)$ where $p(i) = 1$ under $i = r$.

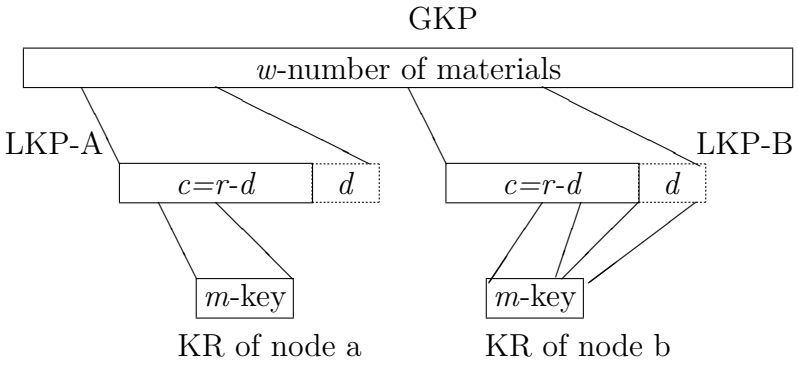

Figure 4.0 Key distribution process

Figure 4.0 illustrates the key distribution process for a node a and b. Node a and b are governed by domain A and B, respectively. The key-ring, KR, for node a and b are randomly selected from its LKP. Both LKPs are subsets randomly selected from GKP. LKP-A has up to c-number of common keys with LKP-B.

4.1.2 Probabilistic Results

P_C is calculated by 1 - Pr[two devices do not share any key in their key rings]. The probability of two end-devices do not share any keys may be affected by the distribution pattern of LKP from GKP. If two LKPs share more keys, the hit rate of two devices managed by each LKP is lager. Therefore i, the

number of different keys between two LKPs will affect the final P_C value. The goal is to calculate $P_C = 1 - \sum_{i=0}^{r} p(i) \cdot p_L(i)$.

$p_L(i)$ is related to constructing LKP from GKP while $p(i)$ is related to distributing a KR for each sensor device from its LKP.

$p_L(i)$ is calculated as follows,

$$p_L(i) = \frac{\begin{pmatrix} w \\ r-i \end{pmatrix} \begin{pmatrix} w-r+i \\ 2i \end{pmatrix} \begin{pmatrix} 2i \\ i \end{pmatrix}}{\begin{pmatrix} w \\ r \end{pmatrix}^2} \tag{4.1}$$

The total number of ways for both LKPs to pick r keys from w is $\begin{pmatrix} w \\ r \end{pmatrix}^2$. Both LKPs have $r-i$ keys in common. There are $\begin{pmatrix} w \\ r-i \end{pmatrix}$ ways to pick the $r-i$ common keys. After $r-i$ common keys have been picked, $w-(r-i)$ keys remains in GKP. The number of distinct keys between the two LKP's is $2i$. The $2i$ distinct keys should be partitioned between the two LKPs equally. The number of such partitions are $\begin{pmatrix} 2i \\ i \end{pmatrix}$.

Next, $p(i)$ is calculated as follows,

$$p(i) = \sum_{j=0}^{m} \frac{\begin{pmatrix} r-i \\ m-j \end{pmatrix} \begin{pmatrix} i \\ j \end{pmatrix} \begin{pmatrix} r-m+j \\ m \end{pmatrix}}{\begin{pmatrix} r \\ m \end{pmatrix}^2} \tag{4.2}$$

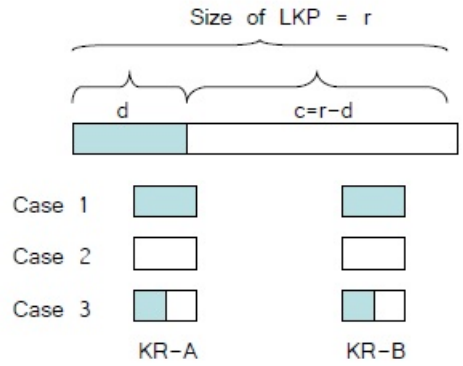

Figure 4.1: The three possible ways to select m keys from r

The way for both nodes to pick m keys from r is $\begin{pmatrix} r \\ m \end{pmatrix}^2$. There are three ways to select m keys from r, as illustrated in Figure 4.1. The first possibility is when m consists exclusively of c-numbers of common keys. The second possibility is when m consists of only d-number of distinct keys. The third possibility is when m consists of both identical and distinct portions. There are $\begin{pmatrix} r-i \\ m-j \end{pmatrix}$ ways to pick from $r-i$ identical portion and $\begin{pmatrix} i \\ j \end{pmatrix}$ ways to pick remaining j keys from the remaining i keys. $\begin{pmatrix} r-m+j \\ m \end{pmatrix}$ is the number of ways the node can select m keys without selecting any common keys with the other node.

.

4.2 Numerical Analysis

Figure 4.2 shows P_C according to variation of w and m under $r = 100$. As the number of keys in the global key-pool, GKP, increases, the probability of a successfull key-establishment between two nodes, P_C, decreases. The

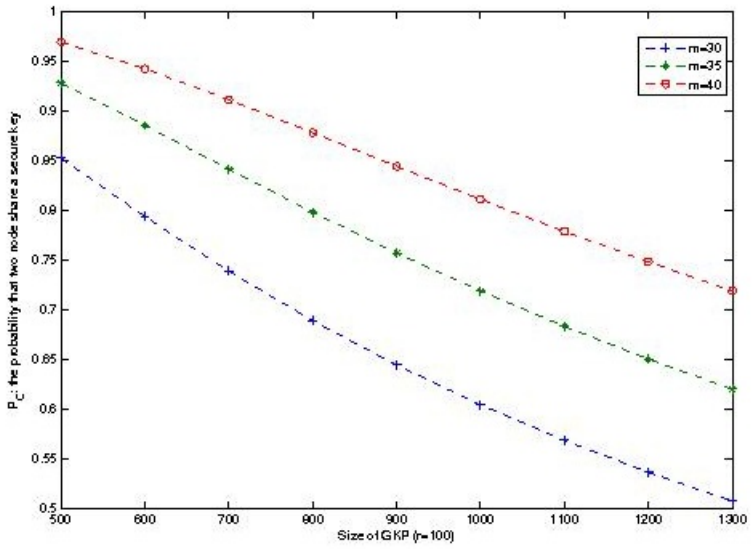

Figure 4.2: The connection rate according to size of w and m.

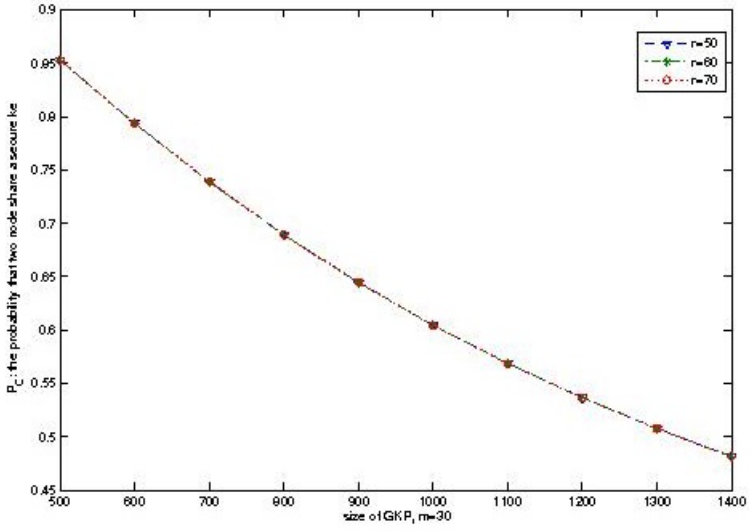

Figure 4.3: The connection rate according to size of w and r.

figure shows three functions with different inputs of m. When the size of KR increases, P_C also increases, which has an intuitative interpretation; the nodes have a better chance of sharing a common key as the total number of keys to choose from is larger. If we want to maintain P_C larger than 95%, then we have to set the size of KR for each device to 40 or more.

Figure 4.3 shows P_C according to variation of w and r under $m = 30$. Interestingly, r does not have any affect on P_C; the probability remains the same regardless of the size of LKP. As r increases, so does the probability for a key to be contained in both KDC's. However, this increase in the local key-pool decreases the chance for a common key to be picked by two nodes, i.e the success-rate for sharing a key. In fact, the increase in probability for sharing a key in the KDCs is exactly as big as the probability for not succeeding in sharing a common key with two different key-rings. These probabilities cancel each other out, and causes the success-probability to stay constant, in parallel to a zero sum game. Therefore, in HIDRP, the important values for successfully establishing a link-key between two nodes from different domains, P_C, are the size of the global key-pool, w , and the size of the key-ring, m, rather than the size of the local key-pool, r.

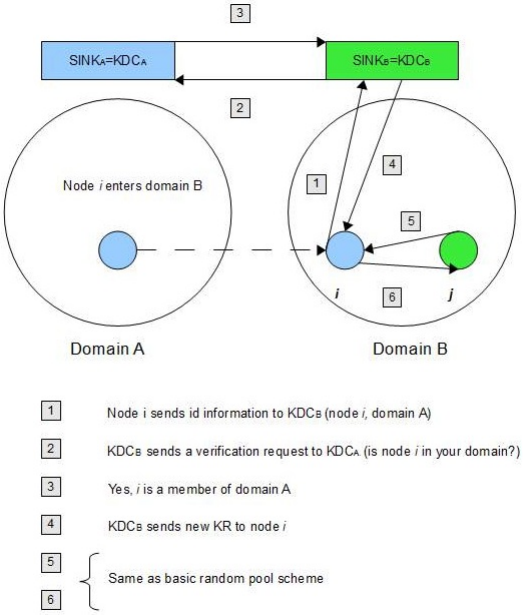

Figure 4.4: IIDRP key-discovery

4.3 Performance Evaluation of IIDRP

When a device comes within the range of a foreign domain, we cannot successfully establish a link-key, unless the keys in both domains originates from a common global key-pool, GKP. However, devices originating from different domains should be able to authenticate one another based on alternative measures. Interactive inter-domain random-pool will address this issue. Since we assume that key-distribution in this scenario has happened in an isolated manner, we do not consider initial link-and path key discovery. In this numerical simulation, the focus has been on the elapsed time from a node enters a foreign domain, to when a link-key has been successfully established between the two participating nodes. Specifically, the round-trip time, RTT, has been measured. In the following, a numerical simulation of the round-trip time of link-key acquisition in IIDRP is shown. The simulation was done in Matlab, and the results from the simulation were saved to files and analyzed using Matlab scripts.

4.3.1 Simulation Scenarios

Figure 4.4 depicts a scenario where a node from a foreign domain A enters domain B. In this case, KDC_B is a foreign KDC of node i. Upon entering domain B, node i identifies the domain by receving beacons broadcasted by the sink or a certain node in the domain. In step 2, node i sends the signature of its domain, Sig_A, encrypted by the symmetric key between the sink and node, SK_{a_i}, and the identity of both domain A, DID_A, and its own id, to the foreign sink, KDC_B. In step 3, the KDC_B acquires SK_{ai} from KDC_A and verifies Sig_A. In step 4, if Sig_A is correct, KDC_B selects a new key-ring at random and sends it to node i, encrypted with SK_{a_i}. In step 5, after receiving the encrypted new key-ring, node i can initiate the key sharing process with any node in domain A. The procedure is identical with the basic random pool scheme. In case of receiving a key-ring with no common keys with the responder device, an alternative route based on multiple link-key paths to the destination node has to be set up.

The first simulations shows the RTT in the scenario described above. The figures shows how the round-trip-time (i.e., the time from a node enters a domain to link-key is received) changes as the number of hops increases. As the simulation has been configured numerically and not by using numbers obtained by simulating real traffic, the propagation time from node to node has been predefined with a mean and standard deviation. In this example, the sink-to-sink and node-to-node values has been set to a predefined mean and standard deviation. Simulating 1000 hops, the RTT time from node to node has been generated from the delay function. This function takes the predefined mean and standard deviation as parameters, multiplies the standard deviation with the randn-function ($0.1 \leq$ x 0.99) which returns a pseudorandom value drawn from the standard normal distribution. The mean is then added to the result. This gives random RTT values close to the predefined mean.

Figure 4.5 shows the average RTT and relation of different node-to-node mean values. Average RTT is shown on the Y-axis and the number of hops

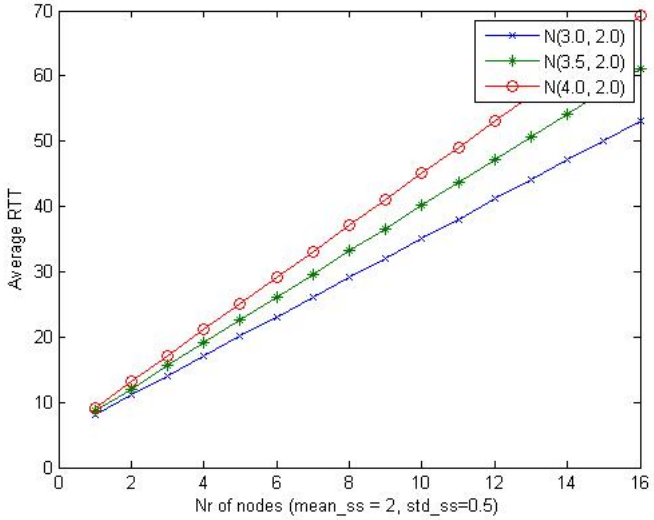

Figure 4.5: Average RTT

is shown on the X-axis. The three graphs indicate the average RTT with different predefined means, with the blue graph representing the lowest mean. The RTT value from sink-to-sink is set constant with a mean of 2 ms, and standard deviation to 0.5 ms. This value is kept constant due to the physical connection between the sink nodes, and RTT values will therefore not vary signifficantly. The total RTT has been derived from this equation: RTT = RTT_dd*(nr of hops) + RTT_ss + PTa + PTb. The signal has to go through n nodes, so this number is multiplied with the roundt trip time from node to node RTT_dd. Furthermore, sink-to-sink time is added. Finally, processing time, PTa and PTb, in the sink node is added.
As we can see from the figure, the average RTT increases as the number of hops increases in all three cases. Higher mean results in an higher growth rate of RTT, as shown by the higher rate of growth by the red graph compared to the blue graph with a lower mean.

The second simulation, shown in Figure 4.6 shows the average RTT on the Y-axis and the ratio between node-to-node RTT and sink-to-sink RTT

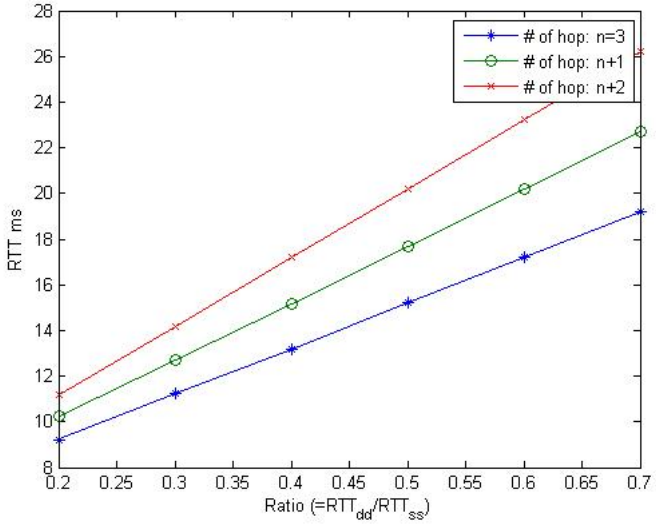

Figure 4.6: RTT ratio

on the X-axis. The blue, green, and red graph represents average RTT as the number of hops has been set to 3, 4, and 5 hops respectively. The average RTT has been derived from the same equation as the previous example, and average RTT has been calulated from 1000 simulations.
The ratio is the fraction of RTT_dd over RTT_ss. Because we investigate an effect of the variable RTT_dd and RTT_ss value simultaneously, we deploy the ratio rather than defining each value.

We consider three cases according to the number of hops between an end-device and sink node. Figure 4.6 shows that as the number of hops between the sink and an end-device increases, the total RTT gets longer. Also, as the RTT_dd gets longer compared to the static RTT_ss, the total RTT increases. Because there are multiple hops between a device and the sink, the relative propagation time for an increase in device-to-device, the total RTT proportionally increases.

Chapter 5

Discussion

Regarding HIDRP, one key issue is to determine the relative proportion of keys in the global and local key pools, in addition to the key chain that end end-devices have to store. If the number of subdomains is high, the number of keys in the global key pool should accordingly be high. The probability analysis in HIDRP showed the probability for successfully deriving a link-key between two devices related to the size of keys involved, especially the size of the global key pool and key-ring in end-device. The results from the calculation showed that in order to maintain a high probability (i.e.,>95%) of link-key establishment, the global key pool should not exceed 600 keys under the condition that the key-ring size is 40. With the size of 30 nodes, less than 500 keys in the global key pool are required in order to guarantee link-key establishment of 85% and above.

Regarding HIDRP, having one single key-pool requires careful planning and central governing. Strong requirements should be devoted on the key revocation mechanisms, since compromised keys will have to be traced back to the global pool for replacement. Subsequently, these keys have to be replaced in every domain where these keys occurred since all keys stem originally from the same key pool. To minimize this rebound effect, one could increase the total size of the key pool. However, this will result in a lower key connectivity.

One merit of RKPD is that an administrator can adjust the preferable key success rate by selecting the key pool or key ring size. Furthermore, such a variable setting can be configured once at the initial phase, that is, before node deployment. Hence, the HIDRP scheme achieves the optimized key connectivity for inter-domain sensor networks. Besides, HIDRP does not require operational changes in the end-devices.

The main difference between the HIDRP and IIDRP is that the IIDRP maintains a two-level topology like the basic RKPD scheme. IIDRP requires end-devices for additional operations for acquiring a new key ring from a foreign KDC.

The simulation of the IIDRP scheme provides an implication of the IIDRP performance according to the number of hops from an end-device to the sink. Based on the number of hops and pre-defined propagation delay between devices, the simulation results show several performance comparisons. However, it should be recognized that this simplified numerical simulation has some limitations; it does not simulate a real sensor network environment. Accordingly, the results does not reflect sensor node behaviour as a real-life simulation would have done. As a result ad-hoc behaviour, and transmission delay inherent in sensor networks are not taken into consideration. Instead, predefined values had to be set which reflect real node-to-node propagation delay. In this sense, the simulation still provides a sense on how the round-trip-time, RTT evolves over node-hops. To fully investigate the potential of IIDRP, real life simulation should be further performed.

The wired channel between the sink nodes presents some challenges. One the one hand, it provides good security with well-known security protocols such as SSL and IPSec where eavesdropping becomes much more difficult than a wireless transmission would have presented. However, this wired line might deem to cause un-negligable overhead if the geographical areas between the domains are big.

Chapter 6

Conclusion

This thesis suggest a solution to multi-domain device registration and authentication in a ZigBee network. In theory, sensor networks are considered a closed environment[9]. Even so, the scheme presented suggests that devices may not necessarily be bound to their home domain.

The subject of this thesis was to propose a scheme in order to enable inter-domain communication by nodes in separate domains in a ZigBee network. Two novel schemes for this purpose has been suggested, IIDRP and HIDPR. Both schemes leverages on the basic RKPD scheme for the distribution of keys. The two schemes differ in how the link-keys are obtained. HIDRP solves inter-domain communication by distributing keys hierarchical using a global key pool, while IIDRP relies on on-site key-sharing from distinctive key-pools to establish a link-key. In contrast, ZigBee uses a master key, provisioned by pre-installment or by the Trust Center to derive the symmetric key. A node that has not been pre-installed with trust information, or been loaded with user-entered data, has no possibilities to join a foreign network.

The numerical analysis in HIDRP showed the link-connectivity probability when different amounts of keys were deployed. It showed that by increasing the number of keys, m, in the key-ring, an increase in the connection rate could be observed. However, as the number of total keys in GKP increased,

the connection rate declined. A doubling of the key-pool size resulted in 15% decline in the connection rate. Furthermore, the graphical calculation showed that the size of LKP, r, did not affect the connection rate when the key-ring size was kept constant. Hence, the important parameters for determining the key connectivity are the size of GKP, and the size of the key ring KR.

The IIDRP scheme gives an effective solution to the inter-domain problem when the domains does not inherit keys from a single KDC_{Root}. IIDRP assumes a wired secure channel between the participating KDC_{Local}'s. The simulations was done in order to investigate the round-trip-time from when a node enters a foreign domain, to when it has obtained the key ring. The results of the simulation showed that as the number of hops between the foreign node and KDC_{Local} increased, so did the RTT.

6.1 Future work

A natural step to further advance or enhance the structure of the propositions will be to implement the schemes in a real simulation environment in order to get key value parameters. The HIDRP scheme should be evaluated based on node compromise fraction, which has not been evaluated here. Also, this scheme depend on strong security mechanisms in order to guarantee reasonable authentication. As such, security in the key delegation process should be investigated further. The IIDRP should be tested on the performance of link-key aquisition in a real simulation environment.

Bibliography

[1] P. Baronti, P. Pillai, V.W.C. Chook, S. Chessa, A. Gotta, and Y.F. Hu. Wireless sensor networks: A survey on the state of the art and the 802.15. 4 and ZigBee standards. *Computer Communications*, 30(7):1655–1695, 2007.

[2] S.A. Camtepe and B. Yener. Key distribution mechanisms for wireless sensor networks: a survey. *Rensselaer Polytechnic Institute, Troy, New York, Technical Report*, pages 05–07, 2005.

[3] H. Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor networks. 2003.

[4] C.K. Chau, J. Crowcroft, K.W. Lee, and S.H.Y. Wong. IDRM: Inter-Domain Routing Protocol for Mobile Ad Hoc Networks. *University of Cambridge Technical Report UCAM-CL-TR-708*, 2008.

[5] W. Du, J. Deng, Y.S. Han, P.K. Varshney, J. Katz, and A. Khalili. A pairwise key predistribution scheme for wireless sensor networks. *ACM Transactions on Information and System Security (TISSEC)*, 8(2):258, 2005.

[6] L. Eschenauer and V.D. Gligor. A key-management scheme for distributed sensor networks. In *Proceedings of the 9th ACM Conference on Computer and Communications Security*, pages 41–47. ACM, 2002.

[7] IEEE Standard for Information Technology. IEEE 802.15.4a Standard (2007) Part 15.4. *Amendment to IEEE Std 802.15.4^{TM}-2006*, ??, 2007.

[8] I. Howitt and J.A. Gutierrez. IEEE 802.15. 4 low rate-wireless personal area network coexistence issues. In *Wireless Communications and Networking, 2003. WCNC 2003. 2003 IEEE*, volume 3, pages 1481–1486. IEEE, 2003.

[9] J. Jeong and Z.J. Haas. Predeployed secure key distribution mechanisms in sensor networks: current state-of-the-art and a new approach using time information. *Wireless Communications, IEEE*, 15(4):42–51, 2008.

[10] G. Lopez Millan, M. Gil Perez, G. Martinez Perez, and A.F. Gomez Skarmeta. PKI-based trust management in inter-domain scenarios. *Computers & Security*, 29(2):278–290, 2010.

[11] A. Perrig, R. Szewczyk, JD Tygar, V. Wen, and D.E. Culler. SPINS: Security protocols for sensor networks. *Wireless networks*, 8(5):521–534, 2002.

[12] R.M.S. Silva, N.S.A. Pereira, and M.S. Nunes. Probabilistic key management practical concerns in wireless sensor networks. *Journal of Networks*, 3(2):29, 2008.

[13] Z.B. Specification. ZigBee Document 053474r17. *Release r17, Zigbee Alliance*, 17, 2008.

[14] J. Wang, Z. Lan, C.W. Pyo, T. Baykas, C.S. Sum, M.A. Rahman, J. Gao, R. Funada, F. Kojima, H. Harada, et al. Beam codebook based beamforming protocol for multi-Gbps millimeter-wave WPAN systems. *Selected Areas in Communications, IEEE Journal on*, 27(8):1390–1399, 2009.