Security and Privacy for Wireless Ad-hoc Networks

By

Audun Pettersen
Frode Åsen

Master's Thesis in
Information and Communication Technology

Agder University College
Faculty of Engineering and Science

Grimstad

May 2005

I Abstract

The common belief of that mobile network makes security and privacy more difficult to establish is not always correct. Also the fact that several types of wireless technology make nodes vulnerable to monitoring and tracking is a common belief, and is often true. We propose a solution where security and privacy might be established between nodes when they are within short visible range of each other in order to exchange critical initial cryptographic credentials. The proposed solution also make sure that every digital track left behind will be useless for monitoring and tracking by rapidly change a nodes identification. We show a solution at a very generic level, and explain its functionality to fully self organized ad-hoc networks. We generalize even more by putting the core solution into several realistic scenarios and show various examples of how security and privacy aspects might be solved based on this solution. We provide a detailed investigation of the influence of such framework.

II Preface

This thesis is part of the Master Degree in Information and Communication Technology at Agder University College, Faculty of Engineering and Science in Grimstad, Norway.

Professor Frank Reichert, which e.g. is an expert at various communication techniques, and is the contact person and the link between Ericsson and HiA for the project ONE, initiated this thesis together with Professor Vladimir Oleshchuk. Oleshchuk e.g. is a mathematician and an expert at computer security.

Our supervisors Frank Reichert and Vladimir Oleshchuk have been a great resource to us. They have provided us with valuable feedback from commencement to the end of all project phases.

We would also like to thank the following persons for their efforts in providing us with information and views that has helped us in our research: Professor Per Egil Pedersen, Associate Professor Folke Haugland, PhD Bjørn Olav Hogstad.

Audun Pettersen Frode Åsen

III Table of contents

IV List of figures

V List of tables

VI Abbreviations

Ad-hoc	-	Latin phrase which means "for this purpose”
CPU	-	Central Processing Unit
LAN	-	Local Area Network
PAN	-	Personal Area Network
PDA	-	Personal Data Assistant
TTP	-	Trusted Third Part
MAC	-	Medium Access Control
NIC	-	Network Interface Card
ID	-	Identification
WWAN	-	Wireless Wide Area Network
WLAN	-	Wireless Local Area Network
WPAN	-	Wireless Personal Area Network
CDPD	-	Cellular Digital Packet Data
GSM	-	Global System for Mobile communication
HiA	-	Agder University College
WUSB	-	Wireless Universal Serial Bus
MIC	-	Message Integrity Code
PKI	-	Public Key Infrastructure
SSCh	-	Secure Side Channel
IrDA	-	Infrared Data Association
OSI	-	Open System Interconnection
UMTS	-	Universal Mobile Telecommunication System
CA	-	Certificate Authenticator
PRI	-	Pseudo Random generated Identification
R&D	-	Research and Development
LLC	-	Logical Link Control

VII Thesis Definition

Security and Privacy for Wireless Ad-hoc Networks

Ad-hoc networks handle links between our personal devices (laptop, phone, headset), and communications with our ever changing surroundings (new people we meet, new rooms we enter, new services we use).
A key challenge is to control the information that our devices directly and indirectly share, and how to establish trust and communication with new parties that we meet.
E.g., most devices have a 48 bit physical address or MAC address that is unique in the world and partly describing the manufacturer of the device. Thus one could easily track a person's movements without him/her being aware of it.
Two devices that get in contact for the first time have to establish communications following the privacy needs and rules established by their owners. The project shall investigate what information can be revealed at what point of time, and what security methods and strategies do apply.
The thesis shall describe a number of scenarios and solution approaches. The proposed solutions shall be evaluated against privacy and security requirements, and if time permits, against performance aspects.

(Frank Reichert, Vladimir Oleshchuk, Audun Pettersen, Frode Åsen)

1 Introduction

Wireless ad-hoc network were originally designed for the military, emergency and relief situations, because it does not need any fixed infrastructure and can be established almost anywhere needed [2]. Each node can act like a router, and the network is operative while it moves. It is therefore possible to exchange data between two nodes even if they aren't in each others range, as long there is nodes between them covering the missing range.
An ad-hoc network is very dynamic, and will be able to change over time as the nodes are moving around, joining or leaving the network.
Support for wireless ad-hoc networking is today integrated in most of our personal devices, like our mobile phone, Laptops, Personal Data Assistants (PDA's), etc. Smaller and simpler devices also use wireless ad-hoc networking, like wireless headset, hands free etc. Use of wireless ad-hoc communication is growing very fast, but important, related technologies seem not be just as much in focus as the wireless technology itself.
As popularity and use grows, the threats are increasing. Personal devices become more common and it is desirable that we can choose to remain anonymous to avoid leaving digital tracks, make use of secure communications when needed, control the data exchanged and establish trust.

In this thesis, we have taken a closer look at the current security and privacy problems which still occurs in state-of-the-art research, with especially focus on trust and anonymity.

HiA is doing a study relating to a project called "ONE", behalf of Ericsson of Norway, Sweden and Germany. One goal of this project is to evaluate security and privacy solutions(technologies) for several scenarios, and we hope that our results will contribute in further research in a such an important field that concern most of us.

1.1 Problems

Wireless ad-hoc networks introduce many technological possibilities, which are increasingly implemented in our personal devices such as digital personal assistants (PDA), cellular phones, and so on. Consequently this will be an area of growth in future, and central elements provided will be a great target area for Information and Communication Technology. Security and privacy is therefore an important part of the whole view, because we want this to be a communication method that we can trust in the future.

By providing improvements for both security and privacy solutions users will get better protection. It should become much more difficult to let malicious devices abuse wireless ad-hoc communication. Further, without a secure connection or communication, it will be difficult to make use of sensitive applications which probably will constitute bigger part of the future area of applications. Security and privacy will play an important role in the future, especial for the next generation of communication devices.

Figure 1: Security Issues affects each other.

Wireless ad-hoc networking includes many security and privacy problems that should to be solved or improved. Whenever a device wireless communicate ad-hoc with other devices it is easy for anyone to listen. In order to communicate secure is should be very hard if not impossible for unwanted participants to listen or interpret data exchange. In ad-hoc communication is there no infrastructure that could support security solutions and this makes secure connection even harder. In order to evaluate security and privacy you have to divide these topics into smaller part: security, privacy, anonymity and trust.

Many of the partial problems are directly or indirectly related which mean that each security issue could affect each other. In other word every partial security issue must be solved in such way that it will fit for the other parts. Security is like a puzzle, where many bricks have to fit each other in every way to accomplish the perfect result as shown in Figure 1. There are no easy ways to make these “bricks” fit to each other. This is often a challenge for making the correct balance between the various issues, or sometimes if possible, finding

smart ways to workaround the problem. In order to trust another entity, you have to know something about the communication partner and this is making the basis for establishing trust. Trust should be two ways, and the other entity also wants to know something about you in order to decide if it should trust you or not. This means that you have to exchange some information with each other in order to consider a trust relationship. At the other hand, you don't want to give away personal information in order to remain anonymous.

Sharing information due to user's direct decision under controlled circumstances as described, is categorized as direct shared information. When operating within a network, devices are usually broadcasting identification which is unique for each device, and often done without owner's knowledge. This is also normally beyond the owner's control and implemented into the network protocol. Such leak of information might be necessary for the network technology to work properly, but might also harm anonymity. Sharing information with lack of control, and without owner being aware of it, as described, is categorized as indirect shared information. Indirect shared information might harm ones privacy and anonymity.

Sometimes it might be necessary to do secure or encrypted communication with other entities. This is typically done when exchanging sensitive information e.g. and it might be important to maintain privacy during a secure communication with a person or device one trust, and still have the possibility to remain anonymous. These problems are tight related, and we will concretize issues to give a better understanding of the problems and how they are related.

1.2 Simple scenario to concretizes the problems

To make a better understanding of the problems one has to face practical behaviours of various devices in wireless ad-hoc networks. We will use a simple scenario as basis for our problem statement.

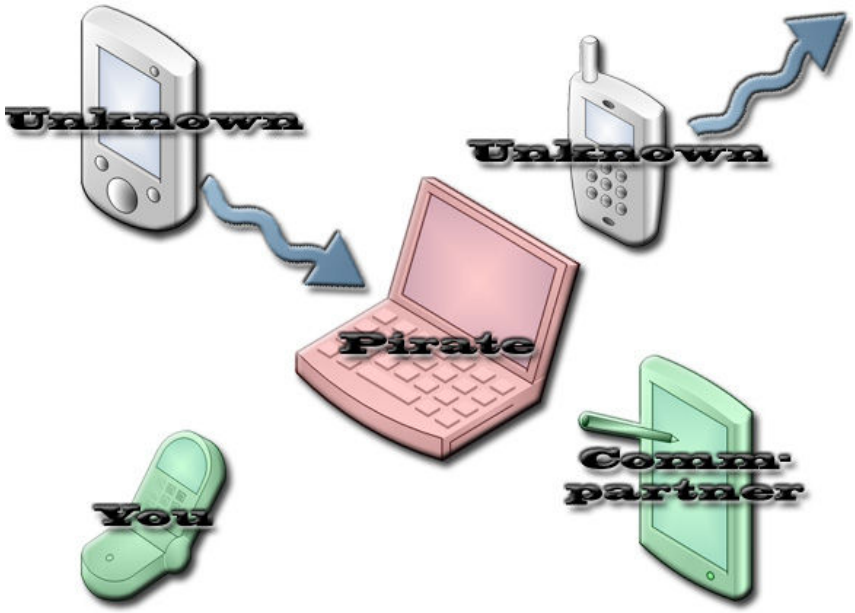

Figure 2: A typical, simple scenario

Figure 2: A typical, simple scenario illustrates five units which are forming an ad-hoc network. One of the devices is moving into the covered range, while another is moving out, these node are indicated with grey colour (label unknown). A third part is a malicious node, indicated with red colour (label pirate). Two nodes which want to do a private and confidential data exchange with each other are indicated with green colour (label you, communication partner).

1.2.1 Trust your communication partner

When operating in wireless ad-hoc networks, among several known and unknown nodes, one has no guarantee for connecting the actual correct device. Malicious devices might clone another's identity, or simply impersonate someone else in order to try obtaining secret information from other nodes. There could also be a problem to separate the actual target node from the rest, when one wants to initiate connection. As long as one can't be sure who the communication partner is supposed to be, the whole basis of establishing

trust is weak. One has to identify who initialize communication, and further trust this entity in order to exchange confidential information with the correct device/person.

1.2.2 Keep sensitive information confidential

To do a confidential conversation between two devices, it isn't enough just to identify the correct device. Since all data are transmitted on the air, everybody is able to listen and further record this information exchange. It is therefore preferred to make data incomprehensible for unwanted parties, which is normally done by using cryptography. Cryptography is the process making data incomprehensible for unintended parties. Cryptography makes use of keys, both to encrypt and to decrypt messages. All trusted and wanted communication partners involved into confidential conversation have to know which cryptographic key or keys used, which means they have to be exchanged during the initial faze of connection. One have to somehow ensure that no others than communication partner is getting the key, and vice versa, get the key from the other part, and know for sure that he or she gave away the correct key. One also has to ensure that no one has changed or corrupted the data during the exchange called active attack such as e.g. "man in the middle".

It is important, in some way, to make sure that no one else than oneself and the communication partner know the cryptography key values. It is further important that exchange between communications partners is done without corruptions, even if there should be some kind of malicious nodes within range. This should make basis for confidential conversation between two or more devices. This particular concept is illustrated by two green nodes, called "you" and "commpartner", in Figure 2: A typical, simple scenario.

1.2.3 Remain anonymous

Most of today's network technologies require some kind of identity for each device which are connected or within range of a network. Unfortunately, such identification is often unique, and might result in digital tracks which are left behind. Other identification credentials such as name or other personal information could also contribute to harm ones privacy. It is preferred, in some way, to let the medium be able to find it way to the correct device, both secured and non-secured, without revealing information which could harm

privacy. This information could be used to track ones movements, locate actual location etc. which is out of control of the actual owner.

1.2.4 Control the information flow

Giving away any personal information might result in harming privacy. One should carefully consider what information to give away and to whom. But there is also information which is given away beyond the owners control, and often without he or she is aware of it. An example for this is the MAC-address which is unique network identifier. It does not directly tell anything about a person, but it is broadcast for each network the device operate in, and one could easily track movements for a certain device. Of course, sooner or later one has to identify oneself, at some level, in one way or another to communicate with another person. An example, in Figure 2, shows that as soon as the incoming grey devices (label unknown) are within range of the network, one digital track is already left behind. The incoming unknown node probably wants to establish trust with someone in the network. One has to consider what kind of information should be revealed at what point of time. One don't want to reveal more than what's necessary. Somehow, one have to gain control of the information given away in order to avoid lack of existing privacy.

1.3 Problem derivations

1.3.1 Security

Definition: In wireless ad-hoc networks, we often talk about the external security, and the main aspect of such security is to secure the data which is transmitted over open networks. The information is secured by several functions: [2], [3], [33]

- *Authentication* – You have to ensure communicating with the right device (person) in order to avoid expose information for any unwanted node (device).
- *Integrity* – You have to ensure that sent information would not be manipulated to avoid false information for you and your communication-partner.
- *Confidentiality* - You have to be sure that no intruders are able to read your information to keep it secret.

Problem: Some of the security problems may be solved by various encryption methods, but cryptography is often claimed to steal both resources, such as energy (battery) and processor usage, in addition to total bandwidth [4]. One therefore has to decide where and when it is necessary with secure data exchange, and with whom. If one decides to establish secure communication with another node (person), there is a quest for how the initial process should be done, since most data sent on the air is vulnerable. Selected methods will often be a balance between use of available resources and security level, and should be selected with care. This is often directly related with information which is shared with others.

1.3.2 Privacy

Definition: "*Privacy is the ability of an individual or group to stop information about them from becoming known to people other than those whom they choose to give the information. Privacy is sometimes related to anonymity although it is often most highly valued by people who are publicly known".* [5]

Problem: Personal devices gets more complex as well as we use various protocols for exchanging information, this resulting that we are loosing control for what data we actually exchange with other devices (persons). Much of the data exchanged might be sensitive, and a malicious device (person) might be able to abuse this kind of information. One should consider what type of information should be allowed to exchange, and with whom. There may also be various points of time which one should exchange such information or not, according to the current state of the communication process. How the data should be exchanged must carefully being considered as well. This is often related with the (lack of) control of indirect shared information between various nodes within a network.

1.3.3 Trust

Definition: Trust in computer science is not that different from what it really means in the real word for us, human beings.

"Trust in sociology and psychology refers to an open, positive relationship between people, or between people and social institutions such as a corporation or government. More specifically, trust is the belief by one person that another's motivations towards them are benevolent and honest". [6]

Problem: Wireless ad-hoc networks consists of a various number of nodes (devices) and they could be formed anywhere with anyone within range. Within a pure ad-hoc with no fixed infrastructure and no global Trusted Third Part (TTP), you might get in trouble while connecting the person you are gong to communicate with. You might connect to the device you think belong to him or her, but the problem is to be 100% sure you are communicating with the correct device (person). With other words, it might be hard to trust the device you actually try to initiate connection with, and as long as you don't trust the other part, you might not want to exchange sensitive information. This is a problem related to direct sharing of information, though, the problem might not be control, but rather what one allows to share, and of what point of time.

1.3.4 Anonymity

Definition: Again, we refer to a well written definition for this subject:

"Anonymity is derived from the Greek word "ανωνυμία", meaning without a name or name-less. In colloquial use, the term typically refers to a person, and often means that the personal identity or personally identifiable information of that person is not known. More strictly, and in reference to an arbitrary element (e.g. a human, an object, a computer), within a well-defined set (called the "anonymity set"), "anonymity" of that element refers to the property of that element of not being identifiable within this set. If it is not identifiable, then the element is said to be "anonymous". [7]

Problem: Wireless Ad-hoc devices allow us to move around while the network is operative (moving) possibility gives us some unwanted disadvantages. Many networks make use of Medium Access Control Address technology (MAC-Address) which is a 48 bits physical address for the device's Network Interface Card (NIC). Among others,

802.11 and Bluetooth state an example for wireless technologies which use MAC-Addresses [8], and simultaneous is qualified for use in ad-hoc network. While moving around with your personal device receiving information from info-beacons and other such nodes, your MAC-Address will be exchanged over the network, and one can easily track devices movements. This may harm ones anonymity, since each MAC-address is worldwide unique. Most users want to use network services, but they don't want to leave any digital tracks behind. Changing such unique value will affect the whole network structure since MAC-address is part of layer two in the Open System Interconnection (OSI) model. This might also do it harder to establish trust between devices, since it could be difficult to recognize nodes without any distinctive mark to look for. This might be a quest for balance as shown in Figure 3. This problem is related to both direct and indirect share of information between nodes within an actual network.

Figure 3: It is often a quest for balance when it comes to Trust and Anonymity.

1.4 Limitations

- Because of both available time for project and our area of research, there will be several aspects we not are going to deal with.

- We will not consider any routing or multi-hop routing security issues for this project, such as AODV, DSR, OLSR and other protocols. All use of these protocols will be considered as transparent to us.

- Our research will be limited to a reduced number of various scenarios, though the chosen scenarios would be the most common use of wireless ad-hoc networking. Definition and problem derivation are described in Appendix A.

- The project includes development of a high level model witch should be able to simulate the improved system. Due to the project time, level of abstractness will be high, and existing low level components will be reused in alternative ways to save time.

- Our research is limited to mainly use of IrDA as SSCh technology.

1.5 Purpose

The purpose of this project is to survey the possibilities of security improvements in pure wireless ad-hoc networking technology with especially focus on some of the user's privacy and security-needs, which they usually are not aware.
For wireless environments, one has to ensure that a connection is established to the correct device, and that the correct device actually belongs to the correct person. When exchanging personal and sensitive information, it is very important to establish trust between the communicating parties, which should be done by help of a secure communication channel as well. When people use wireless device usually don't know that they leave digital tracks behind. Digital tracks are often unique static values for a unit; (device) and one could easily track down person's movements with such information. Being able to control the information flow, the privacy should remain, and anonymity kept in a better way.

This project includes an abstract high level model which is able to simulate and illustrate some of our ideas and proposed solutions. This model is also used for some of the measurements presented in the evaluation part helping documenting the benefits and drawbacks it might have. The vision is to create alternative methods to improve end-users security, privacy, trust and anonymity that could be able to ensure a safer everyday use of our personal devices.

1.6 Motivation

During the thesis, we will expect to gain insights into security and privacy threats and opportunities for wireless ad-hoc technology. We consider this subject as an important factor in further research for this arena, and these themes will be an important part of upcoming technology. The new knowledge we gain will be much appreciated and valued.

2 Literature study

2.1 Introduction

In this chapter we will evaluate different technologies and projects which are related to particular problems in this thesis. We will also explained and derive different challenge which communication faces today. We have performed a massive literature search to carry out which technologies and proposed solutions in order to develop our solution.

In the past decade computer and device communication has had a rapid growth. Nowadays communication moving more and more towards wireless communication instead of wired communication. Wireless technologies have become increasingly popular in our everyday business and personal lives. This type of communications offer users many benefits such as portability and flexibility, increased productivity, and lower installation costs. Wireless local area network (WLAN) devices, for instance, allow users to move their laptops within their offices without the need for wires and without losing network connectivity. Less wiring means greater flexibility, increased efficiency, reduced wiring costs and new possibilities. But wireless communication also arise a number of concern since the media is open for everyone to listen [2], [9].

2.2 Wireless Networking

Wireless networks are many and diverse but are frequently categorized into three main groups based on their coverage range [2], [9], [10]:

- WWAN (Wireless Wide Area Networks)
- WLAN (Wireless Local Area Network)
- WPAN (Wireless Personal Area Networks)

Even though we categorize wireless network into different group they still have similar properties. All wireless links face the same problems, but most of longer range solutions like WWAN have inbounds security solution that will prevent or reduce number of threats. It is important to take notice of those solutions that involved public infrastructure, such as Universal Mobile Telecommunications System (UMTS), faces threats better than solution without public infrastructure such as WLAN in ad-hoc mode.

2.2.1 WWAN

WWAN cover a “wider” area and usually gives the user access to data wherever they go. WWAN includes wide coverage area technologies such as 2G cellular, Cellular Digital Packet Data (CDPD), GPRS, CDMA2000 and GSM. These wide coverage technologies offer regionally, nationwide or typically globally coverage. WWAN often include security solutions which include public infrastructure. Typical operation modus is master/slave where service providers with infrastructure control everything. It is rather rare to use this solution in a self organized ad-hoc network and would therefore not be of importance in this thesis. Figure 4 shows a typical WWAN scenario [2], [9], [11].

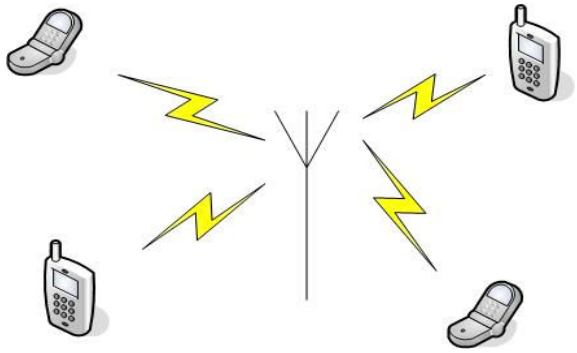

Figure 4: WWAN

2.2.2 WLAN

WLAN include wireless local area networks, such as 802.11, HomeRF and HiperLAN. These technologies offer a regional or typically local coverage. Even though it is several different technologies on the marked, only 802.11 are being widely used in personal devices. Typical operation modes are ah-hoc mode or Access Point/client mode often without public infrastructure. WLAN is the most common wireless network type used in ad-hoc solutions. Figure 5 and Figure 6 shows typical WLAN scenarios. It is important to emphasize that WLAN in ad-hoc mode between advanced devices with equally capabilities are our main focus in this thesis [2], [8], [9], [12].

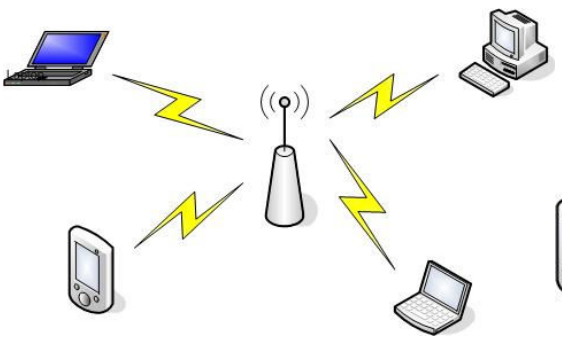

Figure 5: WLAN, AP Mode

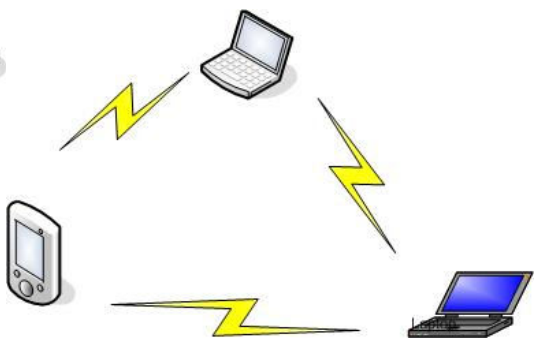

Figure 6: WLAN, ad-hoc mode (main focus)

2.2.3 WPAN

WPAN represents wireless personal area network with technologies such as WUSB, Bluetooth and IrDA. These technologies offer typically up to a few meters coverage and are often mean to replace the need for locally connected cables, such as printer cable e.g. Even though these wireless networks type are rather rare, it is expected to experience a rapid grow in near future.

WPAN's typical operation mode is master/slave and without public static infrastructure. These types of connection does not often control which devices that are involved and several solution does not have any security solution at all. Another problem WPAN often faces is the devices lack of control on direct (indirect) shared information. Many of these solutions would in addition be static since they are expected to replace the need for locally connected wire. This represents an even greater risk for users and the need for better solutions. But it is important to emphasize that all wanted involved devices are typically under control of the same owner and therefore very much increase security possibility. This thesis wouldn't focus on WPAN, but WPAN would be referred in connection with some wireless technologies. Figure 7 shows a typical WPAN scenario [2], [8], [9].

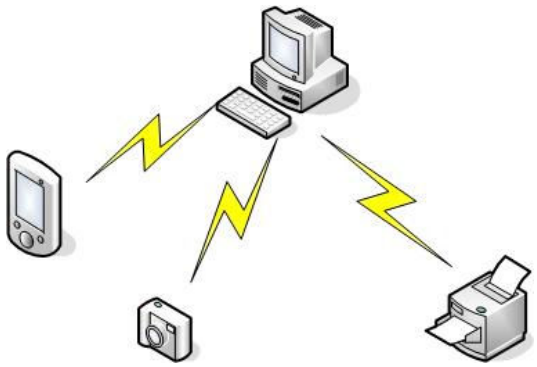

Figure 7: WPAN

2.3 Wireless Ad-hoc Technologies

Ad-hoc that means "for this purpose" is a typical wireless connection with no base station or infrastructure involved. On one side we have e.g. WLAN, in AP mode, which use a fixed network infrastructure and a central master who control everything and have inbound security solutions. Ad-hoc networks on the other side maintain random network configurations, typically relying on a master-slave system connected by wireless links to enable different devices to communicate. Typically, devices discover other nodes automatically within communication range and then form a network. Figure 8 illustrate an example of an ad-hoc network [14].

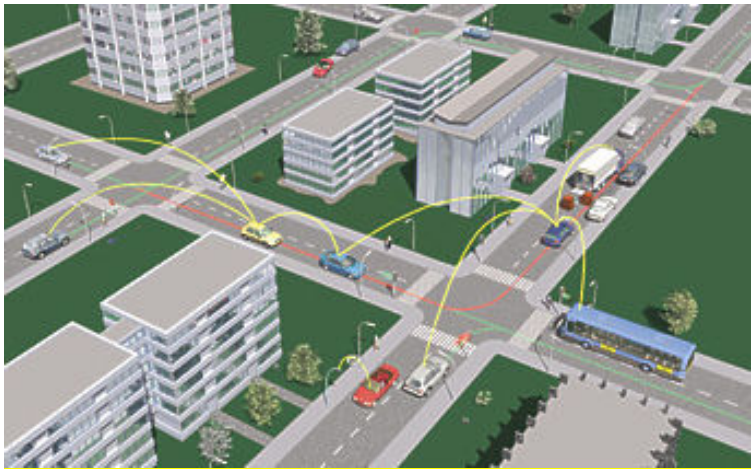

Figure 8: Ad-hoc network (source: http://www.ibr.cs.tu-bs.de)

Wireless ad-hoc networks are designed to dynamically connect remote devices such as mobile phones, computers, and PDA's. These networks are termed "ad-hoc" because of their shifting network topologies [14].

One of the biggest advantages with wireless ad-hoc network is dynamically connection and forming self organized network. But this also represents a problem, because it could be very hard to know exactly who is connected and that are this persons intentions. It is at least very hard or impossible to limit the number of devices and anyone within communication range could be monitoring ongoing transmission.

Another challenge is secure transmissions, because this would in most cases require exchange of cryptographic keys before or in the initial face of a secure communication. This represents an even bigger challenge in ad-hoc network that often are formed without

internet access and therefore without any possibility to make use of any online 3.part verifier like e.g. certificate authentication server, verification server.

We have several ad-hoc technologies that differ in range of use and properties:

2.3.1 Bluetooth

The Bluetooth standard is a computing and telecommunications industry specification that describes how mobile phones, computers, PDA's, printers and digital cameras should interconnect with each other. Bluetooth make use of a low-cost, globally available short-range radio wave. The Bluetooth standard specifies wireless operation in the 2.45 GHz radio band and supports data rates up to 2.1 Mbps. It further supports up to three simultaneous voice channels and employs frequency-hopping schemes and power reduction to reduce interference with other devices operating in the same frequency band. Even if Bluetooth standard is well known does the latest development within communication device tends to not involve Bluetooth support [2], [16].

2.3.2 IEEE 802.11

WLANs are based on the IEEE 802.11 standard, which the IEEE first developed in 1997. The IEEE designed 802.11 to support medium-range, higher data rate applications, such as Ethernet networks, and to address mobile and portable stations.

802.11 is the original WLAN standard, designed for 1 Mbps to 2 Mbps wireless transmissions. In 1999 802.11b became a standard, which operates in the 2.4 - 2.48 GHz band and supports 11 Mbps. The 802.11b standard is currently the dominant standard for WLAN providing sufficient speeds for most of today's applications. Because the 802.11b standard has been so widely adopted, the security weaknesses in the standard have been exposed. Another new standard, 802.11g operates in the 2.4 GHz waveband and support 802.11b standard and support 54 Mbit/s. Where is also another standard 802.11a that operate in the 5.0 GHz waveband and support 54 Mbit/s. This standard is most widespread in the countries that have limited use of the 2.4 GHz waveband, like US [2], [17], [18].

The latest development in communication devices, such as mobile phone, PDA etc, shows that IEEE 802.11 technology support is becoming increasing popular and normal. This technology seems to be the best choice within wireless ad-hoc communication and we expect that it will be even more widely used in the future [2], [17], [18].

2.3.3 IrDA

IrDA stand for Infrared Data Association and is an industry-based group with over 150 companies that have developed communication standards that make use of infrared light as communication media. IrDA are especially suited for low cost, short range, cross-platform, point-to-point communications at a wide range of speeds. The range is typically from nearly zero up to one meter and speed from 16 kbps up to 16 Mbps. IrDA does only support point-to-point communication that means one-to-one communication between 2 devices. Most of today's mobile phones, laptops, PDA etc do have implemented IRDA support [19], [53].

IrDA solutions today are not recommended to be used in transfer of large amount of data because most implemented solutions have limited speed capabilities. But by using infrared light as a point-to-point communication media it doesn't faces wiretap threats such as other similar wireless technologies. This ability makes IrDA a perfect choice as a secure channel that could be used to exchange security credentials that often consist of a limited amount of data [19], [53].

2.3.4 RFID

RFID (Radio Frequency Identification) is an automatic identification method that makes use radio waves to automatically identify individual items. This expression is very general and doesn't say much about the technology used to identify an item. In fact RFID is a loosely bounden technology with several standards and different properties. Table 1 below shows typically parameters and operational frequencies [55], [56].

Frequency Band	Frequency Range	Range
Low Frequency	~125 KHz	< 0.3m
High Frequency	13.56 MHz	~0.9m
Ultra High Frequency	850-900 MHz	3m-6m
Microwave	2.45 GHz	-

Table 1: RFID overview [Source: www.rfidjournal.com]

Even if RFID have several areas of use and capabilities it is often used as an alternative to identify methods such as bar code attach to products (often expensive) and implanted into pets such as cats or dogs. It is not widely used in products that transfer a larger amount of data. It is also not common supported in communication devices and are not expected to be so in the future it's design are more suitable to open exchange of a small amount of data [55], [56].

2.3.5 ZigBee

ZigBee is a specification of high level communication protocols based on the IEEE 802.15.4 standard. This standard designed to use small, low-power digital radios in a WPAN. ZigBee are optimized to exist in applications that require low data rates and low power consumption. The software is designed for easy coding for small, cheap microprocessors. The radio design utilized by ZigBee has been carefully optimized for low cost at scaled production. ZigBee's main usage area today are inexpensive self-organizing mesh network that can be shared by industrial controls, embedded sensors, medical devices, alarms and home automation [19].

It makes use of three different frequency bands and transmission range is between 10 to 75 meters. These bands have different areas of operation and properties as shown in the Table 2 [19].

Frequency	Channels	Transmission Rate	Area of use
2.4 GHz	16 Channels	250 kbps	Worldwide
868.3 MHz	1 Channel	20 kbps	Europe
902-928 MHz	10 Channels	40 kbps	America

Table 2: ZigBee overview. [*Source: http://en.wikipedia.org/wiki/ZigBee]*

Since Zigbee is design to transfer small amount of data in addition to not be supported into communication devices it is expected that this technology will not become supported into mobile phones, laptop, PDA or similar devices in the future either.

2.3.6 WUSB

Wireless Universal Serial Buss (WUSB) is a new extension of USB that combined security, speed and easy-to-use technology. WUSB is based on ultra wideband wireless technology which operates in the range of 3.1–10.6 GHz. WUSB offers bandwidths of 110 Mbit/s at three meters and 480 Mbit/s at ten meters. WUSB operates in master/slave mode and uses a star topology with up to 127 devices. This new WPAN technology has many different usages area as shown in the Figure 9 below [20], [54].

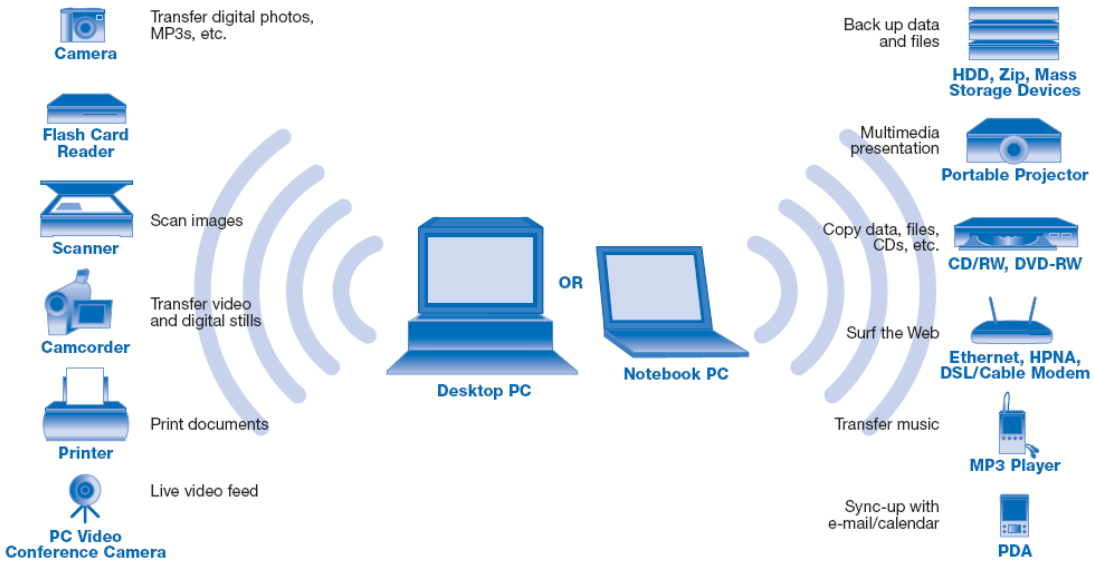

Figure 9: Connection via WUSB

WUSB is an upcoming technology and could become a major supported technology into communication devices. But this is still too soon to predict if WUSB will succeed, but it does have great potentials. It could be a major ad-hoc technology and are expected to become the new marked leader in WPAN within few years.

2.4 Today's use of Ad-hoc

Ad-hoc is mainly used for industrial purposes today, but it's expected to slowly twist towards personal use. Military tactical operations are still the main application of ad-hoc networks today. For example, military units (e.g., soldiers, tanks, or planes), equipped with wireless communication devices, can form an ad hoc network when they roam in a battlefield.
Ad-hoc networks can also be used for emergency, law enforcement, and rescue missions. Since an ad hoc network can be deployed rapidly with relatively low cost, it becomes an attractive option for commercial uses such as sensor networks or virtual classrooms [21].

Another major area that ad-hoc could and are being used are in exchange of information between different or same type of devices. Typical ad-hoc compatible devices today are computers, PDA's, mobile phones and hands free. Several upcoming ad-hoc devices are digital cameras, printers and mp3 players.

Typical information exchange could either be chatting or text messages between devices within range. PDA's and mobile phones are devices that could use ad-hoc technology for this purpose. Several users, within range, could communicate without infrastructure for free.

Another communication purpose is the exchange of multimedia content primarily used for enjoyment. The latest developments within electrical devices have developed a possibility for a new type of applications. Application media examples are pictures, video, animations, music, games, and programs or perhaps more common content that mixes several of these media types. These applications could consist of several megabyte, perhaps purchased illegally and therefore it is preferred that they are exchange without billing and use of public infrastructure. This type of information exchange would typically be between PDA's and/or mobile phones.

Wireless ad-hoc communications are also being used for common data transfer between devices. The main purpose is to replace the need for wires and to communicate more freely.
This information exchange are would range over several area. It could be communication between computers and printers or mp3 players where security risk level usually is consider being low. On the other side could it be business or graded communication between mobile

phones, PDA's and digital cameras where information typically are more sensitive and therefore higher security level. Generally speaking business areas are often in more need of higher security level than home environment.

2.5 Privacy and Security

Today users dependence on producers manufactured solutions that have inbound security and privacy solutions. But unfortunately security and privacy is hard to define and is dependent of several factor such as anonymity and trust. These factors are often not highly valued by the manufacture as well.

Wireless ad-hoc communication devices are dependent of parameters such as security, privacy, trust and anonymity. It is very hard to define these factors independent and in several ways they inflict on each other and in most situations would it have to become balance between these factors. The ultimate or preferred goal is to develop a user-friendly communication solution that are able to communicate in a secure way that give away few if any privacy information to unwanted participants.

2.5.1 Privacy Issues

Privacy has always been a contentious issue for ubiquitous computing and networking. Personal privacy means be able to control information which directly or indirectly could be used to identify an entity –such as email address, shopping history, MAC address or location–to organizations and to others. Privacy relates to control over their personal information [22], [23], [24].

Privacy is an important issue that is becoming increasingly important as we push into ubiquitous computing environments. In fact many services will experience a major disadvantage if the user knows that this service could give away personal data. Advances in location-enhanced technology are even making it easier to be located by others. These new technologies present a difficult privacy trade-off, as disclosing of current location. This feature makes it even more important to maintain user's privacy [22], [23], [24].

We are today making widely use of wireless system such as WLAN/WPAN, but these systems was not design to maintain privacy. Most of today's wireless devices use a static

unique id when communicating. Both Bluetooth and IEEE 802.11, who are the most popular ad-hoc technologies, use a static MAC to unique identify all involved participants. This result in that ad-hoc communication becomes a privacy risk without directly sharing any information. It is difficult to maintain privacy and anonymity in today's wireless systems, if not impossible. Anonymity is a desirable property for users in many communication systems and will strengthened privacy. In fact anonymity could be the only way to maintain privacy in ad-hoc communication. In today ad-hoc communication an attacker will be able to track and identify the communication devices based on static address [22], [23], [24].

2.5.2 Security Issues

Ad-hoc wireless network does not have any predefined infrastructure and all network services are configured and created on the fly. Thus it is obvious that with lack of infrastructural support and susceptible wireless link attacks, security in ad hoc network becomes inherent weakness [25]. Security is an important issue for ad hoc networks, especially for those security-sensitive applications. To secure an ad-hoc network, we consider the following attributes: availability, confidentiality, integrity, authentication, and non-repudiation. This attributes form a "security chain" that together will form the security level. Any weakness in some of this attributes will infect the security level [21].

Figure 10: Security chain in ad-hoc network

Integrity attribute ensure that data being identically maintained during any operation, such as transfer, storage, and retrieval. A message could be corrupted because of benign failures, such as radio propagation impairment, or because of malicious attacks on the network. Integrity guarantees that a message being transferred is never corrupted. A message could be corrupted because of benign failures, such as radio propagation

impairment, or because of malicious attacks on the network. Integrity level is usually ensured by use of mathematical code such as Message Integrity Code (MIC) [21], [26].

Availability ensures the survivability of network services despite denial of service attacks. A denial of service attack could be launched at any layer of an ad-hoc network. On the physical and Media Access Control (MAC) layer, an adversary could employ jamming to interfere with communication on physical channels. On the network layer, an adversary could disrupt the routing protocol and disconnect the network. On the higher layers, an adversary could bring down high-level services. One such target is the key management service, an essential service for any security framework [21].

Authentication enables a node to ensure the identity of the peer node it is communicating with. Without authentication, an adversary could masquerade a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operation of other nodes [21].

Confidentiality ensures that certain information is never disclosed to unauthorized entities. Network transmission of sensitive information, such as strategic or tactical military information, requires confidentiality. Leakage of such information to enemies could have devastating consequences. Routing information must also remain confidential in certain cases, because the information might be valuable for enemies to identify and to locate their targets in a battlefield [21].

Non-repudiation ensures that the origin of a message cannot deny having sent the message. Non-repudiation is useful for detection and isolation of compromised nodes. When a node A receives an erroneous message from another node B, non-repudiation allows node A to accuse node B of using this message and to convince other nodes that node B is compromised [21].

2.5.3 Trust

Trust is an important aspect in the analysis of secure systems and if it's misplaced it could compromise the entire system. A critical part of any system is the developing process how and with whom to form trust relationship. Trust establishment in ad-hoc wireless networks is still an open and partly challenging field. Many ad-hoc networks are based on naive neighbour trust relationships. These relationships often originate, develop and expire "on the fly" and have usually short life spans [27], [28], [29].

Trust could be a before-security issue in the ad-hoc networks. By verifying the relationship, it will be much easier to take proper security measures, and make correct decision on any security issues. A trust model specifies, evaluates and sets up trust relationship among entities. Trust modelling is a technical approach to represent trust for digital processing. Recently, trust modelling is paid more and more attention in electronic systems. Current trust academic work covers such aspects as analyzing the problems of current secure systems and quantifying or specifying trust in digital systems. By applying a self organized trust model in every device an ad-hoc network each node could easily maintain trust constraints itself. This could typically be implemented by adding incoming devices to different trust list (described in chapter 4.4) [29], [30], [31].

2.5.4 Anonymity

Anonymity is a result of not having to reveal personal characteristics such as a name, unique electrical identification or description of physical appearance disclosed. Anonymity is not an absolute condition, that is, the degree of anonymity one enjoys may vary with circumstantial, environment etc [32].

Unique identification in wireless ad-hoc communication such as MAC represents a big problem. By monitoring the wireless network any person could easy disclose and track any communication device based on the MAC address [32].

One of the best methods to achieve anonymity is that communication devices have pseudo random identification that changes periodically. This will prevent an attacker to monitoring people and their devices because "he" could not know which ID to look for.

2.5.5 Cryptography

Cryptography, comes from the two Greek words meaning *secret writing*, is a deep mathematical subject. Cryptography provides the basis for secure communication and is the art and science of concealing information [33]. In order to strengthen encryption security within a system one could increase cryptographic key length. This is usually something which is done in parallel with hardware evolution [33].

In general, we can categorize cryptography in symmetric and asymmetric. These two methods have their benefits and back draws.

Asymmetric cryptography
"Public key cryptography is a form of cryptography which generally allows users to communicate securely without having prior access to a shared secret key. This is done by using a pair of cryptographic keys, designated as public key and private key, which are related mathematically." [34]

- **Benefits [59]**
    - Hard to break
    - Key exchange
    - Support for infrastructure
    - Certificates

- **Drawbacks [59]**
    - Considerably slower encryption algorithms
    - Rarely used for bulk transfers
    - Not proven to be mathematically secure
    - Software encryption is approximately 100 times slower (DES vs. RSA)[59]

Symmetric cryptography
"The encryption key is trivially related to the decryption key, in that they may be identical or there is a simple transform to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link." [35]

- **Benefits [59]**
  - Simple encryption process
  - Use of known encryption algorithm
  - Security is dependant of the length of the key

- **Drawbacks [59]**
  - Shared key must be agreed upon both parties
  - n communication partners means n secret keys
  - Authentication of origin or receipt cannot be proven
  - Key management

2.5.6 Wireless Threats

Ad-hoc network present both challenges and opportunities for mobile users, but are still seems to be the most upcoming wireless topology today. Wireless links renders in an ad-hoc network are susceptible to link attacks ranging from passive eavesdropping to active impersonation, message replay, and message distortion. I addition to all weaknesses that common wired network faces. Network security could be divided into 2 main groups' passive and active attacks [36].

A passive attack is an unauthorized user/attacker monitors or listens in on the communication between two or more parties. Another known term on this action is eavesdropping as shown in Figure 11. Eavesdropping might give an adversary access to secret information, violating confidentiality.

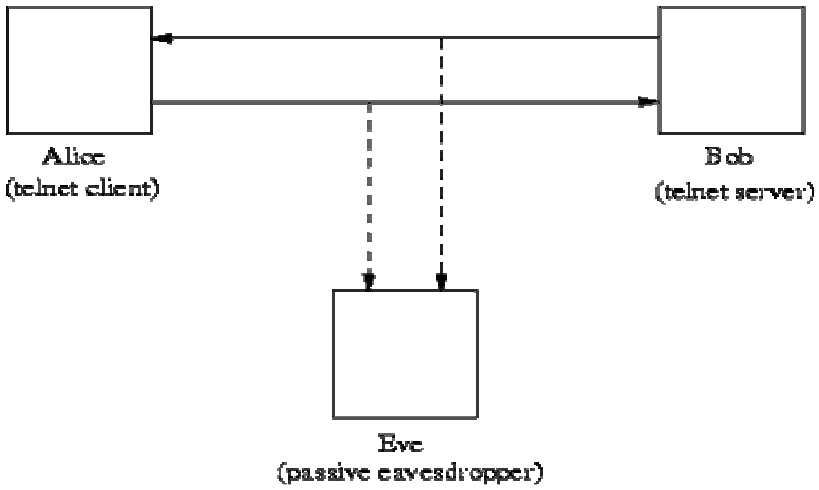

Figure 11: Passive attacker

A passive attack on a wireless network may not be malicious in nature because it is not illegal to listening. Besides wireless communication takes place on unlicensed public frequencies. This mean that everyone one can use and listening to these frequencies. This makes protecting a wireless network from passive attacks difficult. In fact passive attacks are by their very nature difficult to detect and are usually not detected.

Once an attacker has gained sufficient information from the passive attack, the hacker can then process and analyse the collected data offline. Then the attacker has cracked the security credentials could he launch an active attack against the network. Active attacks might allow the adversary to delete messages, to inject erroneous messages, to modify messages, and to impersonate a node. Figure 12 shows an active attack scenario.

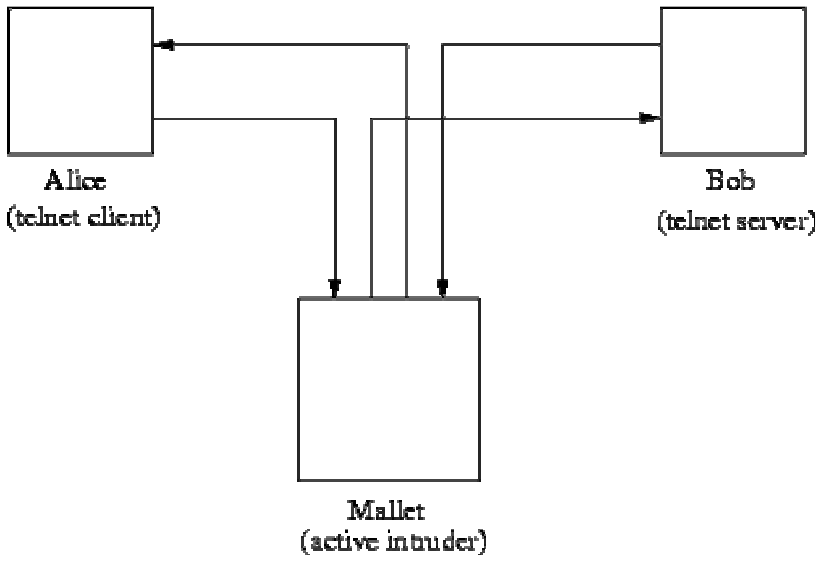

Figure 12: Active attacker

Active attacks are further divided into 4 subclasses:

DoS (Denial-of-Service) are when an attacker prevents or delay the normal use of a service. This could be loss of service to users, typically the loss of network connectivity and services by consuming the bandwidth or overloading the computational resources [37].

Masquerading is when an attacker try to access or collect recourses by impersonate a legitimate user typically an administrator or privileged user [38].

Message Modification is when an attacker alters a legitimate message by changing it. This could be all from deleting, adding to, replacing, or reordering the originally message.

Replay is when an attacker repeated or delays a valid data transmission. This type of attack is either carried out by the originator or by the hacker who intercepts the data and retransmits it [39].

2.6 Related work

An ad-hoc network is dynamic because of frequent changes in both its topology and its membership (i.e., nodes frequently join and leave the network). Trust relationship among nodes can change, for example, when certain nodes are detected as being compromised. Unlike other wireless mobile networks, such as mobile IP, nodes in an ad hoc network may dynamically become affiliated with administrative domains. Any security solution with a static configuration would therefore be insufficient. It is desirable for maintain good security that changes are adapted on-the-fly [15].

Traditional security mechanism such as authentication protocols, digital signature, and encryption play a big role in today's security within ad-hoc network. Even though, it has been proven that they are not sufficient enough by themselves. To achieve better security it is recommended that one apply the principle "distribution of trust". The principle states that no single node is trustworthy in an ad-hoc network because of low physical security and

availability [15]. It is important to remember/emphasize that trust play an important role in the cooperation and interaction between real world entities.

The "PERVASIVE TRUST MANAGEMENT (PTM) MODEL" allows entities to autonomous and dynamic exchange information in a cooperative way via Public Key Infrastructure (PKI) [40].

In the PTM model trust relationship are establish between entities. Each entity handles a protected list of trustworthy and untrustworthy entities, the trust value (degree) associated with them, behaviour's information, the public key and the public key's validity. Each entity manages its own security like PGP [41]. Trust relationships among Certificate Authenticators (CA) could be used (if they exist), but an entity would often rather create its own trust relationships [40].

One of the biggest advantages with PTM is that it minimizes the human intervention since most security management functions can be performed automatically and it can be executed on limited devices. PTM is common used as basis for authentication and authorization [40].

A big disadvantage is that users have to be identified before they could be implemented in this model. Every node will without any pre-knowledge in an ad-hoc network have same trust level. An attacker could do a lot of damage before he become untrusted. Further every user/device has to identify them for this model to work properly. An attacker could at any point simply steal a trusted entity for 2 main reasons; either to steal data or to sabotage a trusted entity [40], [33].

In this thesis we use some elements from the PTM model. We apply self organized trust settings for every node in order to maintain trust without involving other parties. Other nodes are automatic categorized into different trust list levels by their ID and connection methods etc. We also apply dynamic trust list by moving nodes between trust lists on behalf of behaviour.

Frank Stajano and Ross Anderson presents in "The Resurrecting Duckling Model" describes secure transient association between a device and multiple serialized owners. This model based upon a of master-slave principle. Typically will a number of potential slave be in a collected in a birth spot and ready to be random chosen. The child node (duckling)

considers the first node that sends it a secret key as master (mother duck). Then this "ignition key" is received the device will be faithful against its master [42].

This master-slave bond can only be broken by some straight, limited conditions. Master/slave relationship could either be broken by the master, an event or a timeout. Then one of these actions have been successfully applied the slave is free and ready for a new master. Resurrecting Duckling model is most suitable for security in large dumb sensor nodes network with no pre-configuration. A big disadvantage with this model is that it uses a hierarchical security chain. In ad-hoc network this feature not appropriate [42]. This model has not been used or partly used in our thesis because this would require hierarchical security architecture, which in some contest are not possible in various scenarios.

Kong, Zerfos, Luo, Lu and Zhang present in their proposal "Providing Robust and Ubiquitous Security Support for Mobile Ad-hoc Networks" a scalable intrusion-tolerant security solution. This proposal enables intrusion tolerance by applying threshold secret sharing and secret share updates. Secret sharing schemes protect secrets by distributing them over different participants (share holders) [43], [44], [45].

The design is based on certificate approach with a public key infrastructure (PKI). A certification authority (CA)'s functionality are distributing to each local neighbourhood. A coalition of K neighbours can serve as the CA. The CA's function is to jointly provide certification services for a requesting mobile entity [43], [45].

The proposal involves a novel self-initialization protocol to handle dynamic node membership and secret share updates. Each node could be initialized by any K neighbours. Then a node is initialized, it is qualified to be a member to serve its particular neighbourhood [43], [45].

But this solution require a centralized dealer that valid certificates and secret shares in the bootstrapping phase. The centralized management function is no longer needed after initializing K entities. This mean that nodes can't form an ad-hoc network without involved a trusted 3 part [43], [45].

Another possible threat is that attacker could perform a Sybil attack. This means that an attacker takes several identities to collect enough shares so he could reconstruct system secret/private key [46], [47]. Some of these ideas are further used in our solution that involved a local trusted 3.part. We do mainly apply ideas rather methods from this model Asokan and Ginzboorg present in their proposal "Key agreement in ad hoc networks [27]" a shared password-based security solution. They consider a scenario with a local, small group of nodes that wishes to establish a secure session without use public-key infrastructure or third-party services. The proposed solution states that all participants pre-share on a common secret password. This password would then be used in *password-authenticated key exchange* method witch derive a strong shared key starting from only an initial weak password [48].

The proposal introduced a new key agreement scenario in addition to examine various solutions to the shared key agreement problem. It also described previously known protocols for password authenticated multi-party Diffie Hellmann (D-H) key exchange. They also presented improvements *the cube protocol*, a D-H variant, to make it resilient to malicious and benign failures [48].

But it is few drawbacks for this solution. At first it is vital that initial password is being kept secret form others. This particular property could limit the number of scenarios to controlled environment like closed meeting or similar. It would represent a problem/security risk to keep a password secret for others in public use areas. It's highly desirable to have a solution that could work in all use areas [43].

Another drawback is that people would have to type shared password manually into their devices. This factor would automatically limit the number of character. In additional could this property lead to a static non-shifting password that's represent a security threat [43], [33].

We apply the same scenario as Asokan and Ginzboorg with a local small group of nodes wishes to establish trust without public-key infrastructure or third-party services. But our solution makes use of secure side channel to perform initial security credentials exchange. We are mainly using some non-technical ideas of this proposal even though this kind of initialization method could be used in our solution.

Srdjan Capkun, Jean-Pierre Hubaux, and Levente Buttyan present in their proposal "Mobility Helps Security in Ad Hoc Networks [45]" that mobility could in fact heighten security in ad-hoc network. They propose a technique in which exchanging appropriate cryptographic security credentials via a secure side channel (SSCh). An SSCh can only be secure point to point connection and works only when the nodes are within a "secure range" of each other [45].

This idea can be applied to virtually any mobile ad-hoc network at any layer and make nodes complete able to self-organize their security. There is no central authority and the exchange and agreement of security associations is based on mutual agreement between users [45].

The proposal assumes that the activation of the side channel is made by both users consciously and simultaneously. The trust in this system is based on "personal" trust made by the user. This simply means if a user personally trust the other part, then he will become a trusted part of the communication [45].

This proposal base security on public-key cryptography that mean secure side channel could become compromise with eavesdropping without losing complete totally compromise the system [43].

Asokan and Ginzboorg proposal is a strong and good solution, but it faces some problems and disadvantages. At first this solution is based on public key cryptography and would therefore require some data processing of the involved participants. A typically communication device could have limited possessing power and battery this would limit their solution [43].

We have taken several ideas from this proposal and further developed them with a new twist. As Asokan and Ginzboorg we apply a secure side channel which is used to exchange security credentials. Further we applying self organized trust, but with a slightly different approach than this proposal. We are using public-key cryptography, which Asokan and Ginzboorg also presented in their paper, but our solution could make use of symmetric cryptography.

3 Methods

3.1 Introduction

In this chapter we will describe some of the important elements of our procedure doing this thesis. This description of research and development (R&D) is meant to show the path we went from start to end, and it could be used by others who want to do a similar research in the same field.

3.2 Research Methodology

This thesis is based on theory, and much of our work has been literature research, and several parts of the project rely on previous work of others within same field of research. We have studied state of the art within our field used received information for further development. Many parts of this project are based on our own ideas which we wanted to study and implement into our system architecture for further study.

3.2.1 Particular questions

As basis in this thesis we are considering security and privacy in wireless ad-hoc networks, but if we derive this into four groups which we should consider, and we are therefore focusing on security, privacy, trust and anonymity in wireless ad-hoc networks. It is important to emphasize that these themes affect each other directly and indirectly and can probably not be treated independently.

3.2.2 Sources of information

As mention above part of the project relies on the work and research of others in addition to our own ideas. But we think that our concept is based on a different approach than others. We have developed our own proposed solution which consists of parts or ideas from other reaches and existing products that have resulted into a different approach.

3.2.3 Design development

In order to do R&D at state of the art level and to be able to accomplish our thesis we had to perform massive and comprehensive literature searches which also are reflected in an

extensive reference chapter. We have evaluated and developed parts of others proposed solutions in addition to do our own "twist" into a solution which differing from others. Our goal is making a solution with some modification which could be made use of in existing equipment. The proposed solution consists of two parts. The use of secure side channel is based on previous state of the art research by others with a few modifications we have made our selves. The PRI part and related architecture which enforces privacy and anonymity are based on our own ideas. These two solutions are melted into each other in order to make a basis which is able to handle system which should improve our four particular issues (security, privacy, trust and anonymity).

The proposed solution is done at a very general level and should therefore fit into various devices and systems. It is also made general because the particular issues are very much affecting each other and in order to make a core solution which could fit into most of today's ad-hoc devices, a general solution should be the basis.

3.2.4 Data collection

We have used many different information sources and during the project progress we had to adjust our ideas. This resulted in some additional literature search. Sources for information have been libraries, digital libraries, internet, resource persons, other projects and research from sources like IEEE and similar. The propose was to get information directly from trustworthy sources, either it was directly or indirectly by tracking source of information from other papers back to the real source. We consider this as important in order to avoid getting misinformation.

3.2.5 Practical analyses

We have done some experiments in this thesis. Since we base our solution on pseudo random generated ID (PRI) we wanted to find out the probability that 2 or more devices generated the same ID. Such analysis is done because we wanted to see the probability of identity collision within the very same network, and from such an analyse a decision Further we wanted to find out how many bit ID that were rational to use then the system should not, with high probability, generate same ID. In order to evaluate this problem we constructed a software random generator, with different bit length. We made use of Microsoft Visual Studio in *C#* and further used *MATLAB*, an integrated technical

computing tool that combines numeric computations, to derive statistic over random number collision probability. We have also performed a survey with intention to find out peoples awareness on security and privacy within wireless communication systems and what they think of possible upcoming solutions which indirectly are related to out thesis. We also allow for their opinion in the discussion and conclusion part (Chapter 7 and 8) since the end-user actually are the final customer.

3.3 Project Management

To organize the progress of this thesis we identified several milestones with individual deadlines in order to keep our schedule on track. It was natural to derive the project in to three main parts, each with several milestones. First we had to identify the problem and derive the problems to be addressed. This task consumed a certain amount of time since the problem statement was very confused and had no clear target. The second stage was to investigate and research other similar project and subjects in order to understand state of the art and how to do further research from such level. Since this thesis is based on theory, literature study has become a large part of this project and were very time consuming. In stage three we had to work out a solution which could improve today's security and privacy in wireless ad-hoc networks. During stage two we got lots of our own ideas and decided try out a few of them. This resulted in a theoretical architecture development based on the particular problems derived in stage one, our ideas we got from stage two together with our knowledge we acquire during the whole thesis.
During the pre-project phases tasks and temporary milestones was temporary identified, but it process was also part of stage one for this thesis. Identifying the milestones of a project, their order of commencement and completeness, generally increases the probability of success [49].

The process of making a theoretical model was divided into four subjects: security, privacy, trust and anonymity. The short time scope of the project resulted in theoretical model.

In the beginning of our project we were recommended to use NS2, the network simulator, which is a powerful network simulation tool. This tool was meant to carry out all the performance simulations for the thesis. We investigated and performed some tests with this tool and concluded that it wasn't suitable to our project. NS2 is able to simulate both wired

and wireless networks with various components in different environments. However, NS2 is great for simulating dummy traffic in all kinds of network in order to do dummy-measurements, but for our project we actually had to consider the payload information for data in the network. We could not find any existing modules or classes for NS2 doing so. Alternative we could develop our own NS2 components, but this would been off track for our thesis, relative complex and probably very time-consuming. Performance aspects were not required for our thesis, but a thing to do if time permitted it. This wasted task was consuming of valuable time.

The report was continues written during most the project and during the progression progress we have had to change/rewritten several parts in addition to restructure or adding information. The three main stages of the thesis are being crass faded, and many tasks are being worked at continuously.
We illustrate the distribution of work on different part of thesis during project in Figure 13.

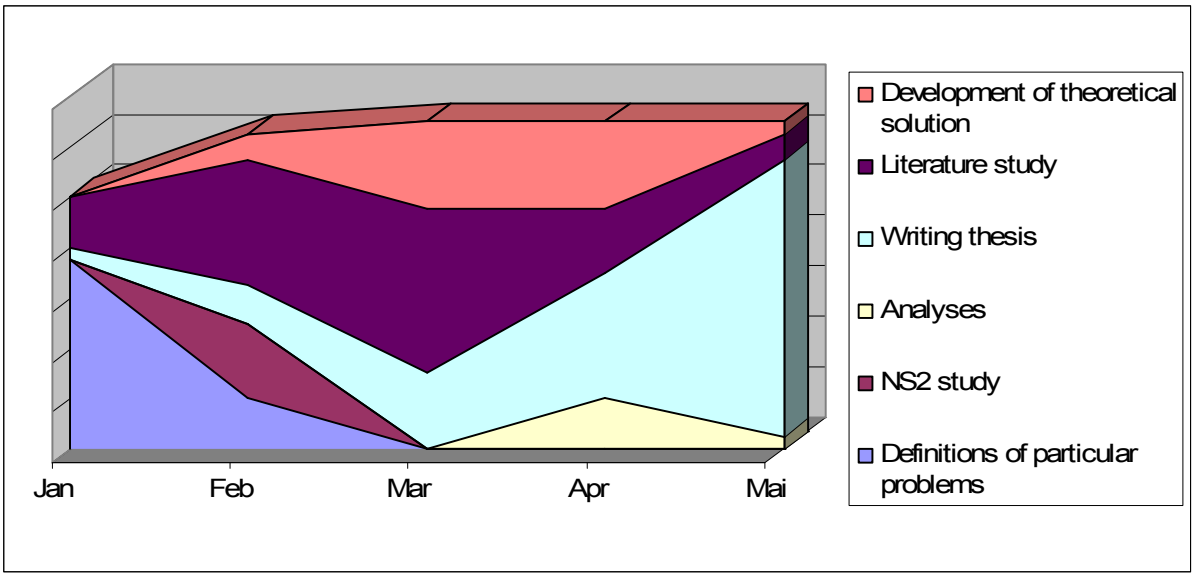

Figure 13: Sketch of progress

4 Proposed solution

4.1 Introduction

As mentioned in the introduction chapter, various security-aspects might counterweight each other in such way that a perfect solution for one aspect does not make it possible for the second aspect to be perfect. Different solutions have to work together without disable or counteract each other. It might be more complex when there are many aspects to consider. We will present and describe a solution for security, privacy, trust and anonymity in the wireless ad-hoc network environment, all operating in the very same scenarios. The solution we present is the solution that seems to fit the security aspects best together. We consider a wireless ad-hoc network of mobile nodes, where each node represents a personal device for the end-user.

We consider this network to be fully self organized, which means that there is no infrastructure, no global central authority or global Trusted Third Part (TTP) and no secret share dealer.
The solution we present in this thesis is partially taken from an existing project "Mobility Helps Security in Ad Hoc Networks" [45], though we have made our own tweaks to make our own solution in order to consider additional issues and improve the security and privacy.

4.2 Solution

When new nodes are within range of an existing network, it should be possible to get a list of active nodes for this network. When receiving this list, it does normally not tell anything about who or what kind of nodes one are registering and all nodes will often be perceived as equals as shown in *Figure 14* (Figure in the middle could be *you*).

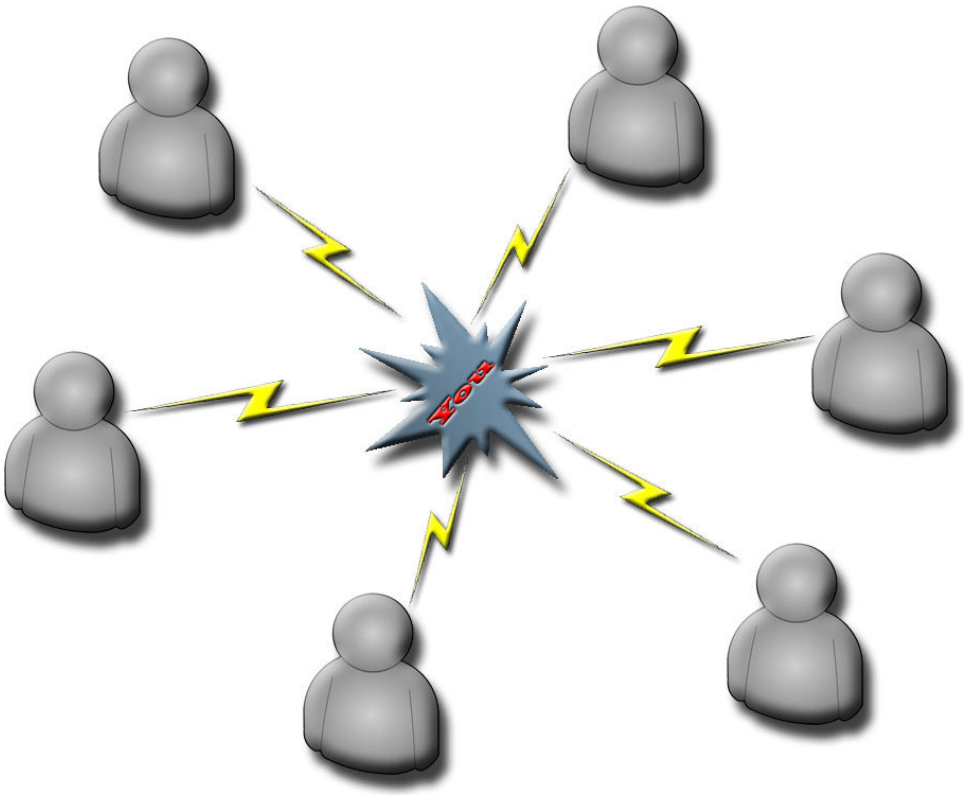

Figure 14: Ad-hoc network where nodes seems equal

Our proposed solution is based on two major fundaments. These two fundaments complete each other and make it possible to improve both security and privacy in wireless ad-hoc networks, parts of this solution is based on state of the art research. The solution is simply using dynamic identifier (described as PRI later) and having the possibility to establish an isolated and directly point to point communication (also called Secure Side Channel, SSCh.

Generally, the dynamic identifier will be the node's address, and for public non-secured use data is sent to this ID and should operate very similar to the IP technology when it comes to routing and delivering of addressed data in the network. But this could be a vulnerable architecture if various threats or malicious nodes should arise. The fundaments by improving security and privacy will be explained later in details in this chapter.

How to make use of this solution in various scenarios with various needs will be explained in chapter 5.

4.2.1 Alternative communication channel for the initial part

One of the major problems by using fully self organized ad-hoc networks is to establish trust between two devices, especially for first-time connections. Then data transfer is on the air, it is vulnerable to both passive and active attacks. The challenges are exchange of encryption keys and initiate the communication channel with the correct node. Communicating on the air might make the establishing of trust very hard. We suggest alternative ways to establish trust and secure communication

The principal of a Secure Side Channel (S.S.Ch.) is relative simple, and have several useful properties:

- Communication is totally isolated from other networks and channels (Therefore it's called Side Channel) and should therefore be immune to both active and passive attacks.
- Trust should be established between the two communicating devices, even for first time connections, due to physical encounter.
- Point to point.

4.2.2 Establishing an S.S.Ch.

In scenarios when it's needed to establish trust and a secure communication channel, the two parts most likely have meet and visually identify each other. The need to set up secured communication is based on these people's physical agreement and trust.

We assume that each device is equipped with a short range connectivity system (e.g. IrDA, possibility for wire etc.). Secure side channel does only work as point to point, and require that the communicating devices are close to each other. In this way, the channel is isolated, kept secure and makes sure that the actual device is identified. Most of today's personal devices are equipped with an Infrared Data Association (IrDA) port, and we consider therefore assumptions for such use as realistic. Due to the physical limits of this way of communicating, a Secure Side Channel is compelled to be both trusted and secured.

4.2.3 Authentication of actual devices

Since the Secure Side Channel only works within short ranges, and when using IrDA one often has to aim the IrDA ports directly towards each other to get it work properly, the purpose for such channel is to exchange critical initial data. The idea is to exchange a so-called security triplet [45]. A triplet is a "package" of three important values that is used for further communication, and is typically values for Identity, Node address and public key. Figure 15 illustrate triplet exchange between to devices via IrDA (SSCh). The exchange of triplets is quite similar the exchange of electronic business cards (vCards) between cellular phones and PDA's etc [50].

Figure 15: Secure Side Channel over IrDA exchanging Triplet.

Most important part of the triplet, when it comes to trust, is the cryptographic key. It will only be the owner of the generated public key who is able to decrypt the encrypted data transmitted. To authenticate the node before transmitting on the air, one has to check the other device's identity and cryptographic key, so no other (malicious) node could be able to decrypt encrypted data. If security triplet exchange is done without error, you know for sure that the remote node is the only one who is able to decrypt your transmitted data. To make sure that correct cryptographic keys has been exchange without error, we apply a simple challenge-response authentication method as illustrated in Figure 16.

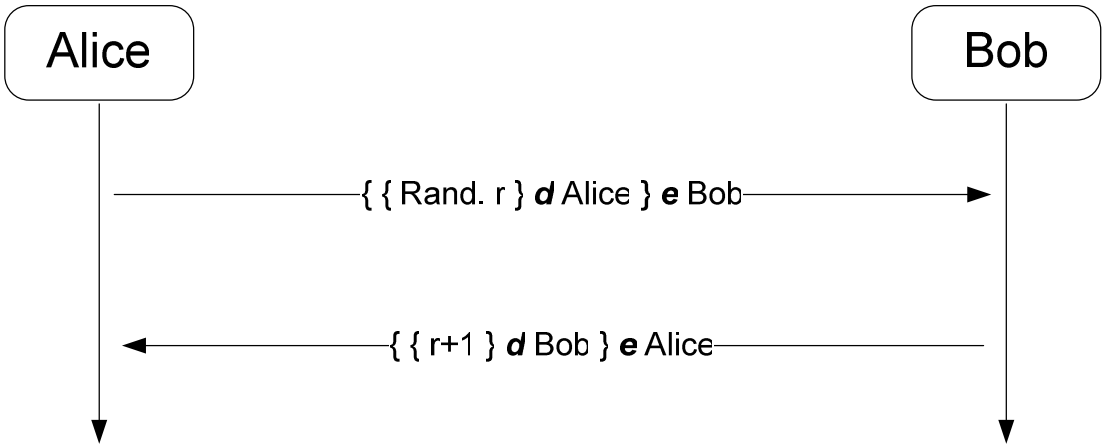

Figure 16: Challenge-response diagram

When both parts have each others public key, they can secretly exchange data which only the other part is able to decrypt. The public key is mathematically related to the private key, but it should not be possible to deduce the private key out of public key(s). The private key is kept secret, while the public key may be distributed. This is called public key cryptography, and is an asymmetric encryption method.

The challenge is simple. As shown in Figure 16: Alice generates a random number (Rand. r), adds digital signature (***d***), and finally encrypts it (***e***) and sends it to Bob. If and only if Bob is the owner of the public key Alice received and used for her encryption, Bob would be able to decrypt the data transmitted from Alice. If he didn't send his own public key to Alice, he would not be able to decrypt and can't give the correct respond to Alice. Bob adds +1 to the received random number (r+1), adds his digital signature (***d***) and finally encrypts it (***e***) and sends it back to Alice. Alice is the one who initiate the secure communication, so she knows she sent her public key to Bob. Now, if she is able to decrypt, and finds her random number is increased by one (r+1) then the challenge response procedure is correct, and she knows for sure that Bob is whom he seems to be.

This challenge response procedure is done over the secure side channel, and therefore one doesn't need the digital signature, because one knows who one are communicating with. But adding the digital signature, one can verify each others keys with just one challenge response since the digital signature is related on the private key. In that way Bob is able to see if Alice gave him the right key in challenge response, even if Alice is who initialized the challenge in the beginning. (Alice is the one who wanted to verify Bob's key, and with digital signature Bob is able to verify Alice key at the same time.)

When the initialization is done, as shown in Figure 17, both parts should have all necessary information and may close the secure side channel. Further communication should be done by transmitting on the air and would be secure. The parts may split up wherever within range for the rest of their conversation.

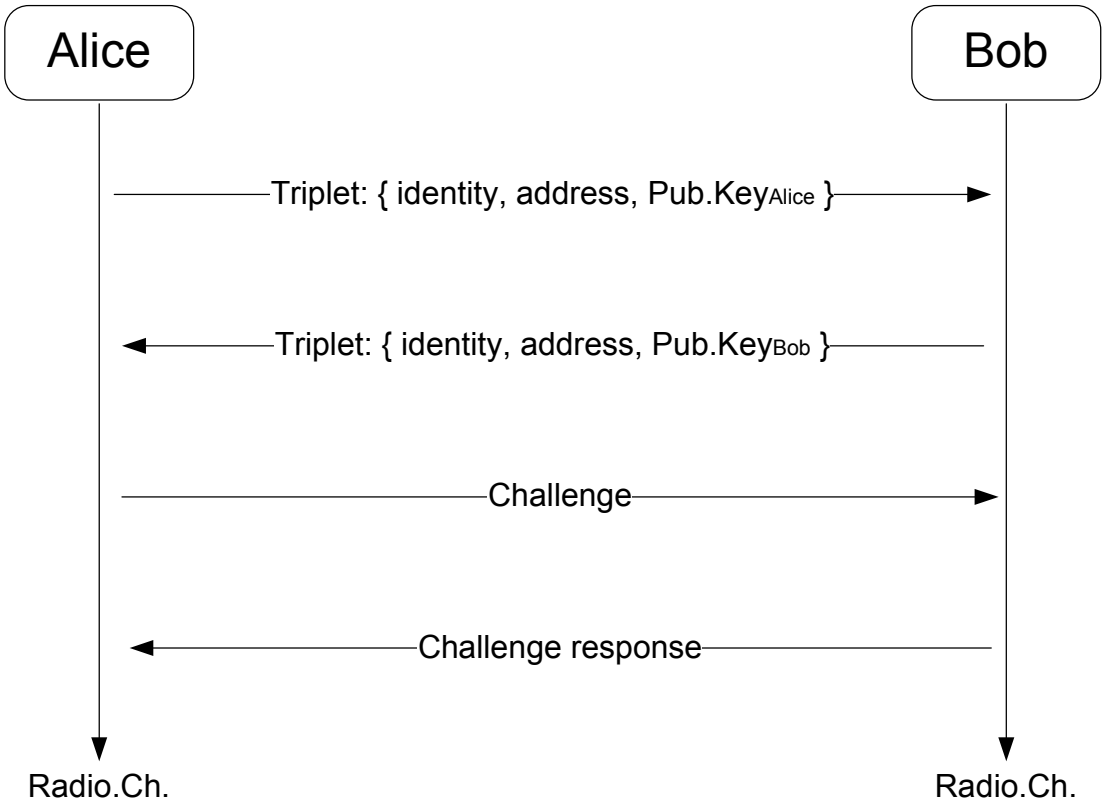

Figure 17: Asymmetric initialisation over secure side channel.

4.2.4 Initializing secure communication

Security credential exchange over the Secure Side Channel is optional, but this is a necessary initialization phase for secure communication on the air. Because it's very hard to establish both trusted and secured communication on the air only, we exchange the critical initial data over the secure side channel, and in this way we are able to" visualize the face" of the device we wish to connect and exchange the triplets containing the needed values to establish a secure connection, without initializing on the air. In this way one may start a secure communication on the air directly, and one does not risk that any malicious nodes could decrypt the transmitted data.

4.2.5 Initialization vs. established

One important property for the asymmetric cryptography is the possibility to exchange keys without compromising decryption key in order to establish a secure communication. But initialization phase in wireless communication faces several critical threats, because one have to be absolute sure that received public key are related to the correct device (ID), and this process is even harder with dynamic identification method. Therefore we propose to do the initialization phase over a Secure Side Channel where one could be sure that other device is wanted receiver. Still in order to prevent error in initialization phase our solution uses an asymmetric challenge-response authentication test.

General, we initiate the communication via public key cryptography. Then the secured communication channel is established we carry out a symmetric session key exchange in order to change encryption and decryption key into a shared common key. By the use of a common cryptographically key one will reduce the communicating devices possessor load.

4.2.5 Handling various nodes

The particular problems will occur in various relations and makes different problems. Usually there will be several types of devices which operate in different ways, and one has to consider these nodes in different ways. Figure 18 illustrates a scenario with several types of nodes and some of them are making a threat and others are automatically and operate alone etc.

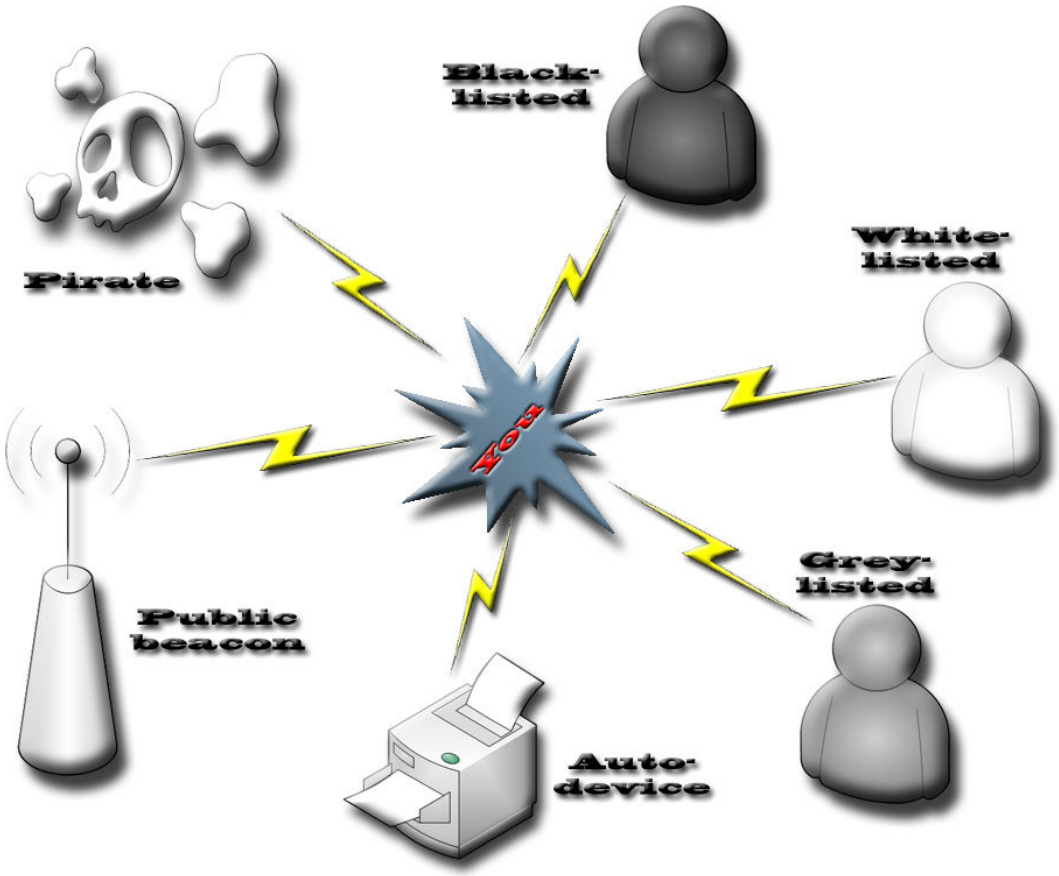

Figure 18: Complex scenario

The idea is to evaluate all other nodes and rate them individually on a trust level scale. Such rating should be done by observing the remote nodes behavior, type of connection and so on. This evaluation is the basis for how one is going to categorize remote nodes individually. Every node should be rated and placed in a certain group (lists). Such different groups have different permissions which should ensure one's security and privacy. As an example we have used ranks nodes for three levels. Blacklisted (bad behavior), grey-listed (unknown or fair behavior) and white-listed (trusted) nodes. This is described in more detail in chapter 4.4.

In this scenario, one of the nodes (Pirate) has malicious purposes and is probably doing either passive or active attacks. A pirate is often hard to discover, especially passive attackers, and in some special cases one can't exclude a pirate [60]. The best way to enforce privacy when exchanging sensitive data, with a pirate in the network, is to establish a secure communication channel initialized by secure side channel or chain of trust (explained in chapter 5) through to the communication partner.

A public beacon is continuously broadcasting some kind of information, for example invitations for commercials sent by stores, or it could be information for tourists when they pass by e.g. cultural monuments etc. This is considered as public beacon, and does normally not require any secure communication channel due to the type of information sent. Beacons could be recognized by a unique filter-value where the PRI describes the type of device. Malicious nodes could easily simulate public info beacons, which mean one, have to decide if one want to trust the beacon or not. This is the case if you for some reason don't have the possibility to establish a secure channel. Opportunities dealing with this problem are described in chapter 5.

Auto devices are types of nodes which operate alone. This could be for example printers, servers with some wanted content etc. Auto devices could be recognized by a unique filter value in the PRI describing type of device. If one have to send or exchange secret information (personal information which should be sent to the printer, storage of sensitive information on the server etc.) one should establish secure communication channel initialized by secure side channel or via known trusted nodes. This is referred to as "Chain of trust".

New nodes might join the network, and are within range, where is no way to know who it might be, and consequently it can't be trusted and could therefore be gray-listed, which means they are neutral. The white-listed node is someone you know, and is therefore trusted. Trust is often initialized by chain of trust or S.S.Ch. and is often operating in an established secure communication channel. The blacklisted node is someone which has proven bad behavior or might be annoying. It might be a pirate, but a blacklisted node doesn't mean that this node had performed pirate activities, but it could be blacklisted for other reasons such as spam, unwanted actions or other disrespectful behaviors.

4.3 Dynamic Identifier

A dynamic identifier is a Pseudo Random generated Identifier (PRI) which is a generated random sequence and should be different and statistically very independent from every other device that uses its output. A pseudo-random sequence is a sequence that is not random, but very hard to distinguish from a truly random sequence. A pseudo-random sequence should also be difficult to predict, i.e., given the first few elements of the sequence it should be difficult do determine some later, yet unseen, number in the sequence [51].

One important reason in to use pseudo random sequence or ID in our project is that it's desirable to make all communicating devices anonym and hence enforce privacy. Instead of using a static identifier (such as e.g. MAC Address) we make use of a long, random identifier. Each communication device bases their identification on a local pseudorandom generator. This would make it virtually very hard to identify each participant in a communication sequence and prevent tracking [51].

4.3.1 Keeping the MAC-address secret

In today's wireless systems, the medium identifies the nodes by their MAC identification. This is a unique static identifier which compromises the anonymity of each user. Both IEEE 802.11 and Bluetooth protocols are constructed in such a way that each online device broadcast their MAC address. This result in major risk of becoming tracked since everyone could read their broadcasted ID as well as the probability getting logged (tracked) at several static nodes.

Another way to remain anonymous is communication by keeping MAC-address secret. Every device involved in the communication which hides the medium identity will be invisible for rest of the network. Since each device is invisible both anonymity and privacy are preserved. This is done by broadcast information which only could be read if the receiver has a specific cryptographic key. These cryptographic keys have to be pre-shared over a secure side channel [52].

4.3.2 Pseudo Random generated Identification (PRI)

Pseudo random generated identification would be able to replace MAC identification in current systems. But broadcasted identification should only be used in those scenarios that require this feature. Several wireless ad-hoc scenarios don't require visible communication partners. In fact it is desirable that devices in secure scenarios don't broadcast their identity to maintain privacy [52].

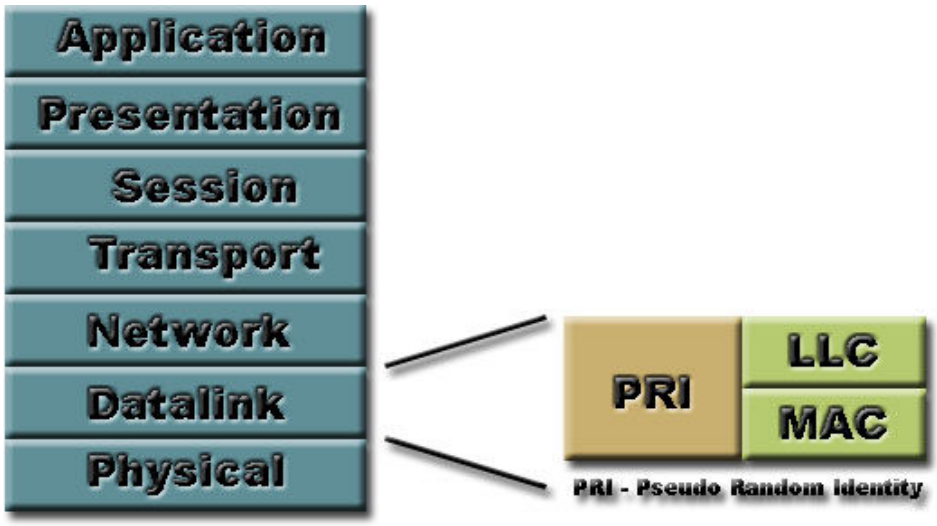

Figure 19: PRI in the OSI-model

The PRI should be implemented in the OSI-model at the same layer as the existing MAC address (layer 2), in order to let the medium know where to deliver data packets. In Figure 19 we have added PRI in layer two additional to the existing MAC and Logical Link Control (LLC) to keep compatibility. The PRI layer is pretty much the same as the MAC layer, but it could vary in length and would be able to be changed quite often, and the value should not indicate anything in order to enforce anonymity. The use of PRI layer could be thought of as a MAC address which is spoofed very often to keep anonymous.

There are several scenarios which require broadcast of identification. In these scenarios it is highly desirable to maintain privacy by obtain random identification in order to avoid leaving static values (tracks). We have two main groups that require two-ways communication: with or without exchanging sensitive information.

To maintain randomness and prevent collisions we will recommend to construct a random ID that consist of 32 to 64 bits, where 8 bits are optional group identification. When the user or device is a part of a group the random ID will consist of 24 to 56 bits and 8 bits group filter. When the user or device is not a part of a group the random ID will consist 32 to 64 bits. Figure 20 illustrates an example of allocation of PRI address field with group filter.

|Group ID | **Random ID** **|**

Figure 20: PRI address field

32 bit identification represent 2^32 that equals more than 42*10^8 different ID's.
64 bit identification represent 2^64 that equals more than 18*10^18 different ID's.

Even with very high amount of combinations, two devices could obtain equal identification so an identification error correction that forces one or both devices to change ID to prevent further identification error should be implemented (described later in Chapter 6).

4.3.3 Change identification

Even though random ID prevents any attacker from directly identify a wireless communicating device it is crucial that ID are being changed on a time based interval to prevent tracking and identification. Any user must be able to choose how frequently the random identification should be changed. This property would make the user able to decide their privacy level and avoid tracking.

To illustrate tracking we present a scenario where a person walks through a town. This scenario is based on a wireless ad-hoc communication device that broadcast its static identity. Every movement could be tracked by antennas or similar tracking devices along the path. Figure 21 illustrates how privacy could become compromise with today wireless technology.

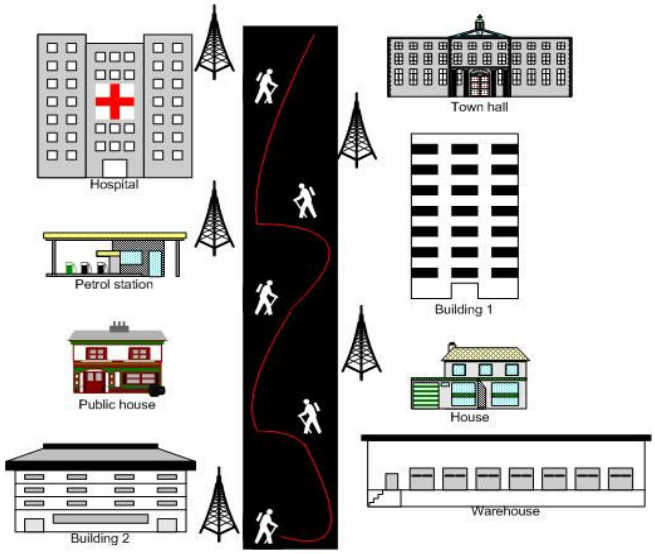

Figure 21: Tracking scenario

4.3.4 Avoiding identity collision when joining networks

As long as every device is generating a Pseudo Random Identity (PRI) there exists a slight chance for duplicate identities. Two devices within range might generate the very same identity, which means an identity collision. For public and non secure conversations, this will lead to routing confusion, and direct addressed information might get sent to the wrong device as well as the right device. As long as this kind of probability exists (as long as the probability is greater then zero), some kind of handler have to take care of such problem.

Figure 22 shows an SDL-diagram of how one could connect to an existing wireless ad-hoc network without making any identity collision and at the same time collect and make a node list for this network (nodes within range). The principle is taken from the idea behind ZeroConf [58]. The idea is to check out the network for equal identities inside the existing network before joining the network with the newly generated PRI.

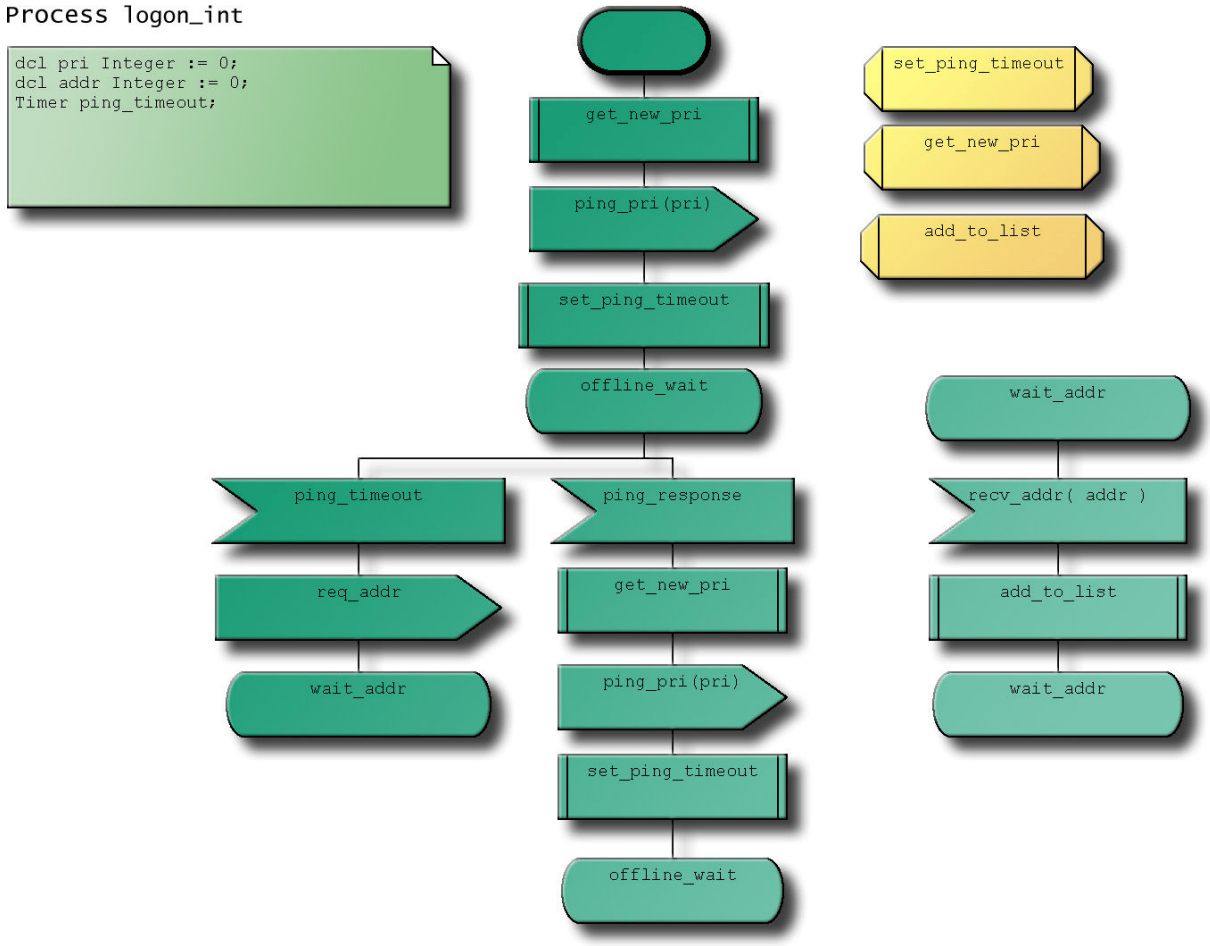

Figure 22: Avoiding collisions and getting node list while logging on a network

One starts with generating a Pseudo Random Identity and simply do a ping-request to the very same address as one just generated. One waits for a certain time, and if someone should actually use the very same address as you just generated, this node will response the ping-request with a pong-response on the broadcast channel. This is done because you don't actually have your own (registered) address in this network yet. If this is the case, one have to start all over again by generating a new PRI and do a new ping-request at this new PRI address. If nobody uses the generated PRI address, no one will response, and there will be a timeout, and if it times out, one might consider ownership for this address in this network.

Next step is to obtain all node addresses in the network. One is now registered with a verified PRI, and does a broadcast request for node addresses. Every node within range will receive this request and might note the senders address before replying with its own address. In this way, every node will be updated when someone joins the network, and the one who is joining the network gets a list of all active nodes. Of course, every (other) node must also be able to response to ping-request and node address (PRI) requests. Such SDL-diagrams is not included here.

4.4 Trust levels with permissions

Trust is an important aspect of distribution information. It is also one of the most important concepts guiding decision-making. In order to handle these aspects automatically we make use of dynamic trust model with associated trust list. By clarifying the trust relationship, it will be much easier to take proper measures, and make correct decision. All decisions should be made on the basis of the trust list: white, grey and black as shown in Figure 23.

Figure 23: Trust lists

A very simple trust list example could have properties as followed:

White trust listed: Access to all shared information.
Grey trust listed: Access to limited/non-shared information.
Black trust listed: Access is blocked.

Since this solution is based on random ID we patch the random identification with one of the trust specification. All parties who typically are connected via secure side channel will be added into the white trust list. All parties who are added via an unsecured connection will typically be added into the grey trust list. Devices that are added via wireless ad-hoc wireless links will therefore be added into the grey trust list. All parties who are black listed are automatic blocked by the receiver.

With the dynamic identification model, other nodes behaviour will result in what group (list) one decides to place the concerned node. Good behaviour could be reworded with a higher trust level dependant of one's device settings (e.g. white-list). Bad behaviour will be punished with a lower trust level (e.g. blacklist).

It is important to emphasize that black listed devices don't necessary means that the user is a pirate. This could simply mean that its behaviour is unwanted by the receiving device. This kind of behaviour could be advertising beacons of certain type or other unwanted behaviour such as annoying nodes (spam etc).

5 Practical use

5.1 Introduction

In the previous chapter we presented the core of our proposed solution. In this chapter we will talk about how this solution might be used in various realistic scenarios, and how it might solve security and privacy issues which are present in such situations.

5.2 Individual Scenarios Affected

We have considered several scenarios when this concept was developed, and our solution is based on the various requirements needed. To understand the scenarios defined, one has to understand what the figures are supposed to illustrate. Basic node types are shown in Figure 24:

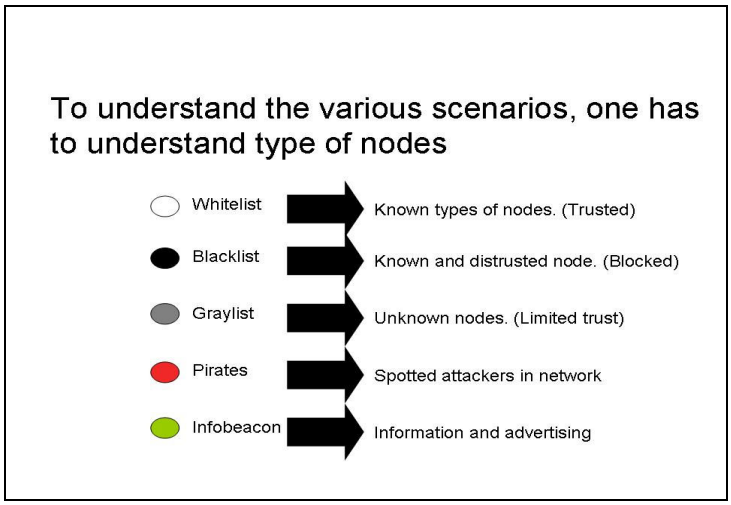

Figure 24; Node definitions

White-list is notification (lists) over trusted nodes, which means one do trust the actual nodes. White-listed objects means that you know for sure who is communicating partner and it might also indicate a secure communication. Gray-listed nodes are those one doesn't know (yet). These devices do normally not represent any immediate danger, but one never knows as long as they are not trusted, and should treat them thereafter. The blacklist is for those who have proven their suspicious or unacceptable behaviour, and they would be blocked from further communication for a given time. Red indicates pirates or hackers who perform attacks in the network, or somehow unwanted. Green nodes

indicate public info beacons, which is typically for broadcast commercial in stores or shopping streets etc.

5.2.1 Local trusted third part (Local TTP)

Since this solution in principal only allows trust after physical encounter, it could be bothersome to actually meet everyone one wants to establish secure and trusted communication with. It could therefore be an idea (solution) to use a local trusted third part to link common trusted nodes. An example could be if everybody in a network is spread out inside an office building, or maybe far out during a rescue operation. It is not be necessary or desirable for everybody to run around to initiate secure communication with each other. A local TTP could be a device who knows many nodes (white listed), but its sub-nodes doesn't know or doesn't trust each other as shown in Figure 25. Since all these sub-nodes have a common trusted device, one could make use of this advantage.

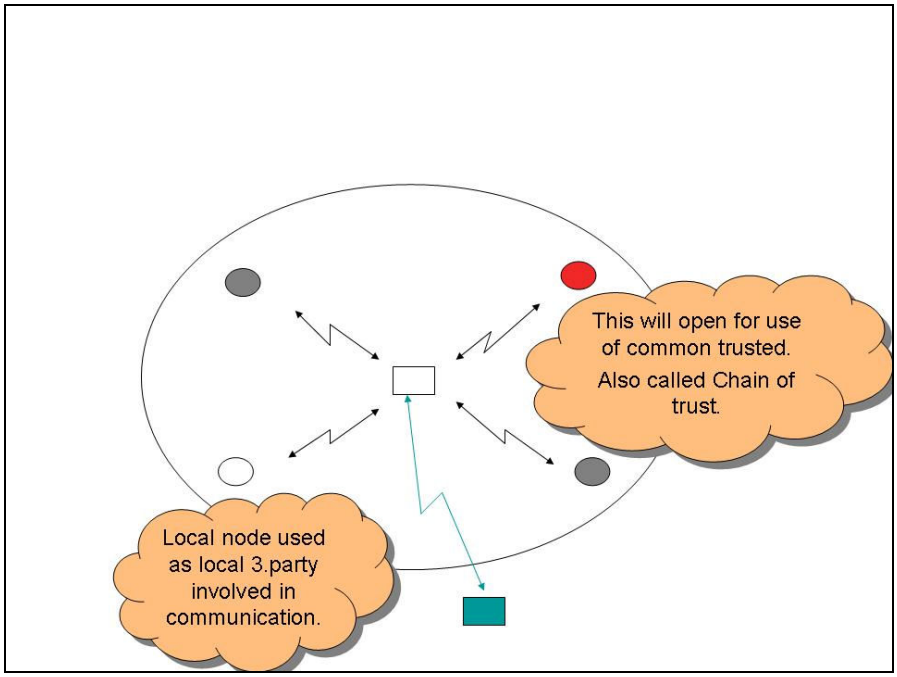

Figure 25: Local third part

To state a simple example, we will use Bob, Alice and Carol, where Bob knows both Alice and Carol, but Alice doesn't know Carol and vice versa. After the secure side channel initiation they could get far away from each other (but still be within range). This type of trust relationship is showed in Figure 26.

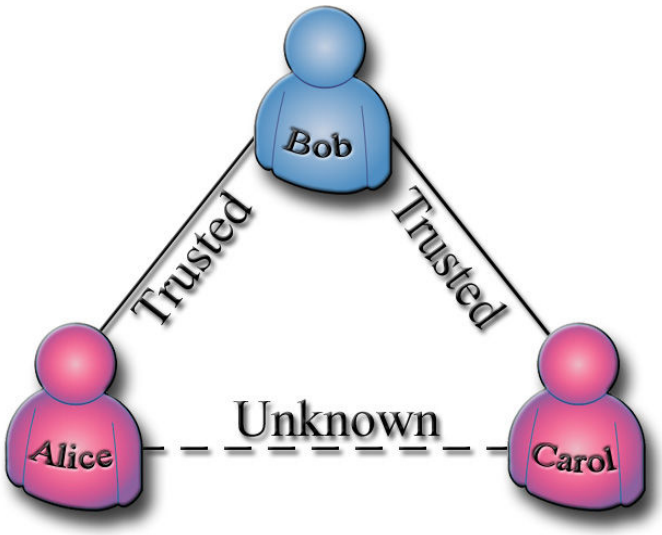

Figure 26: Example of where to use chain of trust

Retrieving trust through a local TTP is in principal based on existing trust relationship, but even so, the local TTP (Bob) should not be able to read the future conversation between Alice and Carol due to privacy and as a principal itself. This is possible by initiate the conversation with public key cryptography.

Alice wants to establish a secure communication channel to Carol, but Carol is somewhere else pretty far away, and the request has to go over the radio channel through Bob (Local TTP) because he knows both of them.

Alice asks Bob to request Carol if she is interested to establish a secure communication channel with her. In this way, the whole session will go through a secure channel. If she accepts the request she will return a response to bob with a triplet who is digitally signed, containing her public key and node address. Bob will deliver this message back to Alice. Alice's request is accepted and she now got everything she needs to start an encrypted channel with Carol. The first thing Alice has to do is to send her own public key to Carol together with her digital signature, which enable her to establish a secure channel back to Alice. But to really ensure that Carol hasn't sent someone else's public key, she has to respond correctly on a challenge from Alice. If everything goes well, Alice and Carol has established a secure communication channel with each other over radio channel through a local TTP (Bob), and Bob isn't able to understand anything of their conversation. As long as trust is correctly placed, one should not be able to compromise the chain of trust. The most important fundament for this method is that both sub-nodes (Alice and Carol) really trust Bob.

Figure 27 describes how the sequence is executed between Alice, Bob and Carol in order to ensure trust and security on the air only (Chain of trust).

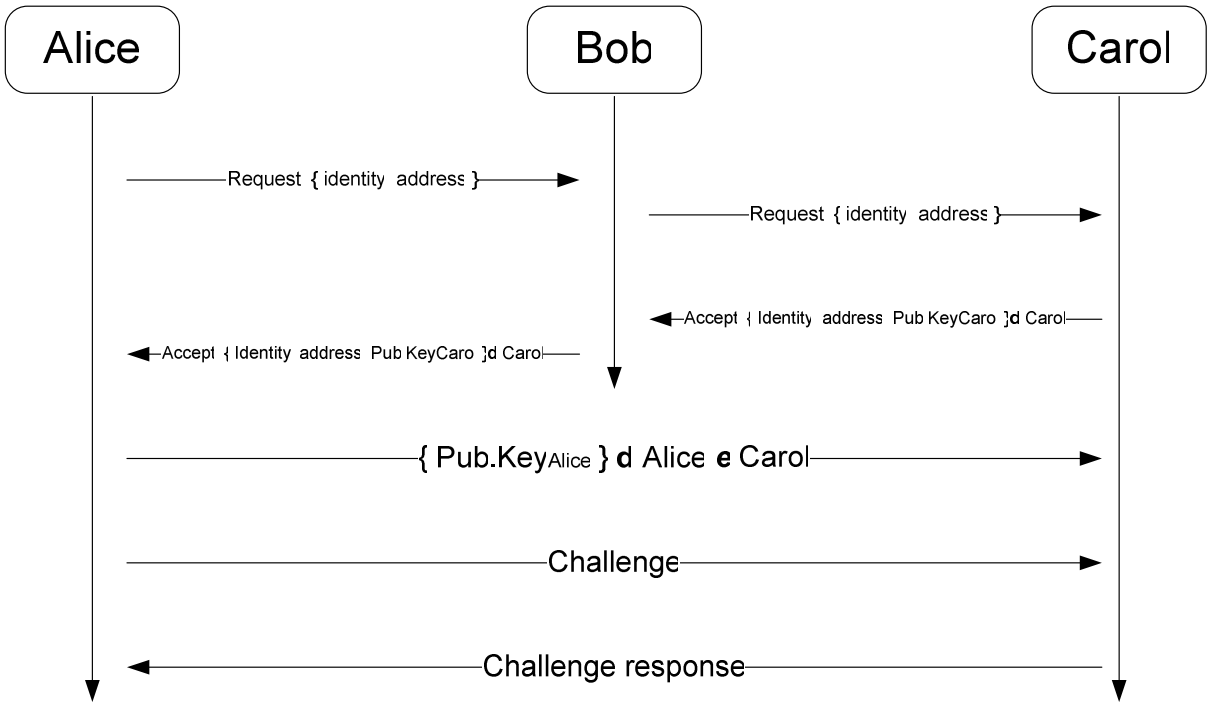

Figure 27: Establishing secure connection through chain of trust

For smaller devices with less processor and battery capacity, it would be smart to move from an asymmetric cryptography to symmetric cryptography for the conversation. Simply by create and exchange common symmetric key over the existing secure channel. Symmetric cryptography requires much less CPU and energy usage, and would make data exchange more efficient and devices will make better use of available energy (longer total operation time).

5.2.2 Information and advertisements beacons

Figure 28 illustrates, for example somewhere in the shopping street, with several info beacons which are surrounding the area. Info beacons are considered to be used for public use, and will therefore be treated as unknown nodes. Info beacons could identify them selves with special identity codes reserved in the identity group filter field. The code could also be able to tell what kind of information that is transmitted from which type of filter-code. A malicious node could easily hack the identity field and identify itself as an

info beacon, but still, it is considered as unknown, and may easily be blacklisted at any bad behaviour if preferred. Once again, permissions for the various groups are important.

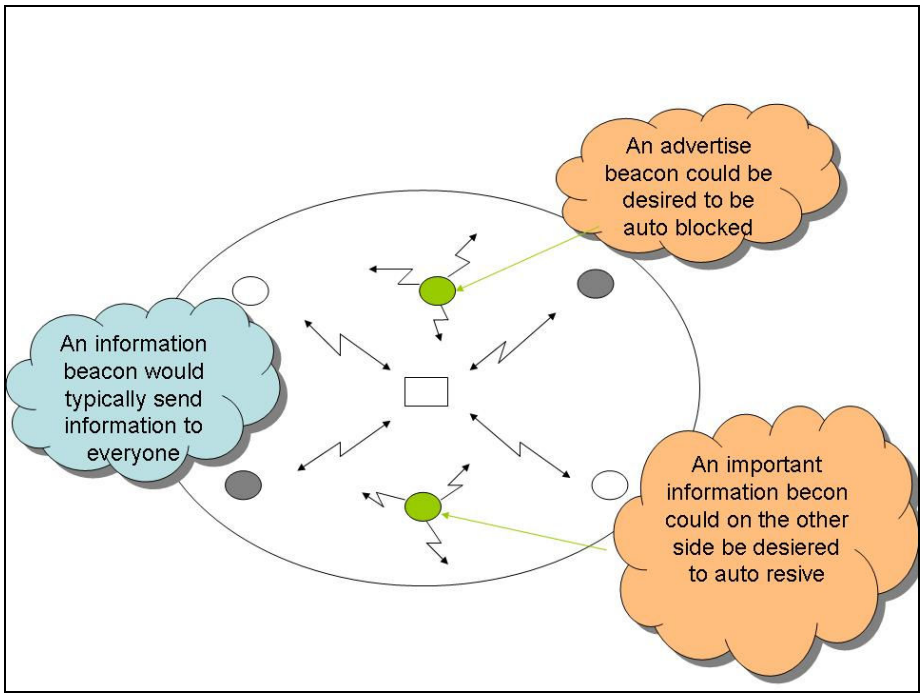

Figure 28: Public beacon scenario

One could for example allow information from beacons with helpful information (tourist/public information), and forbid unimportant info (for example advertisements etc), simply by setting up an ignore list. To keep anonymity, one would typically generate new identity regularly. One could also block release of ones identity to be invisible for the info beacons, in that way one is still able to receive broadcasts, and stay completely anonymous. The result will be that no tracks are left behind at all. But as soon as one want to communicate with the info beacon, (two ways) one have to give away the identification, in order to let the medium be able to route the specific data to the correct device (information exchange between two devices).

Beacons and nodes could typically have a conversation like we have illustrated in Figure 29.

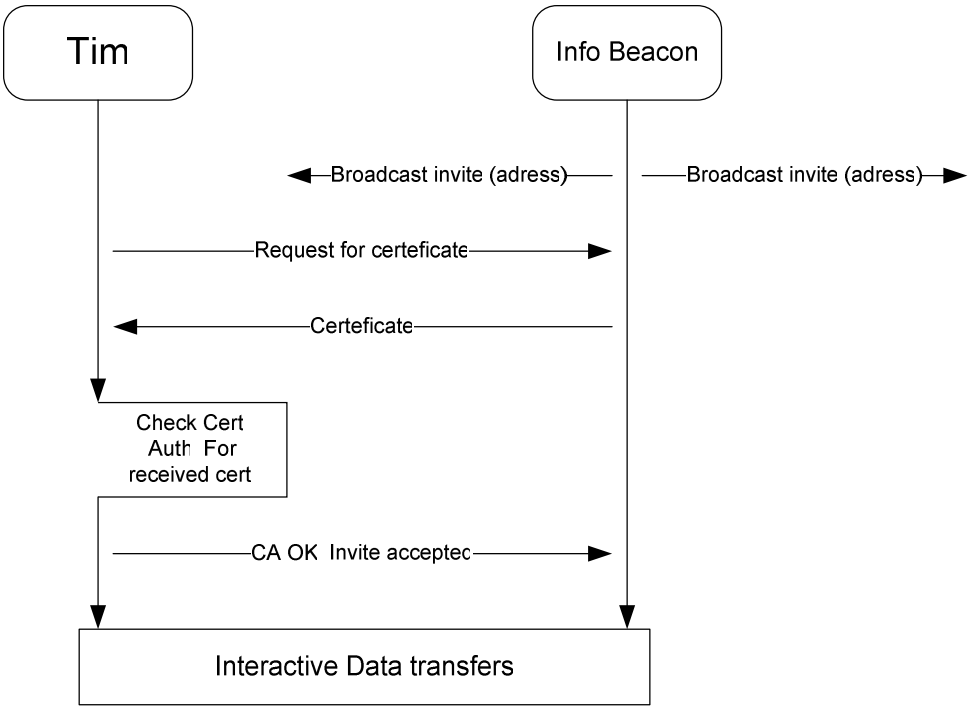

Figure 29: Public beacon sequence

A public beacon would typically broadcast invitations to interactive communication. If a node (Tim) finds information offered by the public beacon interesting and wants to do interactive communication, he would like to minimize the chances of being attacked by a pirate. This is done by answer the broadcasted invite with a request of certificate. The certificate should contain enough information to decide if one wants to trust the beacon or not. One should check out the signature from the Certificate Authenticator (CA). To do this, one must be in hold of CA's public key, which means one must have been in touch with some global TTP in an earlier stage. This is not always the case, and if not, one has to make a sensible decision manually. If one has CA's public key, one may easily check if the signature is correct or not. If the certificate is ok, or one manually decides to do communication, one accepts the invite. Such kind of method is not on a secure channel, and sensitive data is not recommended transferred unless one could initiate a secure communication channel via some kind of automate station with a secure side channel. These types of info beacons used at non-secure channels are primarily meant for advertising, information, maps for tourists etc. and therefore no special encryption methods is required for such use. When several beacons are passed one could also consider if one should generate new identity or not in order to keep anonymous and avoid tracking as shown in Figure 21: Tracking scenario (Chapter 4).

5.2.3 One to many

There might be scenarios where the members of a certain group want to create a common conversation. If there are many members and if everybody should unicast message to everybody it will be a heavy load on the network. One want to send the message once and everybody in the group should be able to receive that message (multicast) as illustrated in Figure 30.

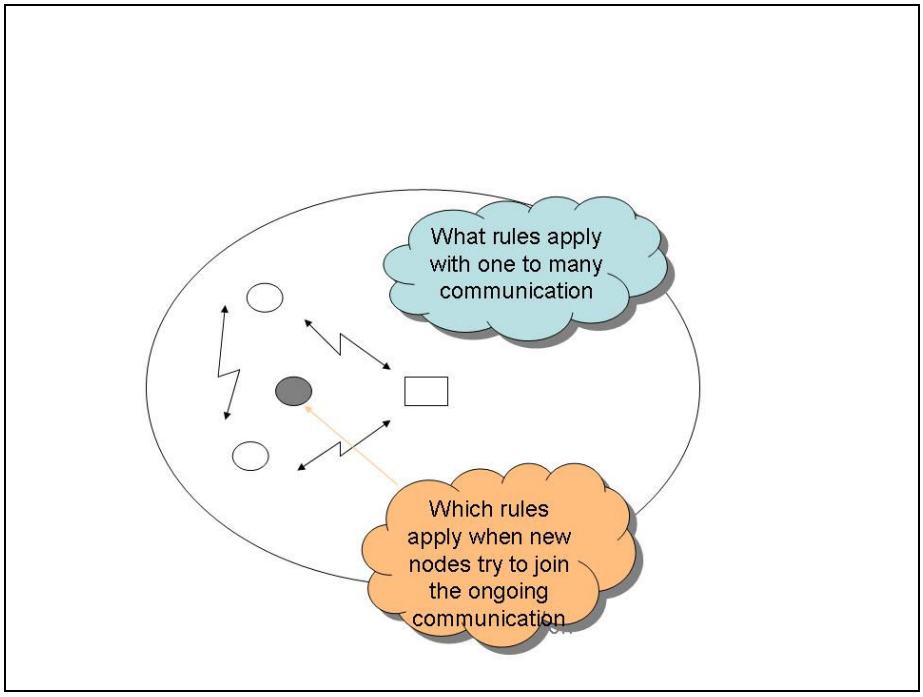

Figure 30: One-to-many conversations

Initiating of a multicast group should be done through existing secure channels. To minimize load on each device, one could generate and distribute a symmetric key to the nodes who wants to join the multicast group. This will at some point decrease secrecy of the secure channel. One could filter nodes via filter field in the identity number. This would not stop unwanted nodes from joining, but could be helpful for the honest nodes. However, the unwanted nodes can't understand anything of the conversation without obtain the common session key which is shared via an existing secure channel, probably initiated through secure side channel. Figure 31 illustrates how one could initialize a multicast group or invite more nodes in the existing group.

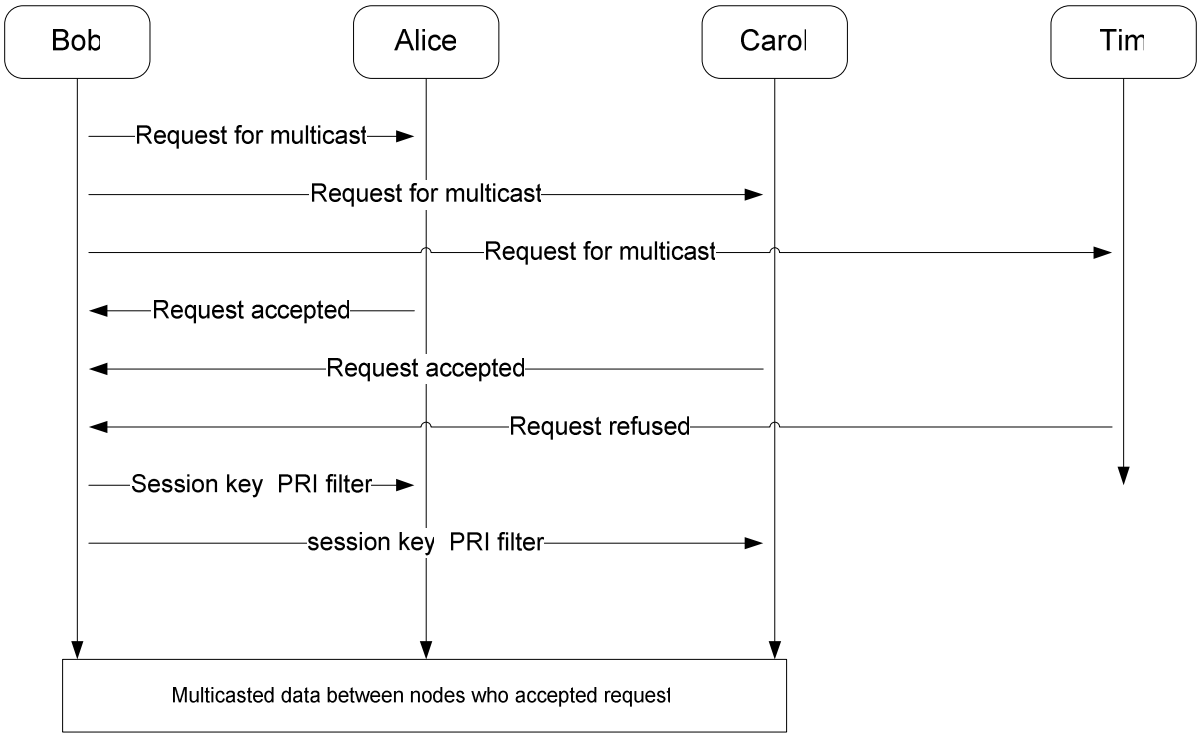

Figure 31: Initializing multicast group

If Bob wants to initialize the multicast conversation, he will send an invitation (request) to the nodes he wants to join into the group over an existing secure channel (probably white-listed nodes). When nodes receive such request, they may accept or refuse to join the group. Those who want to join reply with accept, and those who don't want to join reply with refuse. The one who initialize the multicast group will then generate and send a common session key to everyone who accepted the invitation through the existing secured channel. Everyone should now be able to multicast within this group using the shared key.

5.2.4 Active and passive attackers

As illustrated in Figure 32, the network is under attack by two hackers, where one of them is just listening on the traffic (passive), and the other is trying to intercept an another node (active).

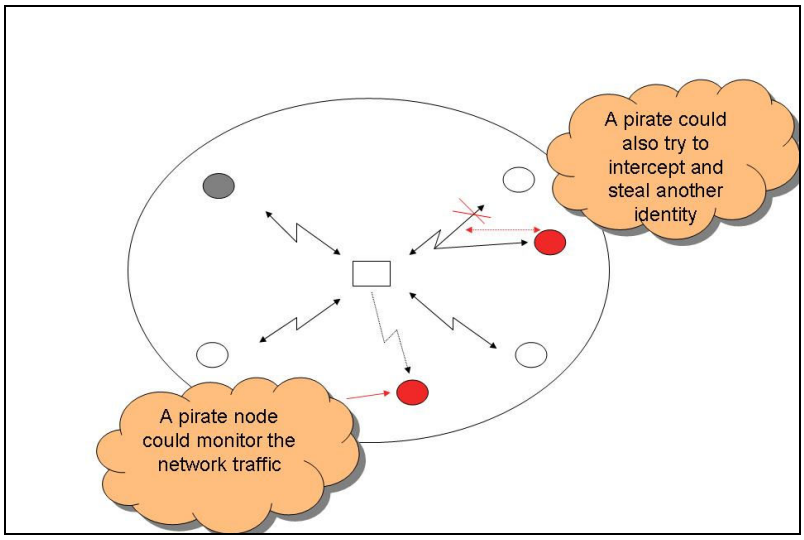

Figure 32: Active and passive attackers in range

The passive attackers is hard to spot, and further more, is some cases it could not be removed without a network-split. As long as the actual nodes are using secure communication channels, and these channels were initialized through secure side channel, the attacker will not be able to decrypt any information obtained. Thought, a malicious device could always record the information on the air, and try to break the key offline later, but with strong keys, this should probably take several years using brute force algorithm. The active attacker could not be blacklisted, because you will also blacklist your trusted part. One could simply generate new identification, but the attacker could easily keep following your identity. To keep it secure, one has no other choice then go for a secure communication channel initialized by a secure side channel or via chain of trust. In such way the attacker could not understand the conversation. One could also block the pseudo generated ID. One will probably be invisible for others, because the medium would not have anything to identify. Collisions in frequency area are still avoided because all devices are listening before sending anything (e.g. aloha likely). The information will be sent on the air with no specific target, but the only ones who are able to utilize the information, are the ones who got the correct keys. However, one must probably let ones communication partner know about this before going invisible.

6 Analysis and results

6.1 Introduction

In this chapter we will have a closer look at some interesting aspects which is present in our proposed solution. The analysis is either directly or indirectly related to the solution, and it should be used to consider what needs one have for what solution. We have taken up some subjects which we see as interesting for this thesis.

6.2 Analysis

6.2.1 Pseudorandom collision probability

Since we are using pseudo random identity there will always be a certain chance for collision between devices generated addresses. This problem has to be dealt with as long as the chance for collision exists and to make reasonable PRI specs we wanted to do such analyse. Procedure for identity collision handling has to exist when:

$\boldsymbol{\alpha > 0}$ Where number of devices within same network: $\boldsymbol{\kappa \geq 2}$

Where $\boldsymbol{\alpha}$ describes the probability for collision between two or more device-addresses within the same network, ($\boldsymbol{\kappa}$ describes the number of devices within range of each other).

We know that as long as two or more devices in the same network are generating pseudo random identity separately, the possibility for collision between the generated numbers is present and have to be handled. But the starting point should be good as possible, so the probability for collision is minimal without occupying to much address allocation to keep things simple.

We describe the probability for $\boldsymbol{\alpha}$ (collision) using η and κ, where η describes number of possible ID-address and κ describes number of devices within range.

It is possible to derive a formula describing collision probability between κ devices with η addressable possibilities:

$$\boldsymbol{\alpha} = 1 - \frac{n!}{(n-k)!n^k}$$

The alternatives for address fields we wanted to analyze are the range from 24 bits to 56 bits, which proportionally give 16.777.216 to 72.057.594.037.927.936 possibilities for the identity address. This is too large numbers for the computer to calculate when we involve faculty. We simply split up the formula and convert it to mathematical series:

$$\boldsymbol{\alpha} = 1 - \prod_{i=0}^{k} \frac{n-i}{n}$$

The numbers are now small enough to be computable, and could now be implemented in order to visualize the results. For our visualization we have used MATLAB.

The outcome of the curves is relative equal since the slope increase in a predictable way. However we show the graph separately since the differences is too big to collect in one single graph. X axis represents κ and Y axis represents α.

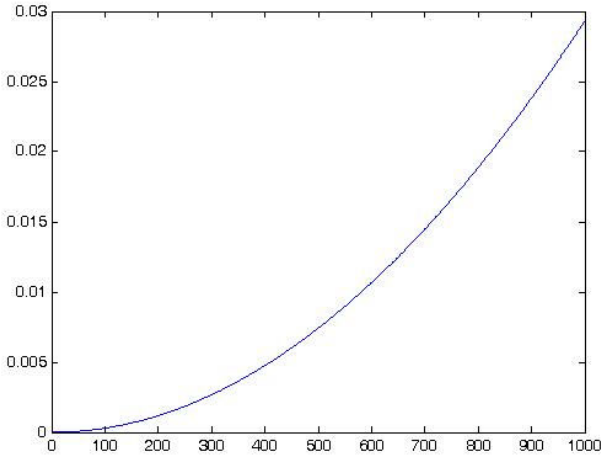

Figure 33: 24 bits address field

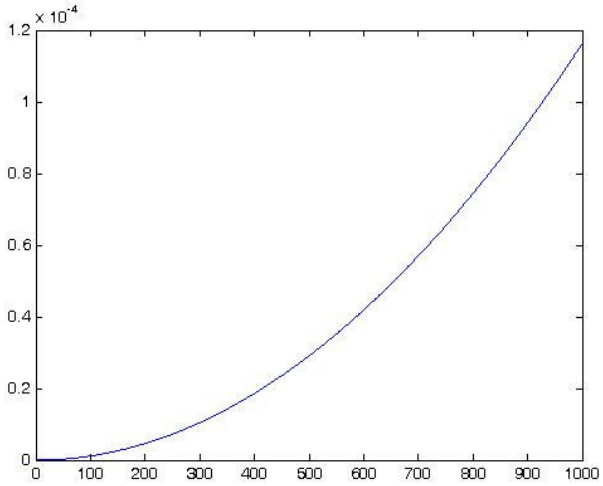

Figure 34: 32 bits address field

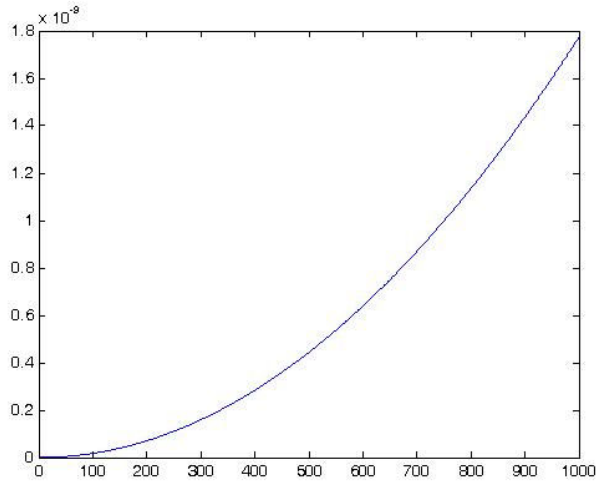

Figure 35: 48 bits address field

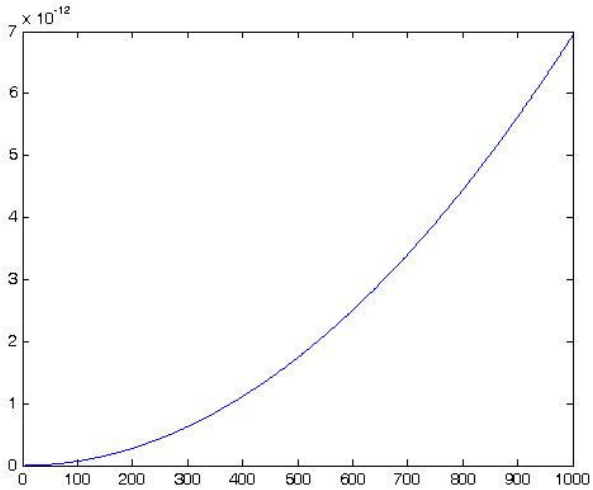

Figure 36: 56 bits address field

The graphs have pretty much the same trends, but not exactly. They have also very different values and are difficult to implement in the same graph. The possibility for identity collisions have to be handled as described in chapter 4 when $\alpha > 0$, but the routine should have as good basis as possible to reduce the possibility of collisions. Address field should be of a certain length, not only to avoid collision between devices identities, but also decrease probability for various devices generating identity's within a predictable range which e.g. could be caused by a "not-so-good" PRI algorithm. PRI Algorithm and address field decides how predictable the address could be and the probability for identity collisions. Since the PRI field also could allocate some of the bits to the PRI-filter as shown in chapter 4, one have to ensure a certain range for the identity range. Our recommendation is equal to or greater than 48 bits PRI field. Using 48 bits one can easily simulate the PRI field simply by spoofing the existing MAC address randomly.

6.2.2 Cryptography and usage

Since ad-hoc devices might be everything from small devices as cellular phones to bigger devices as laptops, various algorithms and procedures might make different load on different devices. Ad-hoc devices will often run on batteries, and the energy consumed might be critical and should not be wasted. Heavy load on the CPU will consume more energy, and according to security, some of the cryptographic algorithms are more optimized for such purpose then others. To state an example, we'll use some results from a research done by University of California and Sun Microsystems Laboratories [57] where they illustrate that the ECC-160 cryptography algorithm use much less energy then the more strong algorithm RSA-1024, due to both the amount of data sent and data computed. This is illustrated in Figure 37

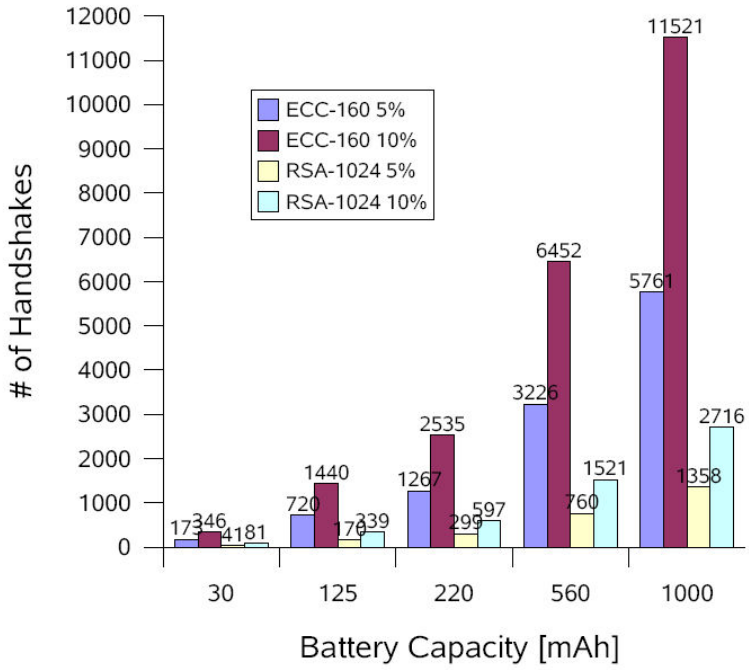

Figure 37: From Energy analysis project (source: [57])

"The computational benefits of ECC-160 over RSA-1024 are apparent, where the RSA-1024 computations consume 4.9 times the energy of ECC-160 computations. Compared to ECC-160, an RSA-1024 handshake also consumes 2.7 times the energy in transmitting and receiving data. Communication costs for RSA-1024 are higher because of the longer key sizes, thus making the certificates larger as well. With RSA-1024, the entire handshake requires the client to transmit 490 bytes of payload and the server to transmit 314 bytes of payload. With ECC-160, both parties transmit the same amount of payload data, 138 bytes." [57]

6.2.3 Privacy and trust survey

To get a point of view for our proposed solution and an overview for which of our steps that is more important for the end-users, we wanted to make a survey with a few simple questions which is indirect related to our proposed solution. We performed an anonymous survey and asked several questions. About 50 people took part in our survey, independent of age, education and sex.

Q1: Do you usually wear wireless items such as Cellular phone, PDA, Laptop etc?
We wanted to know if people usually carry around any kind of wireless equipment, and for who's who do what kind of equipment.

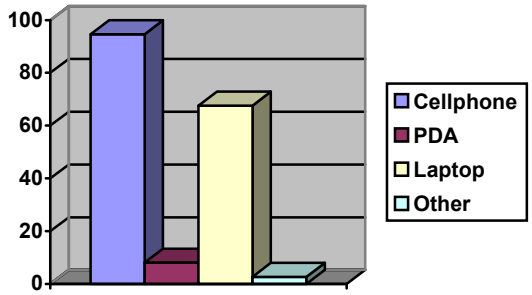

Figure 38: Survey about wireless personal devices

Everybody we asked wear some kind of wireless equipment, and 94.6% of them is using cellular phone. 67.6% of them use laptop and 8.1% usually wears PDA. Only 2.7% use other equipment. It seems like cellular phones and laptops are very popular, and they might operate wireless in several ways. Some people usually use several types of devices, and the need for security and privacy should therefore be presented.

Q2: How do you feel about today's constant increasing of electronic monitoring?
Monitoring people have many important aspects as rescue operations or busting the criminals etc. where one may find the source by tracking electronic devices. At the other side, this offends people's privacy. We wanted to know what people think of this case.

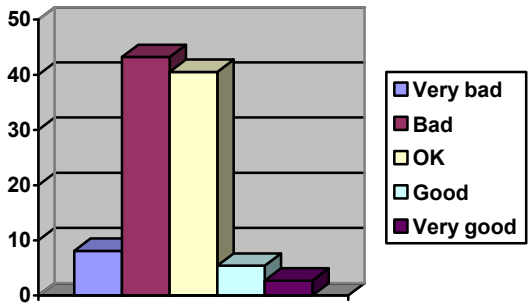

Figure 39: Survey about monitoring

8.1% doesn't like monitoring at all (very bad) and appreciate the anonymous existence. 43.2% think its bad, but still can see a few benefits. 40.5% thinks monitoring is fair, 5.4% think it is good that the society is being monitored, and 2.7% think it's very good.
It seems like people don't think it is too bad to be monitored, actually it has many benefits, but to utilize the benefits, ones privacy is injured. The balance says that people want to have a certain possibility to maintain anonymous.

Q3: Have you been exposed or experienced any kind of wireless abuse?
This question should give a hunt if anyone have done some kind of hacking in a wireless environment, or been a victim of hacking themselves, either for fun or malicious purposes.

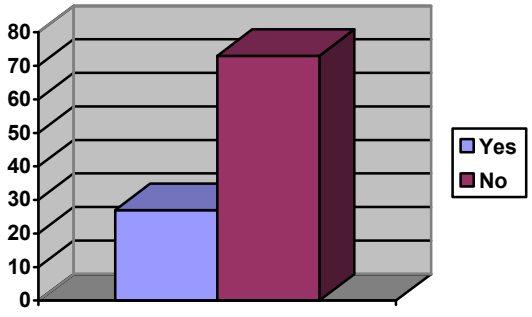

Figure 40: Survey about abuse

When we asked, 27% had actually abused security or privacy, or they had self been abused in some kind of wireless environments, while 73% had never been abused or tried to abuse any wireless weakness themselves. This gives us a pretty clear indication that

wireless networks have to be improved, either it as technical or about ease of use. (User-friendliness making people able to do correct setup)

Q4: How would you consider your trust to wireless networks if you should exchange some sensitive personal information?

If the person should send some important and secret information which is highly sensitive, we would like to know in which degree that person would trust privacy and security in a wireless network.

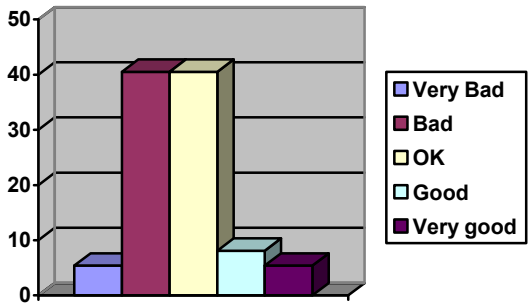

Figure 41: Survey about safety in wireless environments

As we see, 5.4% consider their trust to wireless network as very bad. 40.5% think it is bad and 40.5% think it's quite fair. 8.1% considers their trust as good, while 5.4% fully trust wireless environments. People's trust for wireless environments is not too bad, but the statistics tells us that they aren't quite comfortable with today's solutions.

Q5: Would you do any extra time-consuming effort while making or connecting a wireless network if you knew this would improve both security and privacy in your wireless communication?

If one have any kind of secret, sensitive or personal information which had to be exchanged in wireless environments, is it acceptable with a solution improving security and privacy if this cost extra time and effort to achieve.

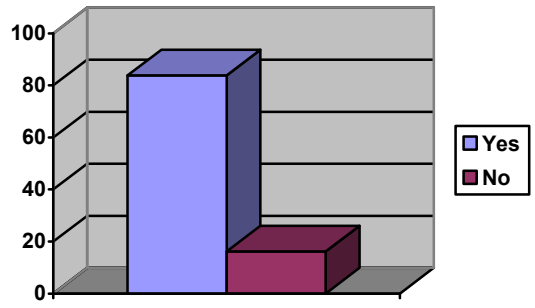

Figure 42: Survey about physical costs for security

83.8% are willing to spend some extra time and effort if this could help them establish better security and privacy for the wireless conversation, while 16.2% wouldn't. This shows us that most of the users are willing to execute heavier routines if this is required to do a safe conversation. However, to make things complex is not an aim.

Q6: If you had a possibility to establish a secure closed subgroup in a wireless network with multicast features (multi conversation), would you used such feature?

We wanted to know if end-users would use such a possibility to establish a secure multi conversation subgroup inside an existing wireless network. This could be used as closed conversation for data exchange in business meetings, or any other kind of groups.

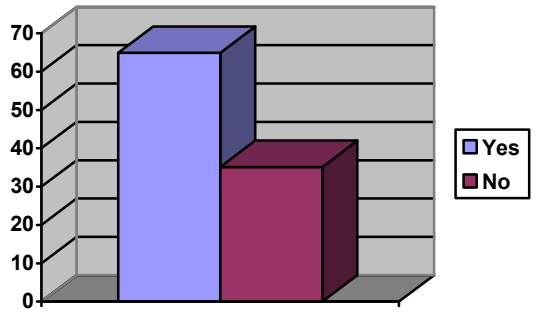

Figure 43: Survey about closed groups

This was just an opportunity that our solution brings up and is also described in chapter 5 as one-to-many scenario. 64. 9% think they would use such a feature, while 35.1% don't think they would. We think that almost 1/3 of the users indicate a good pointer, and we think probably more will use it when they see the advantages of such possibility.

7 Discussion and future work

7.1 Introduction

In this chapter we will take a closer look at the proposed solution which we presented in chapter 4 and chapter 5, and evaluate the result against the privacy and security requirements. Since this is a theoretical architecture we have not tested a prototype, and therefore the evaluation will be based on theory and the model we have developed.

In our general description of proposed model in chapter 4, we have made two major differences from traditional communication devices, the implementation of a PRI layer and active use of secure side channel in order to ensure security and privacy. These two techniques fit each other very good. The PRI ensures the anonymity and consequently part of the privacy while the secure side channel ensures trust, security and part of the privacy.

7.2 Solution properties

One very important aspect about communicating is trust, especially for wireless communication. It doesn't matter how secure the communication channel is as long as one can't trust the remote part. Normally, either it is a network with or without infrastructure it's hard to actually know for sure who you are communicating with. Most of the cases you can't be sure and this could compromise system security.

Using a secure side channel to exchange initial data such as cryptography keys, node address (PRI) and identity solves this problem because one actually have to physical encounter the person or device you are going to do a secure communication with. Our routines also verify that the user actually gave away the right key. In this way one doesn't have to exchange any critical data on the air, and one knows for sure who one are going to communicate with. To physical encounter devices you are going to communicate securely with might be bothersome, especial if one is going to do secure communication with many nodes. One can of course establish secure communication over the air without facing current device by using chain of trust as described in chapter 5 in order to decrease amount of effort used to establish such secure channel. However, the first devices that are going to communicate securely have to initialize via secure side channel before going on the air, which means extra effort needed by the end-users. In our survey in chapter 6 we asked the people if they where willing to do some extra effort to make sure that the communication

channel would be safe. 83, 8% of them would do so, while 16, 2% would not. This method is also necessary in order to trust another device using the PRI layer as identification. One has to establish trust quite often since the PRI layer ensures total anonymity. This is also why PRI suit so perfectly together with the secure side channel.

The cryptography which makes the information flow secure and prevent others from understands the content ensures important parts of the privacy. Our solution is pretty much a general solution, which means that several cryptographic techniques may be used in the system. However, there are some limitations to consider. Not every cryptographic algorithm is actually working at every device due to several reasons. Some of the cryptographic algorithms are also too heavy for certain devices considering both battery capacity and available processor usage.

An analysis done by the University of California and Sun Microsystems Laboratories [57] shows an example (in chapter 6) where one can see the big differences in usage when using different cryptography algorithms. The example stated shows that the RSA-1024 consumes approximately 4.9 times the usage of ECC-160. High CPU usage consumes much battery capacity. Cellular phones, some PDA's and other smaller devices should use lighter cryptography algorithms, while bigger devices as laptops, powerful PDA's etc. could make use of more heavy algorithms if required. For smaller devices it is sometimes impossible to implement certain cryptographic algorithms due to the hardware limitations. Public key cryptography usually require heavy mathematical calculations to generate a pair of keys since the public key and the private key is mathematically related to each other, and such calculations is quite heavy, especial for large keys. However, cryptography generally is a good option to avoid attackers to eavesdrop ones conversation in order to maintain the user's privacy and security and is probably the most used technique to secure communications channels.

The PRI layer is primary set up to ensure the users anonymity in order to avoid tracking and maintain user's privacy. The end-user should have the possibility to stay anonymous whenever he or she wants, simply by generating a new pseudo random identity. This will ensure anonymity and make all tracks left behind useless. This introduces a new series of problems. Using PRI as identity, one can never trust other devices for more than one session, and every grouping of other nodes can just be considered as temporary

categorization and this result in that the secure side channel is being the main fundament to establish trusted connections every time, which might seem to be a bit bothersome. As mentioned before, trust and anonymity is two issues which constitute the opposite of each other, and are therefore difficult to solve both issues perfectly. Our result is a workaround which makes us able to solve both issues, but unfortunately the solution requires some more effort from the users then with the traditional systems. Sometimes there is no need to do secure, trusted and anonymous communication, and if so one don't need to do any of these procedures. Our model supports both cases.

7.3 Security and privacy evaluation

Our goal was to propose a solution framework which improves security and privacy for wireless ad-hoc networks. The security and privacy was derived, as a result we have four points, which is trust, security, privacy and anonymity. These points are integrated in the security and privacy aspect.

We initialize communication through a secure side channel which makes us able to authenticate the communication partner due to physical encounter. The necessary information is exchanged trough this side channel and makes us able to directly start an encrypted conversation on the air. This ensures that no one is immediately able to perform eavesdropping or manipulates data routed without discovering such attack. As described in chapter 1, the required criteria defined for security is fulfilled.

Trust is, in our solution, a continuous considering and is no absolute. This is caused by the PRI technology which makes every compatibility device able to change identification whenever necessary. The authentication through the secure side channel will establish trust. The exceptions could be public info beacons, where one e.g. is driving a car as a tourist and receive some information while passing trough an info-beacon. A device could easily change the PRI's filter value and identify itself as an info-beacon. Without any real authentication one should consider the received information, and make a decision if one should trust the information or not. All in all, trust is established most of the cases, but if the communication channel operates non-secured one might in some cases have trouble trusting certain devices.

Using the PRI layer in order to identify a node one has the possibility to change identity whenever necessary. This ensures users anonymity and tracks left behind are useless to compromise a nodes privacy, because one can not identify owner of the track. This fulfills

the definition of anonymous in chapter 1. Unfortunately, achieving such benefit cause active use of secure side channel to establish security and privacy. A weakness is that one often has to meet the communication partner physically, which actually keeps anonymity at the technical level, but compromise anonymity at the physical level.

The combination of secure communication channel and active use of PRI layer ensures that personal or sensitive information is not given away to other then those whom one choose to give this information, both information in the conversation and other information which might leave tracks behind. This should fulfill the need of privacy.

All in all, our proposed solution have improved the security and privacy aspects in wireless ad-hoc network, and solutions fits pretty well together, but unfortunately this will cause user-friendliness probably are made worse.

7.4 Further work

Since this thesis has become a theoretical architecture development there is no prototype made. The first thing to do should be to implement a formal model which could be used to eliminate logical errors and do the fine adjustments. SDL or Promela should be well suited methods for such purpose.

A formal model for the proposed solution should consist of typical ad-hoc properties in additional to the PRI layer and the secure side channel. After making sure that devices are able to exchange information with each other as proposed and the PRI works as supposed etc. one might start the “serious” testing. Security and privacy is the vital parts, and by attacking such model with logical expressions (e.g. in Promela) one could be able to discover and solve security or privacy weaknesses. With such formal model one might be able to “attack” the proposed framework in several ways. The use of formal methods is an efficient way of testing abstract system-models for eliminating critical bugs, errors and weaknesses, but it takes a lot of time.

Further, a simulator or a model at a lower level could be made in order to evaluate the performance aspects, and maybe optimize if possible.

8 Conclusion

After studying several related projects, algorithms and techniques we have seen that there are many technologies which could be used in many ways. Due to the limitations of this project, available ways of making improvements has decreased. While developing solutions we have tried to stick to the motto: “Simple is better” and as a result the principle of the solution has become simple, but implementation in certain ways and systems could be quite complex. However, we think the principle of secure side channel combined with the pseudo random generated identity (PRI) gives us many advantages and new ways of thinking, though at a pure technical level and it seems like security and privacy is improved. Unfortunately, one of the biggest advantages with our solution also approaches to be a disadvantage. The level for physical existence (user-friendliness) has not improved. The proposed system architecture at this point require the end-user to actually physical encounter the remote device in order to establish a secure connection initialized by secure side channel, which could be bothersome to do too many times. Chain of trust will of course make this process a bit easier. Further, one could stay technically anonymous (PRI identity), but as long as it is no automatic device one encounter, one probably have to meet the owner of the remote device, which will compromise some of the anonymity aspects in the real life (physical level). Generally spoken, the proposed solution should be able to enforce user’s privacy and security, but there is still long way to go in order to achieve acceptable user-friendliness. This solution is quite realistic to implement into today’s devices, since most of devices have built-in infrared transceiver. There exist no device with such thing as PRI layer, but one could easily simulate a 48 bits PRI layer simply by spoofing the MAC address when needed. This thesis has proposed use of solution in a given number of scenarios, but in real life one have to consider far more situations in order to be able to handle and secure all kinds of events. Also user-friendliness has to improve since people probably would not make use of solutions if they are too bothersome.

9 References

[1] http://ikt.hia.no/aml/public-projects/2005-ONE/2005-ONE-public.html

[2] Frode Sørensen: ”Moderne IP-nett” ISBN:82-7772-279-6. Norge Books A/S – 2004

[3] Chris Brenton, Cameron Hunt: ”Active Defence” ISBN: 0-7821-2916. SYBEX Inc. 2001

[4] Mencer, O. Morf, M. Flynn, M.J.:”Hardware software tri-design of encryption for mobile communication units” Dept. of Electr. Eng., Stanford Univ., CA. ISBN: 0-7803-4428-6. 1998

[5] http://en.wikipedia.org/wiki/Privacy

[6] http://en.wikipedia.org/wiki/Trust_%28sociology%29

[7] http://en.wikipedia.org/wiki/Anonymity

[8] Pahlavan, Kaveh: “Principles of wireless networks: a unified approach” ISBN: 0130930032. Prentice Hall PTR; 1st edition (December 11, 2001)

[9] P.Nicopolitidis, M.S. Obaidat, G.I. Papadimitriou and A.S. Pomportsis. “Wireless Networks”, Wiley 2003

[10] http://en.wikipedia.org/wiki/Wireless_network

[11] http://en.wikipedia.org/wiki/WWAN

[12] http://en.wikipedia.org/wiki/WLAN

[13] http://www.intel.com/technology/comms/uwb/download/Ultra-Wideband.pdf

[14] Charles E. Perkins, Charles Perkins:”Ad Hoc Networking” ISBN: 0201309769. Addison-Wesley Professional; 1st edition (December 29, 2000)

[15] Dr. H. Al-Raweshidy, “Ad-hoc Network”, http://www.brunel.ac.uk/about/acad/sed/sedres/nmc/wncg/security/adhoc/ , Brunel University London

[16] http://en.wikipedia.org/wiki/Bluetooth

[17] http://en.wikipedia.org/wiki/802.11

[18] Jochen H. Schiller: “Mobile Communications” Second Edition. ISBN: 0-321-12381-6. Pearson Education Limited – 2003

[19] http://en.wikipedia.org/wiki/Infrared_Data_Association

[20] http://www.usb.org/developers/wusb/

[21] L. Zhou and Z.J. Haas, “Securing Ad hoc Networks”, IEEE Networks

[22] Jason I. Hong, Jennifer D. Ng, Scott Lederer and James A. Landay: "Privacy Risk Models for Designing Privacy-Sensitive Ubiquitous Computing Systems" , ACM, 2004

[23] Sunny Consolvo, Ian E. Smith, Tara Matthews, Anthony LaMarca, Jason Tabert, and Pauline Powledge.: "Location Disclosure to Social Relations: Why, When, & What People Want to Share" ACM, 2005

[24] http://en.wikipedia.org/wiki/Data_privacy

[25] *P. Vinayakray-Jani,"* Security within Ad hoc Networks*"* Nokia Research Center, Helsinki, Finland

[26] http://en.wikipedia.org/wiki/Data_integrity

[27] Diamadi, Z. Fischer, M.J.: A simple game for the study of trust in distributed systems. International Software Engineering Symposium 2001

[28] Warne, D., Holland, C.P. Exploring trust in flexible working using a new model. BT Technology Journal, vol.17, no.1, p.111-19. Jan 1999

[29] Zheng Yan, Peng Zhang, Teemupekka Virtanen: "Trust Evaluation Based Security Solution in Ad Hoc Networks". Nokia Research Center, Nokia Group, Helsinki, Finland.

[30] Perlman, R.:"An overview of PKI trust models" IEEE Network, vol.13, no.6 p.38-4

[31] Daniel W. Manchala, Xerox Research and Technology: E-Commerce Trust Metrics and Models. IEEE Internet Computing, vol.4, no.2 p.36-44, 2000

[32] http://en.wikipedia.org/wiki/Anonymity

[33] Matt Bishop: "Computer Security – Art and Science" ISBN: 0-201-44099-7. Pearson Education, Inc. – 2003

[34] http://en.wikipedia.org/wiki/Public-key_cryptography

[35] http://en.wikipedia.org/wiki/Symmetric_key_algorithmsymmetic

[36] Dr. H. Al-Raweshidy, "Ad-hoc Network", http://www.brunel.ac.uk/about/acad/sed/sedres/nmc/wncg/security/adhoc/ , Brunel University London

[37] http://en.wikipedia.org/wiki/Denial-of-service_attack

[38] http://www.caci.com/business/ia/threats.html

[39] http://en.wikipedia.org/wiki/Replay_attack

[40] Florina Almenarez, Andres Marın, Celeste Campo, Carlos Garcıa R.: PTM: A Pervasive Trust Management Model for Dynamic Open Environments,

http://www.it.uc3m.es/pervasive , Dept. Telematic Engineering, Carlos III University of Madrid, Spain

[41] Zimmermann, P.R.: The Official PGP User's Guide. MIT Press, USA

[42] F. Stajano and R. Anderson: "The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks". Computer Science, 1999

[43] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang: "Providing robust and ubiquitous security support for mobile ad hoc networks", 2001.

[44] http://en.wikipedia.org/wiki/Secret_sharing

[45] Srdjan Capkun, Jean-Pierre Hubaux, and Levente Buttyan, "Mobility Helps Security in Ad Hoc Networks," Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing, pp. 46 - 56, ACM, 2003.

[46] J. Douceur: The Sybil attack, 2002

[47] F. R. Schreiber, Sybil, Warner Books, 1973

[48] N. Asokan and P. Ginzboorg: "Key agreement in ad hoc networks" Computer Communications, Pages 1627-1637

[49] Bennet & McRobb.: The Waterfall development phase model: , 2002

[50] http://www.imc.org/pdi/

[51] http://en.wikipedia.org/wiki/Pseudorandom_number_generator

[52] Brent R. Waters Edward W. Felten Amit Sahai.: "Receiver Anonymity via Incomparable Public Keys", Department of Computer Science, Princeton University

[53] Patrick J. Megowan, David W. Suvak, Charles D. Knutson. "IrDA Infrared Communications: An Overview" Counterpoint Systems Foundry, Inc

[54] www.intel.com/technology/ultrawideband/downloads/wirelessUSB.pdf

[55] Patrick J, II Sweeney.:"RFID For Dummies" ISBN: 076457910X, For Dummies (April 1, 2005)

[56] www.rfidjournal.com

[57] Arvinderpal S. Wander Nils Gura, Hans Eberle, Vipul Gupta, Sheueling Chang Shantz. "Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks" University of California, Santa Cruz Sun Microsystems Laboratories.

[58] http://www.zeroconf.org/

[59] http://www.cs.umbc.edu/CSEE/index.html

[60] Asad Amir Pirzada and Chris McDonald.: "Establishing Trust In Pure Ad-hoc Networks" School of Computer Science & Software Engineering, The University of Western Australia

Appendix A

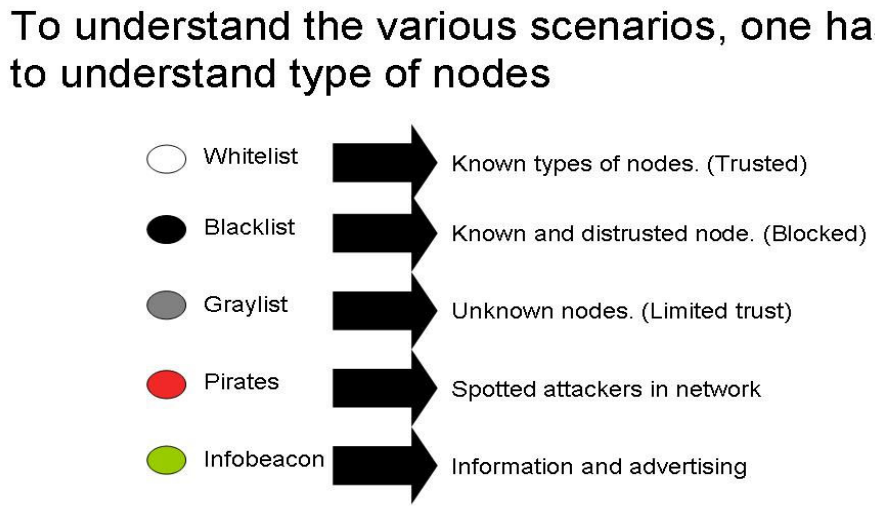

Figure 44: Type of nodes

The requirements for security and privacy might vary for various situations since the environments might change caused to the independent network structure (various scenarios). We will examine the various requirements and practical needs for several scenarios to map the most essential problems which are considered to be the most default environment situations for pure ad-hoc network. Our chosen scenarios are graphically illustrated in appendix A.

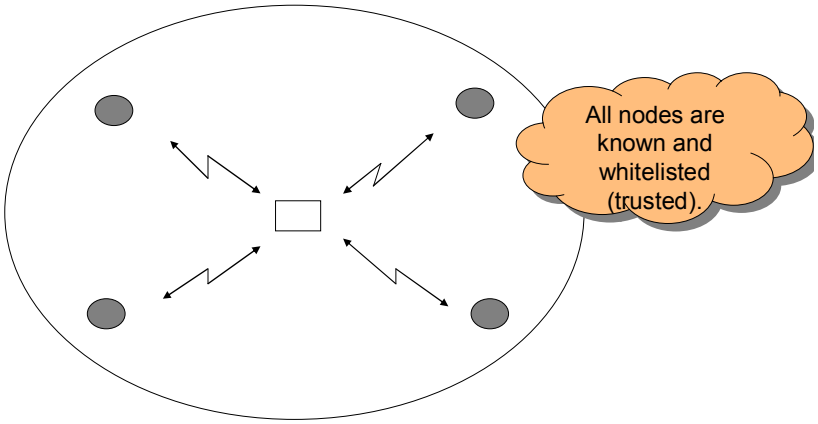

Figure 45: Ideal scenario

Description: Figure 45 shown an ideal scenario where every single node in the network trusts each other. They are in an isolated network, which means no one is neither joining nor leaving the network. This could be in some what of isolated place where the persons owning the nodes know for sure that no one is able to even get near the range of covering.

Problem: This is the ideal scenario, and there is actually no specific problem. For such ideal scenario one probably don't need encryption at all, though, if all the parts have an open relationship and no secrets for each other. If everybody follows the rules, communicating should be done without any problems. We assume that friends don't act as malicious nodes. For this scenario we do not consider how they established trust to each others.

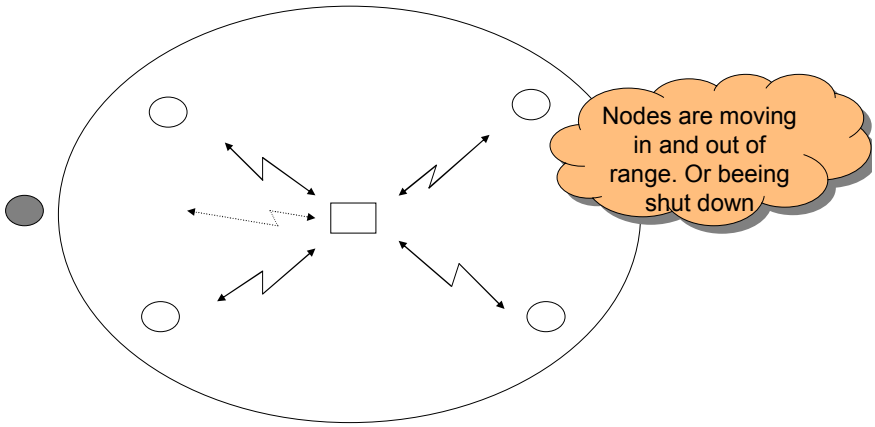

Figure 46: Practical scenario I

Description: Figure 46 show a scenario describes very usual environments. In difference from the previous scenario, this network is not isolated, and nodes are able to join and leave the network. Nodes can be shut off (run out of battery) or turned on within covering range. This could be a situation where a group of friends (trusted) establish a network, but there are other people walking by, or maybe others network is nearby in the same area. (For example public rooms, office buildings, airports, cafés etc.)

Problem: When a node are showing up and disappears continuously, you probably don't know everyone in the network, maybe two network which in principle was two separated network is joined together because of two groups too close to each other. People with other devices are walking by and so on. One probably wants to separate the networks, and some of the nodes might want to establish secure connections caused to required sensitive data exchange. Keys need to be exchanged between correct devices, and there is no guarantee that there are no malicious nodes somewhere in this network.

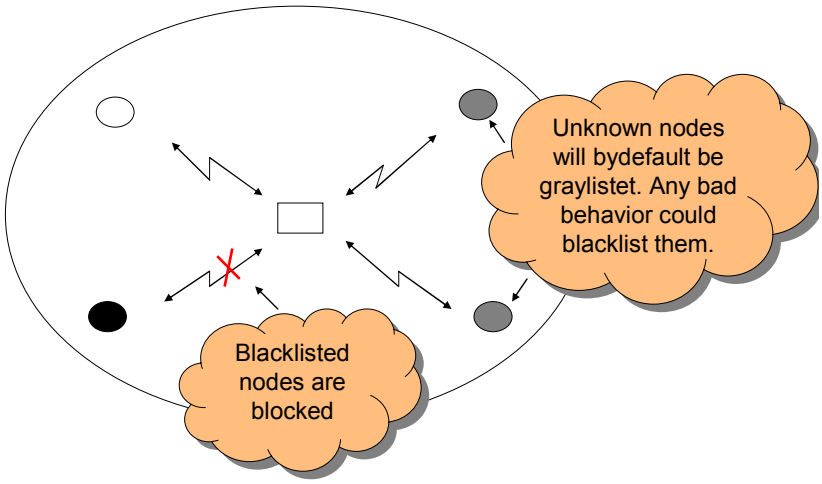

Figure 47: Practical scenario II

Description: Figure 47 shows a scenario is a bit more complex then the previous ones. Two of the nodes within covering range is unknown nodes, the third node is a trusted node, while the forth node is a node which have done some suspicious behaviors and therefore it's a mistrust situation between our node and the forth node. It could be a pirate, or just a buggy device. Anyway, one has decided to blacklist the suspicious node. As for the previous scenario, this could for example be in public rooms, office buildings, airports, cafés etc.

Problem: When a node is mistrusted, it has to be caused by some kind of bad behavior which made you decide to move the node from grey list or white list to blacklist. It might not be easy to detect such suspicious behavior. Other nodes which are in the area might also be in "danger" with such node(s) nearby. One also knows that an attack isn't always done by a single node. Such situation might be critical.

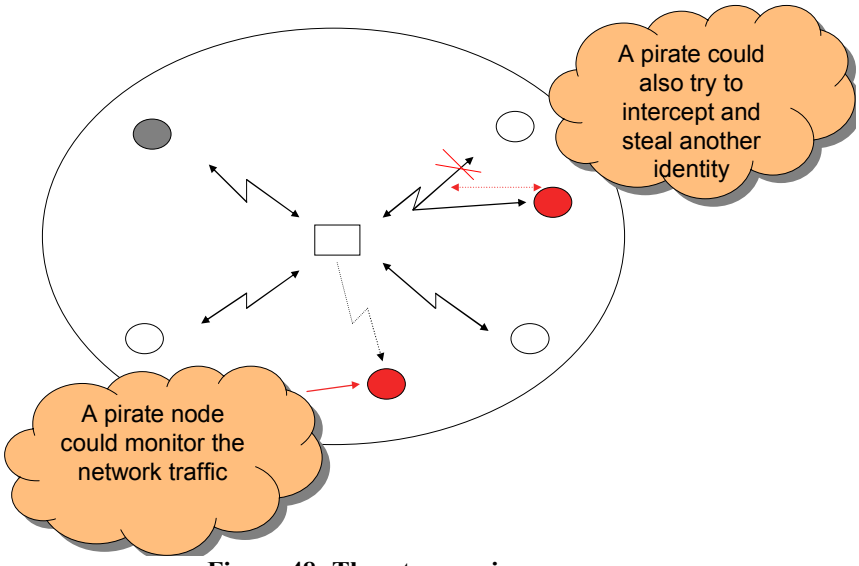

Figure 48: Threat scenario

Description: Figure 48 show a scenario that includes three trusted nodes, one unknown node and two pirates. One of the pirates is a passive attacker, which means it isn't doing anything activity to do the attack, but is simply just listening on the air, trying to receive some useful information. The other is an active attacker, which means it does something active to make his attack, which in this case is to steal another nodes identity or address trying to takeover the information flow. This could typically happen in small areas with many unknown and different people, and maybe where there is a lot of important information exchange.

Problem: Often one will not notice the passive attacker at all, but if one should discover him or her, it could be dangerous to exclude that node from the network, because it could be a critical link which binds two groups together and is therefore an important router for way of traffic. Simultaneous, one doesn't want anyone else, and especially not pirates, to monitor ones information sent trough the network.

The active attacker, which is trying to steal another nodes identity or address, might also cause problems since probably both of the devices will receive the information. One could probably not blacklist it either, because you will also blacklist your friend too at the same identity or address. It might be really hard to separate them from each other.

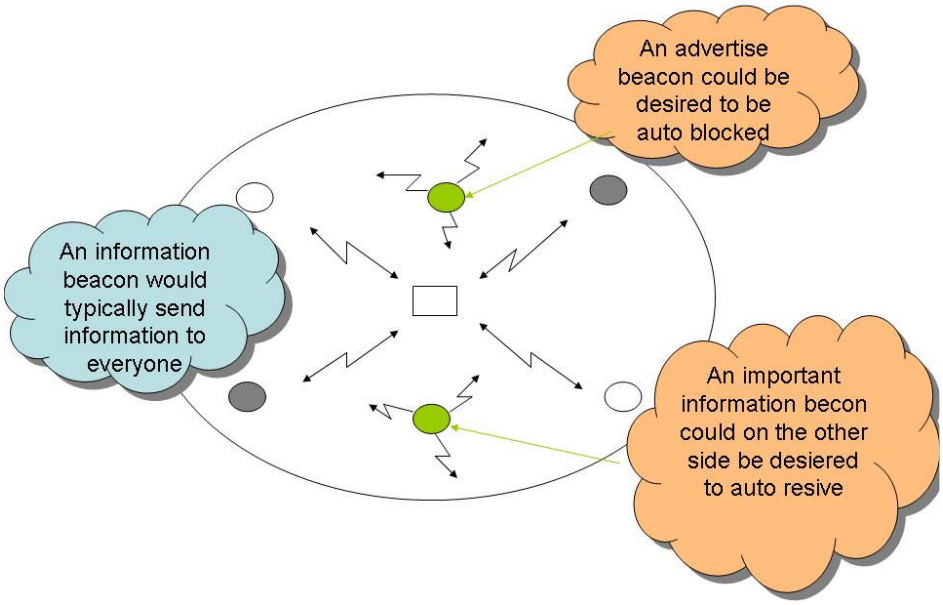

Figure 49: Information / Adverticement beacon scenario

Description: Figure 49 show an information scenario which is pretty ideal for pedestrian shopping streets etc. We got several info beacons which are sending advertisements or information to the bypassing nodes. This could be a big business as commercials in future, information for tourists etc. Typically one move from one place to another while passes by several information beacons which is trying to get your attention in some way or another. Info beacons will often be equipment for public use, and should therefore not be considered as malicious nodes in the first place.

Problem: With such system, one probably wants to block information that is sent from some of the public beacons to avoid getting spammed. A question is which beacons should be blocked, and when. How could one tell the difference between the various beacons? However, there should be some possibility to filter the information flow.
When moving trough several beacons, one will usually leave lots of digital tracks behind, such as MAC-address etc. Since the info beacons most likely is static equipment, (non-mobile devices) it could be pretty easy to track down a person's movement with such information at every beacon, since such information is unique for each device.

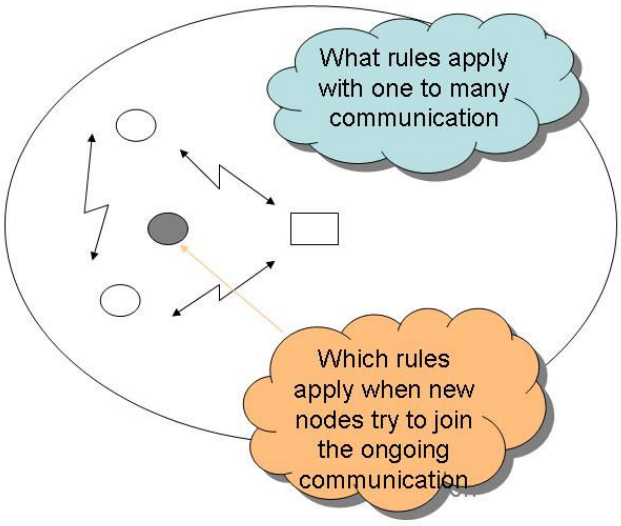

Figure 50: One-to-many scenario

Description: Figure 50 show a one-to-many scenario. Some people might require establishing a secure and closed channel between themselves where one of them is supposed to multicast information to the others, which means a one-to-many communication. Typically scenario where there are many people communicating, and a tiny group has established a closed communication just for them and one of the users have (probably) some important information to share with everyone in that tiny group. This could also be a scenario which not requires any secure communication, but simply wants to do a multicast of some non-sensitive information or data.

Problem: In multicast conversations where every device should spread their information to the rest of the group, information will flow in certain ways trough the network and one have to deal with the closed group only. Especially when the group is secured, there might be many factors to consider. When nodes are joining or leaving the group, they have to be able to involve or quit the conversation on the fly. Establishing of trust in such multicast environment might be bothersome, hard and might also be time-consuming what network establishment consider.

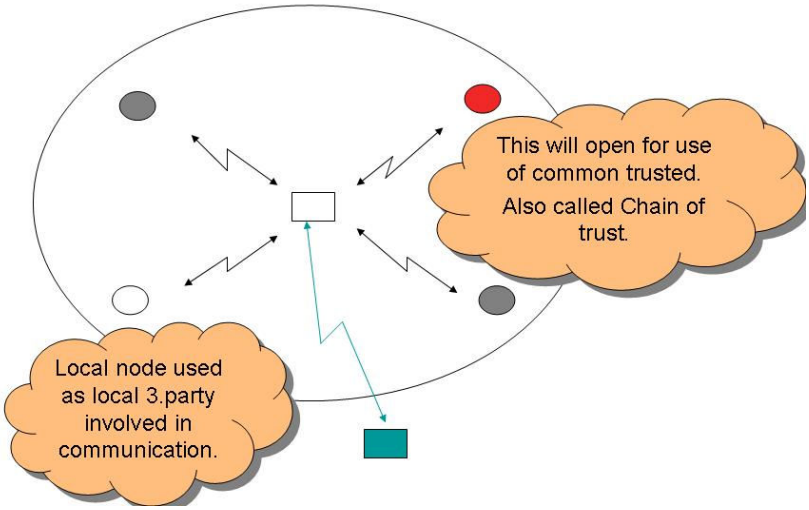

Figure 51: Local TTP as Chain of trust

Description: Figure 51 shows a local TTP scenario as "Chain of trust". Ad-hoc is in principle meant for establishing of network without possibilities for any fixed infrastructure, independent of any third party nodes or applications and has the possibility to totally organize itself. But in this scenario, the nodes are under coverage of another network, which could be just a local Access point (AP), maybe with connection to internet, or the nodes could be in coverage of a global network. (For ex. the GSM network) When an Ad-hoc network is established in coverage, one could make use of the resources available to make the network as good as possible. One trusted node, two unknown nodes and one pirate is represented in this scenario. To verify nodes, one might have the possibility to so thorough the third part. This could be certificate checks or similar. This might have several opportunities, and probably enforce the security in the system.

Problem: We would not always be able to find a superior network covering the established Ad-hoc network, and if so, the trusted third part (TTP) possibilities could not be used. The trusted third part (TTP) also has to know something unique about every device so it could be able to recognize devices when nodes want to verify a possible connection destination (another node within coverage of the TTP). One often want to be anonymous, but how to verify the others? One also has to establish a secure connection when communicating with the TTP so no sensitive data could leak in the ad-hoc network. It is important to emphasize that we have no guarantee that there are no malicious nodes nearby.

Appendix B

Since the original formula derived require extremely large numbers we had to rephrasing the mathematical formula in order to be able to compute without crashing the computer.

The original formula could be expressed as:

$$\boldsymbol{\alpha} = 1 - \prod_{i=0}^{k} \frac{n-i}{n}$$

Where $\boldsymbol{\alpha}$ represent the probability for collisions for K devices in the very same network where each device has N bits PRI field available to address their identity.

The MATLAB code became pretty simple:

```
clear all;
k = [1:1:5000];          // Calculate a continuous graph up to 5000 devices within the same network
n= 2^48;                 // Actual device operates with 48 bits for current calculation.
x = zeros(1,length(k));
for kk=1:length(k)       // Loop in loop in order to multiply the particular results given in the formula.
   sum=1;
   for i=1:k(kk)
      sum=sum*(n-i+1)/n;
   end
   x(kk)=sum;
end
plot(k,1-x);             // Plot the value
hold on
```