Authenticated Location in Wireless Mesh Networks

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

Abstract—Location is part of the context of an ensemble of mobile nodes in a wireless mesh network. In this paper we present a concept and an architecture for a location aware Digital Rights Management system. This system uses signal strengths in a mobile ad-hoc or mesh network to determine the position of each node and to authenticate these position information. It enables devices to control access depending on their position. We describe algorithms, protocols, security threats, and a prototype.

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

Acknowledgment: Rainer Sasum and Jan Eckhoff for implementing parts of the positioning algorithm as part of their Master’s thesis. Sebastian Speicher and Martin Garbe for some very helpful discussions. Clemens H. Cap and Dieter Gollmann for advice.

I. INTRODUCTION

In [1] we have presented a method how a satellite based positioning system such as Navstar GPS or its upcoming European pendant Galileo can be used to determine the position of a trusted device. This trusted position information is then being used to enable access to data or devices protected by Digital Rights Management (DRM). The system introduced in that paper requires a trusted device consisting of a satellite receiver to determine the position and a precise clock in order to detect rerouting or repeating attacks. Both prerequisites are expensive to realize. Therefore we have been looking for different location providers which are suitable for pervasive computing environments. In this paper we show how a wireless mesh network can be utilized to determine a trustworthy position information which can be used in a DRM process. The nodes in the network form an ensemble of independent nodes which requires special consideration when authenticated position information is required.

A. Scenarios

Within the research community and the general public Digital Rights Management (DRM) is discussed very controversially. Beside all ethical and practical disadvantages DRM has eligibilities where copyrighted or classified material has to be protected. Usually this protection is realized by binding a resource to a certain context such a single computer or a single person.

The idea of authenticated positioning and location driven DRM has been developed after finding a vast variety of scenarios where location is essential for controlling access to resources. A small fraction of those scenarios is presented here:

• An Oscar nominated movie shall be only viewable at the referee’s home only. [2]
• TV shows or DVD movies are licensed to a single country only.
• A smart device that refuses to work outside its home environment.
• A hard disc containing the blueprint of a nuclear bomb can only be read on the premises of the lab. [3]

We formerly addressed these scenarios in [1] with a satellite based location provider, but concluded that a more locally operating location provider such as one based on a radio network would be more feasible for some scenarios. A disadvantage of a satellite based location provider is that it works poorly indoors. In all scenarios there is an obvious need for Digital Rights Management with location as an arbitrative credential to gain access to a resource. With our idea it is possible to use authenticated position information to enable access to restricted digital material or to restricted devices.

B. Idea

With the system presented it is possible to limit access to devices or digital material. Digital material has to be encrypted and devices have to be locked. A secret key can only be utilized to decrypt the digital material or to enable any other process when the device is within the specified area (“green area”). The trusted device can be manufactured as a chipset in order to be integrated into a variety of devices. Examples are TV set top boxes or satellite receivers, data viewers / data storage devices, mobile computers.

The system uses plausibility checks to ensure the received signal has not been tampered with - for instance has not be reradiated on a different location or replayed.

To fulfill the scenarios two tasks have to be accomplished:

• One task is to determine the position of a mobile device within a wireless mesh network, preferably without additional hardware.
• The other more complex task is to authenticate the position. In the concrete case the DRM device has to reach a preset certainty of its own position in order to grant access to its protected data.

We have fulfilled both tasks by providing a location provider for mesh networks and by providing a tested protocol that ensures trust in position information. In this paper we present an authenticated location provider that works with the aforementioned scenarios. To the best of our knowledge there is no similar system.
C. Structure of this paper

In section II we briefly discuss existing technologies in the fields of authenticated positioning, Digital Rights Management, and wireless network based location providers. Section III introduces our new approach on a conceptional level. We report about first experiences with the system in section IV. A brief conclusion is presented in section V.

II. Technological Basis

In this section all major technologies needed to implement the proposed solution for authenticated positioning and position dependent rights management are presented in a very short way. Those technologies include DRM and network based positioning systems as a possible location provider. At the beginning fundamentals of authenticated positioning are discussed. An overview of the current patent situation is also given.

A. Digital Rights Management (DRM)

In order to understand how location can be used as input for a Digital Rights Management system we would like to give a very brief overview about DRM.

Digital Rights Management [4] allows the copyright owners of multimedia content to decide under which circumstances they want to allow users to access documents. Access can be restricted to read, write, change, update, and other operations. A more comprehensive overview about DRM technologies can be found in [5].

Managed material is secured by cryptographic methods such as encryption, watermarking, and signing. For our proposed solution encryption will be necessary to protect the digital material from being read outside the enabled area. Encryption can be done by several algorithms such as RC4 [6] and AES [7] depending on the nature of the digital material [8]. Further information about relevant cryptography for DRM is available in [9].

B. Positioning

In "An authenticated Camera" [10] Kelsey, Schneier and Hall present how an image taken by a camera can be bound in space. Their idea is to use a time stamping service to bind an image and a time and to interact with a "nearby" trusted device to bind image and location. They explain possible attacks such as "rerouting" signals and state that these kinds of attacks are very difficult to inhibit. The focus of their paper is different from our scenarios, but we will use their terminology of possible attacks.

C. Location Service 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 [11] 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 then calculates the position by solving a maximum likelihood problem.

III. Concept, Architecture and Security Threats

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.

A. Conceptional Overview

At first we give an overview for better understanding. Details are presented later as noted in the following text.

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

- A public key infrastructure (PKI) has to be established.
- The position has to be calculated. In this case a location provider that utilizes signal strengths is being used.
- The position has to be authenticated. Trustworthy components of the system have to reach a predefined level of certainty that the observed device is in the calculated position. This part is realized by a web of trust.
- The DRM 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 "green area" (above a given certainty level).

We use the term "green area" for the area where the DRM protected material is accessible inside. The transmitted shape data which define a "green area" can be protected by signing them with the private key of a trustworthy CA (certifying authority).

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 tradiionally being achieved using a public key infrastructure (PKI) [12] 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 the DRM module instantaneously if it is located within the "green area".
Nodes deriving 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.

The following data is relevant for the function of the location based DRM system:

- The system receives the copyrighted material or already contains it on storage media.
- The location is provided by a our authenticated positioning system.
- Furthermore the shape information is necessary for the DRM system to decide where it enables access to the copyrighted material.

The copyrighted material is encrypted. The key will be generated by the DRM system when access is granted. The format is defined by the copyright holder. As the chipsets are a trusted device of the copyright holder it can either contain a general key or a user-dependent key. In the latter case the protected material can be encrypted in a way that it can be decrypted by several keys [8].

Shape information defining the ”green area” has to be signed as well but does not have to be encrypted. This prevents them from being manipulated. Manipulation of shape data will obviously result in the total ineffectiveness of the entire system.

The concept relies on two assumptions:

- The trusted hardware is protected against manipulation attempts which are directed against timers, stored keys, and cryptographic functions.
- All cryptographic processes are strong enough.

B. Creating a public key infrastructure

Proving authenticity requires certificates in a public key infrastructure [12]. For ease of use we utilize public key encryption [13]. 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 [12] can be used for this purpose.

C. Position determination

Basically we use signal strengths for positioning. As shown in several publications [14], [15], [16], [17] 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 useless for MANETs and makes them impractical for stationary networks. In earlier research [18] 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 1 shows schematically how the model is parameterized.

D. Risk estimation and threats

In [1] a detailed risk analysis has been performed. A highly possible rerouting attack against the system works by having
a fixed receiver station within the "green 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.

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 rerouting 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 electromagnetical 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. Another possible threat 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.

E. Authenticated positioning

Section II 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 DRM module.

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 [19] 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 (position 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 rerouting 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.

As already shown a rerouting attack could be carried out on different layers. Rerouting on the physical layer requires a receiver that forwards the entire spectrum used for communication between stations. This could be accomplished on wired connections or wireless on a different channel or frequency. This is an unlikely attack because the required devices are expensive and need to forward the same bandwidth that is used for communication.

Possible countermeasures for physical layer rerouting are devices that determine the round-trip-time between sender and receiver and compare the latency with an expected value. To accomplish that, devices incorporating both transceiver and the authentication module are needed. Commercial-off-the-shelf (COTS) WLAN devices will not provide access to those timers. Timings need to be checked on higher levels with those devices which affects the accuracy of latency measurement.

On higher network layers an attacker has to forward digital data packets. This is easier than forwarding an entire frequency spectrum and hence implies a higher risk for the system. As pointed out before rerouting attacks can be exposed by detecting signal latencies. Delays are harder to detect in layers above the physical layer. This is caused by several buffers in the protocol stack. For very exact determination of delays the latency caused by those buffers has to be known to the authentication module. This also includes latencies caused by the remote node’s buffers.

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.

![Fig. 2. Nodes' certainty about their position. The arrows mark the threshold which is necessary for enabling access.](image)

**IV. First Realization of the Concept**

In order to show the feasibility of our approach we have implemented a prototype on a Linux driven TV satellite receiver [20] with a built-in harddisc. The position is determinated and authenticated using a wireless mesh network. We are supporting a wireless community network [21] and distributed positioning algorithm / protocol. In a second step we have collected real data from several access points manually. A summary of those results are presented in section III of this paper. Further detailed results under the aspect of location technology will be published separately as they are out of scope for this work. We have implemented the protocol in order to run it on real wireless nodes in our community network. The implementation performed as predicted after simulation and in laboratory environment. In 95 per cent of cases we are able to provide location information with an accuracy better than 35 meters in all test cases.

After those location related tests we have focused on authentication and Digital Rights Management. We have collected several attack trees and virtually tested the system against those attacks. For the attacks mentioned in section III we are certain that the system is proof. We believe that all relevant attacks mentioned in section III-D are impossible. In cases where an attacker is able to block the system - as it happens for example when the attacker performs a denial of service by jamming the wireless connections - the protected material will be not accessible at all.

**A. 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 I.

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

**TABLE I**

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 [21]. 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 known positions for each node. Figure 3 shows the radiomap for that network.

![Radiomap for the test network.](image)

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 II.

<table>
<thead>
<tr>
<th>Max. error (in m)</th>
<th>Number and percentage of measurements below error</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 - 5</td>
<td>5% (5)</td>
</tr>
<tr>
<td>5 - 10</td>
<td>12% (12)</td>
</tr>
<tr>
<td>10 - 15</td>
<td>21% (21)</td>
</tr>
<tr>
<td>15 - 20</td>
<td>50% (50)</td>
</tr>
<tr>
<td>20 - 25</td>
<td>70% (70)</td>
</tr>
<tr>
<td>25 - 30</td>
<td>78% (78)</td>
</tr>
<tr>
<td>30 - 35</td>
<td>88% (88)</td>
</tr>
<tr>
<td>35 - 40</td>
<td>100% (100)</td>
</tr>
</tbody>
</table>

**TABLE II**

DISTRIBUTION OF ERRORS IN PRODUCTIVE MESH NETWORK

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.

V. CONCLUSIONS AND OUTLOOK

We have introduced our idea of authenticated positioning used for location based Digital Rights Management. The system uses a wireless network and propagation models to determine a position. This position is authenticated by a protocol creating a web of trust. A digital rights management system grants access to protected material. Access depends on an authenticated position information which is provided by a distributed protocol. The system is suitable for all usage scenarios mentioned in section I.

Currently we are developing methods to describe and to measure the system’s expected and demanded confidence in the indicated position. At this point the accuracy of the location provider and the confidence needed for the decision of the DRM system are strongly linked. We need to determine an upper limit for the position error which depends from the geographical configuration of the mesh network. We also have to find ways to describe the value of the data to be protected and to derive the required confidence from that value.

REFERENCES
