Two Methods of Authenticated Positioning

Thomas Mundt
University of Rostock
Institute of Computer Science
Chair for Information and Communication Services
e-mail: thm@informatik.uni-rostock.de

ABSTRACT

Recent studies and publications have shown a demand for a secure method to proof someones or somenthings position via a communication channel. In this paper we present a concept and two architectures for location dependent access control. We start with a number of scenarios. Some of the scenarios play in a global context, some others in a more local environment. We address boths groups of scenarios with different methods of positioning (location providers). We are using a WLAN mesh network to determine the nodes' positions. We introduce a trustworthy hardware module used for positioning and controlling access to secured data. We show different types of attacks against such systems. Due to the special nature of different location providers we compare several ways how these attacks are impeded.

Categories and Subject Descriptors

D.4.6 [**Software**]: Operating Systems—*Security and Protection*; C.2.1 [**Computer Systems Organization**]: Computer-communication Networks—*Wireless communication*; K.6.5 [**Computing Milieux**]: Management of Computing and Information Systems—*Authentication*

General Terms

Algorithms, Measurement, Performance

Keywords

WLAN Positioning, Context / Location Awareness, Mesh Networks, MANETs, DRM, Authentication

1. INTRODUCTION

Access control systems as described in this paper have an eligibility when interlectual property is to be protected. Usually this protection is realized by binding digital material to a certain ressource - such as a memory card or music player - a certain person, a certain computer, or a certain context. Somethings location is part of its context. There is an obvious need for a system that grants access to protected data at certain places only.

The idea of authenticated positioning was driven by a series of scenarios that circulated in the media during the last 2 years:

- A company wants to assure that confidental material remains within the company.
- An Oscar ™nominated movie shall be viewable at the Academy juror's home only.
- TV shows or DVDs shall be limited to a single country.
- The lock of an amored car should open only near the bank.
- A harddisc containing confidental material should be accessable (decryptable) only when inside the a determined area.

Some of these scenarios require position methods in the area of many square kilometers, other scenarios play in a more local environment. Therefore, we have used different location providers and adapted the authentication mechanism to these positioning systems. The first solution was based on satellite navigation systems and hence more suitable for a wider outdoor area. The second solution uses our own positioning method which facilitates an ad hoc Wireless LAN or mesh network. A detailed description of our satellite based solution can be found in [12].

For short range positioning and especially for indoor use we are utilizing a location provider that determines distances by measuring the electric field intensity of neaboring nodes. Because in most cases there are obstacles absorbing energy, we have to process data before finally calculating each node's position. In our concrete implementation we are using off-the-shelf WLAN hardware.

The main component of our system - independent of the location provider being used - is a hardware module which is protected against manipulation. This module is responsible for positioning and detection of any possible frauds. We will show that re-routing is the most promising way of attack. Hence, the module contains a precise and trustworthy time source. We will later explain re-routing and other possible attacks and why a trustworthy clock is needed. The module is also responsible for granting access to the protected digital material or to generate an unlock signal in other scenarios. Such a module has to be implemented in hardware in order

Q2SWinet'06, October 2, 2006, Torremolinos, Malaga, Spain.

to harden it against re-engineering or manipulation. Just like modules used in Digital Rights Management systems our module could be integrated in a variety of devices such as:

- TV sets, settop boxes, or satellite receivers.
- Devices used for displaying data, such as notebook computers.
- Storage devices, such as hard discs.

Both presented methods of authenticated positioning use plausibility checks to ensure that received signals have not been manipulated, for instance by receiving signals within the approved area and retransmitting it to a spoofing device outside. We will explain this in theory and on a prototypical implementation. Several tests have been performed. We will give further details in the following texts as follows: Section 2 illustrates threats and attacks against the proposed system, section 3 explains the state of the art and technologies necessary for the realization of our concept. Section 4 describes two methods of authenticated positiong conceptionally. We will develop these concepts into a prototype and test bed in section 5. Inthis section we also discuss advantages and limitions. Section 6 concludes this article and directs into further developments.

2. SECURITY THREATS AND ATTACKS

The simpliest way of authenticated positiong would be a proximity sensor which detects when another device with fixed position is withing range of any kind of transmission, such as infrared light or ultrasound. Two types of attacks are obviously suitable to cheat such a device in the process of determining its position. Most likely are re-routing attacks. These are performed by placing a receiver within the approved area and distributing its signal to illegible devices outside the approved area as shown in figure 1. Apparently the only effective method to perceive such re-routing attacks is detecting the time delay caused by the distance between the spoofing receiver inside the approved area and the remote device. The latency will increase by some time in the range of milliseconds. Measuring round trip times is very easy. But how to detect re-routing without having a return channel, which is for instance the case with satellite navigation systems as location providers? We are using a very stable time source and a secured mechanism of its synchronization with a trustworthy external clock. Section 4 will provide a more detailed answer to this question.

Longer delays will be caused by recording and replaying the signals at another location used to determine the position. Countermeasures against this `replay attack` are the same as those used against re-routing.

Re-routing can be performed on several layers of the signal processing chain. A re-routing of the entire spectrum which the sensor is perceptive to is conceivable - although causing some engineering problems. Easier are re-routing attacks on the digital layer, meaning forwarding bits and bytes and retransmitting a signal that is equivalent to the one originally received.

Other attacks concern the cryptographic sub-system. Those attacks are out of scope and will not be discussed in this paper as they are a general problem of cryptography.

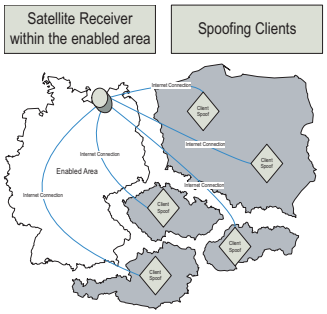

Figure 1: Principle of re-routing.

Both location providers discussed in this paper use wireless signals. Those signals are subject to denial-of-service attacks by jamming selected frequencies or a larger spectrum. Those attacks will lead to false rejects. There will be no false accepts caused by DoS attacks.

3. TECHNOLOGICAL BASIS

3.1 Authenticated positioning

In "An authenticated Camera" [9] Kelsey, Schneier and Hall discuss how a picture taken with a camera can be saved with an authenticated position information. They explain possible attacks and introduce "re-routing". In their examples they use GPS signals which are being forwarded. They conclude that this kind of attack is hard to prevent. An article "GPS Spoofing Countermeasures" [23] gives a general overview about methods to secure GPS against spoofing attacks. To the best of our knowledge there exists no practical working system for authenticated positioning. The inventor holding US patent 5,922,073 [19] ("System and method for controlling access to subject data using location data associated with the subject data and a requesting device") claims to have a solution for the problem described in this paper. A description his solution is not given in the patent. It contains only a vague description of the principles.

3.2 Access control

In order to understand how a position information can be used as input of an access control system - we will not use the term *Digital Rights Management* (DRM) for our concept because it is slightly misleading - we give a brief introduction. One of our sample scenarios requires TV shows to be limited to certain reception areas. DRM enables "owners" of interlectual property to control the circumstances under which users can access documents [3]. Possible types of access are for instance *Read, Write, and Change*. A wide variety of possible payment options is implementable, such as *pay-per-view, pay-per-copy, or pay-per-instance*. A more comprehensive introduction of DRM can be found in [22]. Digital material is protected through cryptographic methods such as encryption, watermarking or signatures.

A simple form of Access Control is used for encrypted satellite TV broadcasts. A non-public section of the Digital Video Broadcast (DVB) [15] standard defines a scrambling and encryption mechanism which prevents unauthorized persons from watching the protected broadcast. The standard calls this Conditional Access (CA). The TV station uses a Subscriber Management System (SMS) to grant

access for registered paying viewers. This is realized by sending an Entitlement Management Message (EMM) to the receiver. An Entitlement Control Message (ECM) which is also being sent is used to decrypt the Control Word (CW) necessary to descramble the digital content. The actual cryptographic process is realized in a smart card. The smart card is unique for each customer. Its inputs are ECM and EMM and its output is the CW. The standard does not define the concrete implementation of the cipher algorithm. Frequently used systems are SECA, Irdeto, and VIACRYPT [15]. Decryption is implemented on the smart card, descrambling runs on the receiver.

3.3 Location providers

3.3.1 Satellite based navigation

Most of the scenarios backing our ideas are playing in larger areas such as countries or cities where the content should be enabled. For this purpose a regional location system would be insufficient. We concentrate on satellite based location providers. For our purpose it does not matter whether the US operated GPS or the announced European Galileo [14] will be used. Most of the features are identical. Galileo is the new European global navigation satellite system. Its orbital component comprises of up to 40 satellites. GPS uses up to 32 satellites. The satellites are equipped with highly precise clocks. The time signal and signals describing the ephemeris (trajectory parameters) are constantly transmitted. A portable unit receives the signal and computes its position by using the time difference of signal arrival and the information about the satellites position.

For our purposes we have to assure that the satellite signal is authentic by itself. Basically signals have to be digitally signed. Galileo provides several service levels [20, 4]. These are "Open Service" (OS), "Safety of Life" (SoL), "Commercial Service" (CS), "Public Regulated Service" (PRS), and "Search and Rescue" (SAR). The OS service level uses unencrypted signals and is free of charge. Receivers can use single or dual frequency measurements. There is no integrity check on this level. Signals in the CS and PRS levels are encrypted and integrity can be checked which will necessary for our concept. CS level services can be bought from licensed companies. SoL applications are also free of charge, have equivalent precision as OS (with dual frequency measurements) and use integrity checks as well as authentication of the satellite signal. For this purpose the signal is digitally signed with the private key. The public key is distributed. Further details can be found at [20].

3.3.2 WLAN and Bluetooth location providers

Conventional WLAN infrastructures can be used for positioning purposes. The obvious methods to achieve this are to determine the distance by either measuring the signal propagation delay or by measuring the signal strength. Due to the structure of modern buildings and the incapabilities of WLAN network cards and normal access points both values cannot be practically used. Instead an inferent approach has been developed and is commercially available. The basic idea behind this approach [13] is to utilize a general propagation model and to parameterize this model through a number of test measurements. The pure mathematical calculation of such a model would be too complex.

The mobile client has to measure the signal strengths of all surrounding access points and delivers these data to the positioning engine which than calculates the position by solving a maximum likelihood problem. The system is not effected by the fact that several access points transmit at the same frequency because it uses the integrated signals.

Other approaches utilize modified access points in order to determine the distance to the mobile client via measuring the signal run time. Examples are WhereNet (WLAN) and UbiSense (Bluetooth).

3.4 Detection of re-routing attacks

3.4.1 Precise clocks

Some location providers do not have a bidirectional communication path between all components. GPS receivers for instance works offline most of the time. In order to prevent the system from re-routing attacks while being offline (without return channel) it is necessary to implement a precise clock within the system. Remember that re-routing causes small latencies. This clock must be secured against manipulation. Secure protocols for the initial synchronization are discussed later. Depending on the clock drift the times between subsequent recalibrations can be adjusted. High stability quartz based clocks at reasonable prices suitable for integration into consumer electronics have a precision of about 5*10E-7 [21]. The drift caused by temperature changes is less than 10E-12. Long time aging processes do not have much influence as they are predictable and very constant over time. This makes it possible to build clocks with less than 15 seconds time error per year. We will show later how often time synchronization is needed with this clocks to avoid rerouting attacks.

3.4.2 Authenticated clock synchronization

In order to synchronize the clock of the proposed DRM system it is necessary to exchange timestamps with a trusted device. In his PhD thesis of 2004 [11] Mykhailo Lyubich presents a method for secure time-stamping which can be used to synchronize clocks between two devices. He discusses a variety of threats against such a system such as impersonation and replay. For our needs it is sufficient to authenticate the trustworthy, external clock against the DRM module. This can be ensured by establishing a challenge-response-scheme.

4. CONCEPT AND ARCHITECTURE

In this section we introduce the idea and describe our motivation for the chosen architecture. The architecture depends very much on a threat analysis which is given later in this section. The relationship between threat and design decision is also figured out.

We discuss our idea on two examples. These are a location provider developed by us which uses a WLAN ad hoc network for positioning and for comparison a satellite based positioning systems.

4.1 Conceptional overview

In order to determine an authenticated position the following task have to be accomplished in the given order:

- The position has to be calculated.

- The position has to be authenticated. Components trusted by the rights owners have to reach a predefined level of certainty that the observed device is in the calculated position.

- The access control module has to decide on the basis of the authenticated position information whether it grants access to the protected material. Access is generally granted when the position is within the "approved area" (above a given certainty level).

Figure 2 gives an overview about the system's general functionality. Inputs are signals of the particular positioning system, a description of the approved area (shape information) and the encrypted data. Depdendent of calculated position and the module's certainty about the calculation and hence the position, the module will grant or deny access.

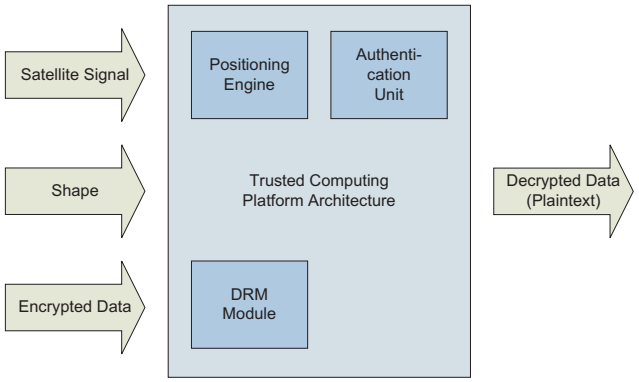

Figure 2: Authenticated positioning.

We use the term *approved area* for the area where the controlled material is accessible when the device is inside. The transmitted shape data which defines an approved area can be protected by signing them with the private key of a trustworthy CA (certifying authority).

In [12] a detailed **risk analysis** has been performed. A highly possible **re-routing attack** against the system works by having a fixed receiver station within the approved area and to distribute its signal across a connection. Rerouting could be performed on different network layers. On the physical layer the entire spectrum could be forwarded. The bandwidth of a IEEE 802.11g (draft) compliant channel is about 22MHz. On the MAC layer an attacker would have to forward up to 54Mbit per second for example. GPS uses much lower bandwiths. Hence, those signals are a potentially easier to be re-routed.

The purpose of every cryptographic process is to raise the costs for breaking into a system well above the price of the data to be protected. The costs for a re-routing attack comprises of the following:

- Costs for the data connection (either analogue or digital)

- Costs for the reference receiver (including A/D converter when using a digital connection)

- Costs for the transmitter which re-radiates the signal

We would estimate the overall costs for this kind of attack of about 1000 EUR or less. This is very inexpensive compared with the possible result. Therefore the proposed architecture must reflect this and increase security significantly. We do not see a method to attack the system except assaulting the cryptographic parts or by performing a rerouting attack. Increasing cryptographic security is beyond the scope of this paper. Rerouting attacks can practically only be prevented by observing time delays.

Other ways would demand to check for electromagnitical radiation which is obviously much harder in mobile environment. We optimized our system for this purpose and will present the result in the following section.

4.2 Authenticated positioning in a wireless mobile ad-hoc network

Section 3 explained how signal strengths and a parameterized propagation model can be used for position determination in a wireless network. We want to use this position to enable or disable access to protected digital material. We have shown that a rerouting attack is the most likely attack. In this section we present how a position can be proven to the access control module.

Basically we use signal strengths for positioning. As shown in several publications [17, 10, 6, 18] deriving the position directly from signal strengths of surrounding APs does not deliver accurate position information. We will use an adapted method. This method uses a propagation model which is normally being calibrated by several test measurements. This calibrated model will be used to find the most likely position according to the current measurement of signal strengths. The need for calibrating the model renders these methods useles for MANETs and makes them impractical for stationary networks. In earlier research [16] we have simplified this by calibrating the propagation model (also known as radio map) with information available from surrounding nodes - which means, we do not have a distinguished mobile calibration client. Instead, in order to calibrate the propagation model we consider measurement reports from nodes with known positions. These nodes determine the signal strengths to other fixed nodes. The difference between expected signal strength and real signal strength is used to parameterize the propagation model. The error between expected and measured attenuation is virtually distributed over the entire distance between two nodes. By performing this within all nodes in sight of each node a two-dimensional model will be generated. Figure 3 shows schematically how the model is parameterized.

For the system to work the nodes have to be authenticated - at this time "authenticate" refers to the nodes itself and not to their position. This is tradionally being achieved using a public key infrastructure (PKI) [5] or a web-of-trust. For our purpose a PKI will be sufficient. By these means nodes can proof their identity.

The **position is determined** by indirectly measuring the signal strengths of surrounding nodes. The following text of this section explains the positioning process in full detail. Some of the nodes are located at a fixed position which is determined by other means or pre-defined. Those nodes act as basic nodes or level zero nodes. Level zero nodes are used as fixed points for the location of all other points. The position of a level zero node is considered authentic by definition. A level zero node is able to "unlock the door" of

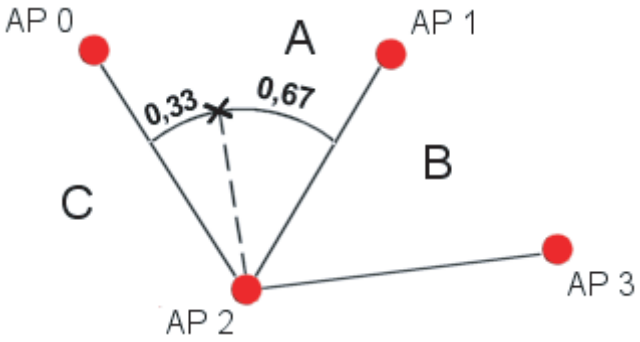

Figure 3: Distributing the error in two dimensions.

the DRM module instantaneously if it is located within the "green area".

Nodes which derive their position directly from "level-0-nodes" have to earn the defined level of authenticity. In a two dimensional space at least three other nodes in a good geometric constellation are required to determine the position. If all of the three nodes are "level-0-nodes" the other node becomes authenticated. In most configurations of a mesh network there are usually more than three nodes available in the neighborhood for distance measurement. A higher density of nodes increases the trustworthiness of each node.

The structure establishing that **authenticity of position information** is similar to a web of trust preventing the system from a classic man-in-the-middle attack. Other possible attacks against the authenticity of the location such as replay and rerouting attacks are addressed later in this paper. In order to create a web of trust a node receives digitally signed measurement reports from other nodes. A measurement report contains the signal strength of the observed node. The signal strength is a good indicator for distance when combined with a statistic approach as we will show later in this paper.

Since some nodes might be mobile all measurement reports have to be tagged with a time stamp. The frequency of running the positioning procedure depends on the speed of the mobile node. A very precise time stamp is additionally necessary to prevent the system from a rerouting attack in which a proxy node is actually connected with a spoofing node outside the "green area". As our design uses a trusted hardware device in each node to protect the digital material the entire communication at the wireless side would have to be rerouted to and from the spoofing node.

Proving authentity requires certificates in a public key infrastructure [5]. For ease of use we utilize public key encryption [7]. Each node carries a unique private key which will be used in the authentication process as well as for decryption of secret messages. The corresponding public key is signed by a Certifying Authority (CA) which belongs to each closed user group in our system. For our purposes it is most feasible that the CA is operated by the provider of the digital material to be protected - in some scenarios this might not be acceptable since the CA may deny further access to the material. In these cases a trusted third party may be introduced to host the CA. Traditional certificates such as X.509 [5] can be used for this purpose.

As mentioned before all nodes are able to proof their identity by using a unique certificate which is signed by a CA. In order to proof its own position a node has to collect several measurement reports from surrounding nodes. Each measurement report contains the signal strength of the observed node as it is seen by the node generating the report. All reports are digitally signed using the node's private key.

Some special nodes called "level-0-nodes" have a certificate available that marks them as nodes with a position that is not doubtful. Their position might have been securely determined by other means such as GPS [8] or land surveying. The signatures of a CA ensures that only distinguished nodes can claim to be a "level-0-node". Nodes which derive their position from "level-0-nodes" receive measurement reports as well as position reports. Both information are signed and therefore being marked as originated by a "level-0-node".

All reports from nodes other than "level-0-nodes" contain their calculated position (postion report) and the signal strength of the node to which the report is addressed (measurement report). All reports are signed as usual by the sender. In order to proof the calculated position the sending node also includes the signed reports which were used to determine its own position.

Following this scheme ensures that every node is able to see and check the paths which were used to determine its own position back to at least three "level-0-nodes".

In order to prevent re-routing attacks we have to detect those attacks first and then to deny authentication for that node. The only practicable method to detect rerouting in our wireless scenario is to detect delays caused by forwarding signals. Detecting extra radiations would be almost impossible.

With COTS WLAN devices we are able to measure latencies on the MAC layer with an accuracy of 0.2 to 0.1ms. Effects such as an occupied over-the-air channel can be eliminated by performing several measurements and using the minimum as latency. For this purpose the authentication module inside the chipset should have full control over underlaying network layers, allowing it to determine the latency between the point in time when a signal is received at the antenna and the point in time when it reaches the authentication module. This makes rerouting attack discovery much easier.

A node denies sending measurement reports to nodes failing the latency tests. The communication is also monitored by other nodes. If a third node witnesses any frauds it will immediately broadcast a fraud report. Possible denial of service attacks against those fraud reports are monitored by other nodes which then will generate fraud reports as well. By that an unfriendly node can be separated very fast and will be excluded from further communication. False fraud reports which mean another form of denial of service are addressed by sending fraud reports regarding these fraud reports.

As explained before, the position of certain nodes is known through other means of positioning. These nodes are labeled with a position certainty of 1. We will call these nodes "level-0-nodes". Nodes which derived their position from those "level-0-nodes" have a position certainty of less than 1. This depends on the signal strength (as function of the distance) to and geometry of the surrounding "level-0-nodes". "Level-0-nodes" broadcast their own position and

measurement reports containing the signal strengths of other "level-0-nodes". These data are used to parameterized propagation model. Nodes with at least three "level-0-nodes" as neighbors with a reasonable geometry between them calculate their position and broadcast this first fix to surrounding nodes. On receiving position estimations of other nodes each node refines its own position estimation and broadcasts the result. The algorithm will converge after a few iterations.

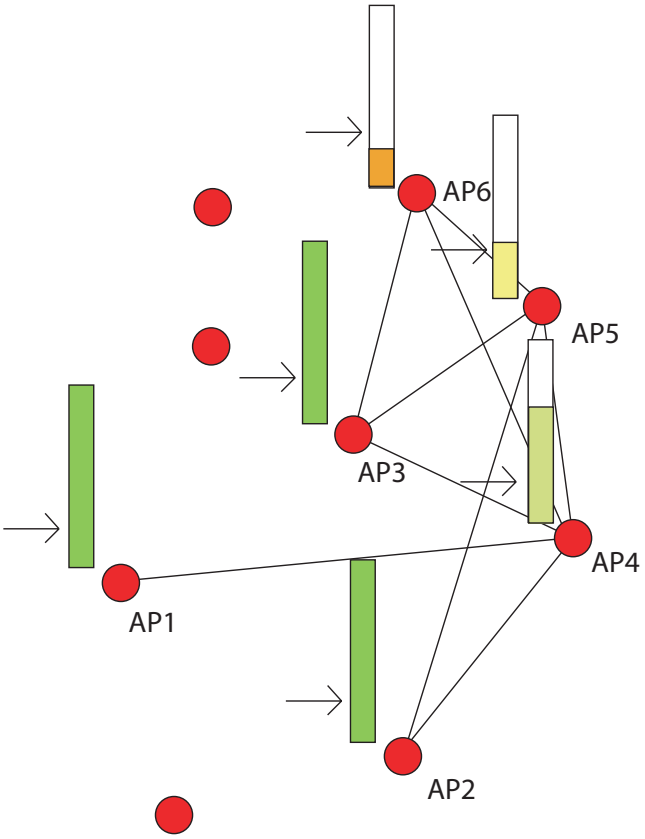

Figure 4: Nodes' certainty about their position. The arrows mark the threshold which is necessary for enabling access.

A specific threat to this location provider are **fake nodes**. These nodes could be set up with a fake initial position to that pretend to be part of the trusted network. The following section will also show how the system can be protected against fake nodes. **Denial of service attacks** against a wireless network can be easily performed as well. The authenticated positioning method will address this problem as well where security is at stake.

4.3 Authenticated positioning using GPS or Galileo

In order to use position information to enable access to controlled material it is necessary to find a way to authenticate the received satellite signals.

The satellite signal contains a very precise time information which can be compared with an independent time source in order to detect the re-routing of signals. This internal clock must be protected against manipulation. The clock has to be integrated into the device since there is no constantly usable response channel for synchronization with external time sources. As analyzed in this paper in section 3 current state-of-the-art clocks have a typical error of less than 15 seconds per year. Assuming that an internet connection is used to distribute the satellite signal there will be a delay of at least 5 milliseconds caused by active network components. An ISDN connection would generate at least the same latency values. Connections with less latency will be much more expensive and require a dedicated leased line. They are practically impossible. Assuming the clock error of 15 seconds per year - which is a reasonable value for inexpensive quartz driven clocks as shown in the last section - the clock will pickup an error of 5 milliseconds in about 3 hours time. This means the clock has to be synchronized every 3 hours in order to enable detection of rerouting attacks.

This time can be further increased when the clock drift is known and constant and can be calculated in advance. Each time the clock is synchronized with an external source the drift can be determined and stored inside the chipset.

The re-routing attack could be improved - seen from the attacker's point of view - by manipulating the timestamps of the satellite signal before it is re-radiated at the receivers site. This would imply the need for full decoding of signals. Galileo for instance includes signed timestamps. An anti spoofing mechanism is also included in current GPS signals for governmental purposes. Signed timestamps make it possible to detect every kind of manipulations executed by the attacker to conceal delays caused by rerouting attacks.

The internal clock inside the device itself can only be set up in a trusted environment. This prevents it from being manipulated Algorithms to perform authenticated time synchronization are described in section 3. The time between mandatory time synchronization depends on the precision of the clock. It is impossible to use a data stream such as a TV program for time synchronization since the data signal is subject to the same rerouting attack. A dial in connection can be used for that purpose. When the device fails to synchronize time for a grace period it will disable access to the DRM protected material.

A **replay attack** can be performed very similar. The satellite signals will be recorded at a position inside the shape. Later the signals can be broadcasted at every other location. This fraud can be fought by the same methods as against the rerouting attack.

A specific threat regards the use of **simulated satellites**. This can relatively easily be solved when the positioning signal is signed itself. Galileo will use public key cryptography for this purpose. So called "certified receivers" will be able to check the digital signature. For GPS this is currently only available for governmental users.

The transmitted shape data which define the area where the protected material is accessible inside can be protected by signing them with a private key and thus using public key cryptography.

5. TESTS AND DISCUSSION

5.1 Results of the WLAN location provider

We have simulated the authenticated positioning system to check whether the algorithm will calculate a position and whether this position is precise. We considered both parts, the positioning itself and the authentication. In a second step we have collected and entered measured values into

the system in order to perform the calculation with real data. These data have been collected in a roof top network of about 150 nodes which is supported by the author. We than programmed the algorithm for commercial-off-the-shelf access points with Atheros chipsets. We have tested those under lab conditions. Our real test implementation showed that there are too much data to be processes, which exceeded the memory limit of our access points which is 32MB RAM in the concrete example. Other chipsets such as Broadcom could not be tested since their drivers are not open source.

Our experiments show that precision of position and certainty about position depent on the same factors, mainly distance and geometry. A detailed analysis will be published later when we have more real data available.

5.1.1 *Precision of positioning*

As already noted we are taking only calibration measurements from fixed nodes into account which naturally reduces the precision of the propagation model. With the help of a Master's thesis we have evaluated the accuracy of this simplified system. In a real world scenario the average positioning error inside a building increased from 2 meters to about 10 meters as shown in Table 1.

Max. error (in m)	Number and percentage of measurements below error	
	Bayesian	Simplified
1	35% (7)	13% (4)
2	75% (15)	26% (8)
3	85% (17)	35% (11)
4	85% (17)	52% (16)
5	90% (18)	61% (19)
6	95% (19)	74% (23)
7	100% (20)	77% (24)
8	100% (20)	87% (27)
9	100% (20)	90% (28)
10	100% (20)	97% (30)

Table 1: Comparison of error distribution under equal laboratory conditions.

In another Master's thesis a student has broken this algorithm into a distributed, iterative system that can run on low-resource nodes itself. For practical tests we use commercial access points running on Linux.

For outdoor tests we have manually collected signal strengths from a wireless community network [1]. A distributed algorithm to run directly on the access points and to determine the position there has been developed and simulated but was not available at the time of performing the measurements. Therefore we have entered these data manually into the system performing the simulation. As the same methods are used in the offline system and the distributed system running on the access points the results are equivalent. The network consisted of about 30 stationary nodes with well know positions for each node. Figure 5 shows the radiomap for that network.

For most of the nodes we have taken three or four surrounding nodes and their signal strengths to compute the position of the given node. The distance between known and calculated position is distributed as in Table 2.

We consider these results to be sufficient for the purpose of mesh network based location aware dependent digital rights management. Further aspects of increasing the accuracy are beyond the scope of this paper and will be published separately.

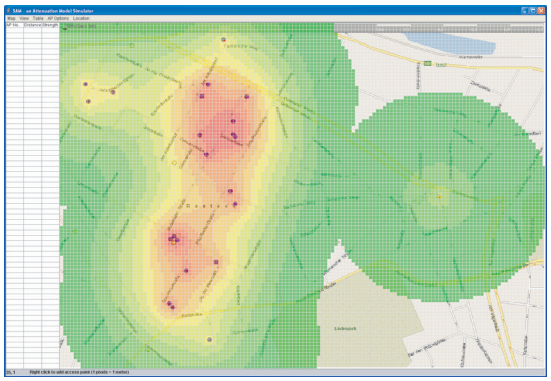

Figure 5: Radiomap for the test network.

Max. error (in m)	Number and percentage of measurements below error
0 - 5	5% (5)
5 - 10	12% (12)
10 - 15	21% (21)
15 - 20	50% (50)
20 - 25	70% (70)
25 - 30	78% (78)
30 - 35	88% (88)
35 - 40	100% (100)

Table 2: Distribution of errors in a productive ad hoc network.

5.2 Comparison with a satellite-based system

In order to show the feasibility of our approach we have implemented a prototype on a Linux driven TV satellite receiver [2] with an in-built harddisk. We successfully performed serveral test with GPS. We used artificially generated latencies to simulate re-routing. We were not able to use authenticated satellite signals as they are only available with special receivers.

5.3 Discussion

Both location providers are suitable for authenticated positioning. The types of attacks are basically the same for both systems. Different implementations are necessary due to the fact that satellite based system do not provide a method to measure round-trip-times easily. Therefore clocks in these systems have to be stable for a longer time.

Both concepts are based on two assumptions:

- The entire hardware comprising of positioning module, authentication unit, and access control, is secured against manipulation. This hardware is trustworthy for the rights owner.
- All cryptographic processes are secure.

The first assumption is trivially necessary for access control and authentication unit. The positioning module has to be trustworthy as well in order to prevent attackers from

manipulating the interface between positioning and authentication unit.

Both concepts do not provide absolute security against manipulation. The need of detecting re-routing attacks implies narrow timings. With a maximum latency of 5ms for systems without a return channel is a compromise between stable clocks and the simplicity of re-routing attacks.

As the drift does not have that impact on WLAN based location providers - or generally those with a return channel - timing is much easier. On the other hand we have to provide timing data from very low level components of the driver. In some cases even a change of WLAN hardware would be necessary. Common WLAN protocols do not provide a possibility to guarantee shorter round-trip-times, for instance by using priorized requests and replies.

6. OUTLOOK

The security of our WLAN based location provider depends much on the presets for the required confidence level. We believe that further activities are necessary to define those presets with respect to the value of the information to be protected. An error estimation while calculating one node's position would have some advantages in the same direction. We have started empirical studies that measure and calculate the distribution of errors in a testbed of more than 150 nodes, some of them being mobile.

7. REFERENCES

[1] The Opennet Rostock. "http://www.opennet-forum.de/".

[2] Dream multimedia. "http://www.dream-multimedia-tv.de/", 2004.

[3] J. Feigenbaum. *Security and Privacy in Digital Rights Management*. Springer, Heidelberg, 2003.

[4] G. W. Hein, J. Godet, J.-L. Issler, J.-C. Martin, P. Erhard, R. Lucas-Rodriguez, and T. Pratt. Status of galileo frequency and signal design, 2002. http://europa.eu.int/comm/dgs/energy_transport/galileo/doc/galileo_stf_ion2002.pdf.

[5] R. Hunt. PKI and Digital Certification Infrastructure. In *Proc. of the Ninth IEEE International Conference on Networks (ICON 01)*, Bangkok, 2001. IEEE Press.

[6] S. Ito and N. Kawaguchi. Bayesian based location estimation system using wireless lan. In *Proc. of the Third IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOMW'05)*, Kauai, Hawaii, Mar. 2005. IEEE Press.

[7] B. Kaliski. A survey of encryption standards. *IEEE Micro*, (6):74–81, November/December 1993.

[8] E. D. Kaplan. *Understanding GPS: Principles and Applications*. Artech House Publishers, Norwood, 1996.

[9] J. Kelsey, B. Schneier, and C. Hall. An authenticated camera. In *Proc. of the 12th Annual Computer Society Applications Conference (ACSAC)*. ACM Press, december 1996.

[10] T. Kitasuka, T. Nakanishi, and A. Fukuda. Wireless lan based indoor positioning system wips and its simulation. In *Proc. of The 2003 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM'03)*, Victoria, BC., Aug. 2003. IEEE Press.

[11] M. Ljubich. *Methods for Enhancing the Security of Java Card based Payment Protocols*. PhD thesis, University of Rostock, Rostock, Germany, 2004.

[12] T. Mundt. Location depdendent digital rights management. In *Proc. of 10th IEEE Symposium on Computers and Communications*, La Manga del Mar Menor, 2005.

[13] P. Myllymaki, T. Roos, H. Tirri, P. Misikangas, and J. Sievanen. A probabilistic approach to wlan user location estimation. In *Proc. of the 3rd IEEE Workshop on Wireless LANs*, Bonn, Germany, Sept. 2001. IEEE Press.

[14] O. Onidi. Galileo is launched, 2002. http://europa.eu.int/comm/dgs/energy_transport/galileo/doc/galileo_is_launched.pdf.

[15] U. Reimers. *Digital Video Broadcasting (DVB). The International Standard for Digital Television*. Springer, Heidelberg, 2000.

[16] R. Sasum and T. Mundt. Assessment and comparison of radio network based positioning technologies. Technical report, University of Rostock, Aug. 2005.

[17] B. Schilit, A. LaMarca, G. Borriello, W. Griswold, D. McDonald, E. Lazowska, A. Balachandran, J. Hong, and V. Iverson. Challenge: Ubiquitous location-aware computing and the place lab initiative. In *Proc. of The First ACM International Workshop on Wireless Mobile Applications and Services on WLAN (WMASH 2003)*, San Diego, CA, Sept. 2003. ACM Press.

[18] V. Seshadri, G. V. Zaruba, and M. Huber. A bayesian sampling approach to in-door localization of wireless devices using received signal strength indication. In *Proc. of the Third IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOMW'05)*, Kauai, Hawaii, Mar. 2005. IEEE Press.

[19] K. Shimada. Patent US 5,922,073: System and method for controlling access to subject data using location data associated with the subject data and a requesting device, 1999.

[20] The European Commission. Mission high level definition, 2002. http://europa.eu.int/comm/dgs/energy_transport/galileo/doc/galileo_hld_v3_23_09_02.pdf.

[21] J. R. Vig. Introduction to quartz frequency standards. Technical report, Army Research Laboratory, Oct. 2002.

[22] W. Rosenblatt et.al. *Digital Rights Management: Business and Technology*. John Wiley and Sons, New York, 2001.

[23] J. S. Warner and R. G. Johnston. GPS Spoofing Countermeasures. http://www.homelandsecurity.org/bulletin/Dual Benefit/warner_gps_spoofing.html, 2003.