Sense and Trace
A privacy preserving distributed geolocation Wifi based tracking system investigated through simulation

Bachelor-Thesis

in Computer Science at the VU University Amsterdam

January 17, 2013

Author: Daniel L.J. Genis[1] - daniel.genis@gmx.de
Study: Bachelor in Computer Science
University: VU University Amsterdam
Mentor: Eyüp S. Canlar[1,2] - canlar@di.uniroma1.it
First reader: Mauro Conti[3] - conti@math.unipd.it
Second reader: Bruno Crispo[1,4] - crispo@disi.unitn.it

[1] VU University Amsterdam, Netherlands
[2] Sapienza University of Rome, Italy
[3] University of Padua, Italy
[4] University of Trento, Italy

Abstract

Smartphones are becoming increasingly popular and come integrated with a vast array of tools, such as GPS, Wifi access and Bluetooth. Several researchers already envisaged to use smartphones for distributed sensing purposes. A particular proposed distributed sensing protocol is Sense-And-Trace (SAT), in which mobile devices collaboratively sense their environment to collect information about other mobile nodes with the final aim of tracking potential target nodes.

The expected benefits of using a distributed sensing network are better localisation accuracies compared to current GSM network based localisation solutions, without the need to deploy or maintain stationary infrastructure.

In this paper we analyse the tracking accuracies and communication (bandwidth) requirements of SAT protocol in a simulated urban environment. We simulate 9056 walking pedestrians during a 24 hour period inside a 9 block area in downtown Chicago.

Our experiments show that tracking accuracies are within 10 meters at 1 minute positioning intervals in an ideal simulated environment using 15 second detection intervals. The bandwidth requirements are 3 megabit per 1000 scanning nodes, also using 15 second detection intervals.

Contents

1 Introduction

Current GSM network based mobile phone localisation systems require the deployment and maintenance of infrastructure. The positioning accuracies achieved by tracking mobile phones through the GSM network are within 100 meters 66% of the time [6]. Smartphones offer an alternative to build a distributed sensing and tracking network for urban environments with the expected benefit of higher tracking accuracies.

Smartphones come with Wifi and Internet access built in and are capable of intercepting Wifi traffic. Each time a device communicates over Wifi the MAC address of that device is transmitted over the air in plain text. In current Wifi implementations the MAC address is static and therefore can be used as an identifier to track a device.

The Sense-And-Trace (SAT) protocol [5] has been proposed as a reliable, secure, privacy preserving distributed tracking alternative promising higher tracking accuracies compared to current GSM network based tracking. It has been designed to be used by Law Enforcement Agencies (LEA) to track targets of interest. Unlike GSM network based tracking the SAT protocol does not rely on deployed infrastructure.

Through simulation we show that the tracking accuracies of SAT are within 10 meters at 60 second positioning intervals and a ScanningInterval of 15 seconds. In our simulation the bandwidth requirements of SAT are under 3 megabit per 1000 scanning nodes using the same ScanningInterval of 15 seconds.

Motivation. SAT promises to offers higher tracking accuracies compared to GSM network based tracking. SAT is secure, easy to deploy & maintain and is decentralised. SAT uses smartphones as a distributed sensing network does not require any deployment or maintenance of infrastructure.
Current GSM network based tracking solutions offer tracking accuracies of 100 meters. GSM network based tracking solutions require the cooperation of the mobile phone network providers. Furthermore GSM tracking requires the deployment and maintenance of infrastructure. For example after a natural disaster the required tracking infrastructure may not be available anymore. The SAT protocol is unique as it proposes higher tracking accuracies. SAT is easy to deploy.

Contribution. We show the theoretical capabilities of the Sense-And-Trace protocol through simulation to determine its tracking accuracies, and its communication overhead (bandwidth) requirements. Using simulation we are able to show that the tracking accuracies are within 10 meters at 60 second positioning intervals using a ScanningInterval of 15 seconds. With a 15 second Scanning Interval the outgoing bandwidth requirements are 3 megabit per second (total) for 1000 scanning nodes. Our simulations show that SAT promises better tracking accuracies compared to GSM network based tracking, while using an acceptable amounts of bandwidth for its operation.

Outline. The remainder of this paper is outlined as follows. Section 2 discusses the related works and their relationship to our research. Section 3 explains how the SAT protocol works. In Section 4 we present the simulation setup and environment. Section 5 presents the simulation results and an analysis of the tracking accuracies and bandwidth requirements. In Section 6, we discuss implementation challenges and potential solutions. Lastly we present our conclusions in section 7.

2 Related works

Canlar et al. [5] originally proposed the SAT protocol and describe the SAT protocol in great detail. Their paper is useful for those readers who would like to get a more detailed picture about SAT. We will however explain the SAT protocol's ideas and principles in our paper, in particular we focus on the SAT communication model and explain this in an easy to understand fashion.

Cayford et al. [6] researched the accuracies of network based mobile phone positioning data to use for real time traffic jam analysis. They conclude that measurements have reached 100 meters accuracy for 66% of the measurements in GSM network based tracking. SAT was proposed to provide better tracking accuracies compared to GSM network based tracking.

Al-Kuwari et al. [3] conducted a Survey on Forensic Localisation and Tracking Mechanisms on Short-Range and Cellular Networks, investigating localisation algorithms. In particular they look at trustworthiness, accuracies, and possible attack vectors against the algorithms investigated. They also elaborate on current GSM network based tracking accuracies. They state about the E911 mandate that in the USA telco operators have to be able to localise 911 callers within 100 meters 67% of the time and within 300 meters for 95% of the time.

Cheng et al. [7] evaluated the feasibility of building a wide-area 802.11 Wifi based self-positioning system. Their research is in the context of determining your own position via the surrounding Wifi Access Points (AP). Their results show that a smartphone can determine its own position with 14-59 meters accuracy based on Wifi positioning alone in an urban environments. They tested 9 positioning algorithms in 3 different cities. Over all algorithms and cities their research resulted in an average Wifi self-positioning accuracy of 24.28 meters.
They also investigated the Wifi communication ranges and the relationship between Wifi communication success rates and distance to the Access Point (AP). Based on their research we chose to use a Range of {15, 30, 45} meters for our simulation study.

Radar, an indoor self-positioning system, has been proposed by Bahl et al. [4]. They showed that for a device to be able to reliably determine its own position inside a building a radio map needs to be created beforehand to achieve high positioning accuracies. Using Wifi access points and their signal strength as distance indicator researchers showed that the self-positioning inside a building is accurate to within 3 meters using the previously generated radio map.

Likewise Lorincz et al. proposed MoteTrack [13], a highly robust radio frequency based self-positioning system for indoor use. Their focus was on being robust and decentralised to ensure maximum availability in natural disaster environments. MoteTrack degrades gracefully if some deployed radio frequency beacons become unavailable to use for self-positioning. Like Radar, MoteTrack requires a previously generated radio map to achieve high accuracies in indoor environments. In addition MoteTrack requires the deployment of infrastructure (devices emitting beacons) to achieve its robustness and high indoor accuracies.

Zhu and Cao proposed a distributed positioning proof system named APPLAUS [14], which is a Bluetooth based location proof system. APPLAUS is designed as a proof mechanism to ensure that the phone actually is located where it is claiming to be. A Mobile phone asks nearby other Bluetooth enabled phones to vouch for the phone's current location, which it then submits proof to the server. APPLAUS, as well as SAT, use random pseudonym certificates for encryption to ensure the privacy of all parties. SAT however is intended to track targets that do not have the SAT application installed.

Husted et al. [11] researched how a distributed geolocation scanning network called Malnet can trace and detect other Wifi enabled phones. They show that 10% of the mobile phone population can trace a target with less than 18 second positioning intervals, in an urban environments. For our evaluation we also use 10% of the simulated population as basis for the SAT tracking network. Like Husted et al. we also use the UDel Simulator to simulate the movements of 9056 people inside the Chicago downtown area. Husted et al. used Landscan to obtain the population density for the Chicago 3x3 block map. We also use a population of 9056 in our simulations, based on Husted et al's work.

Fu et al. [8] showed that a high gain antenna on top of a roof can pick up Wifi probes with a distance of up to 1 kilometer away with clear line of sight. They also analysed various triangulation algorithms and their effectiveness. While they used a high-gain antenna on the roof of a large building, a setup which is not like our SAT protocol, it is important to note that Wifi probe requests can be collected at a distance. Using previous work from Cheng et al. [7] distances of up to 100 meters can be achieved without line of sight.

Karlson et al. [12] showed that Wifi is enabled during the day for 75% of people who use smartphones. This is an important observation since SAT relies on Wifi and its unique MAC addresses to uniquely localise targets.

The SAT protocol aims at creating a secure, privacy preserving, distributed tracking network for use by Law Enforcement Agencies (LEA). SAT does not require any deployed infrastructure or previous training for its operation. SAT is meant for tracking targets urban environments, unlike Radar and MoteTrack. Smartphones can self-locate themselves with accuracies of 25 meters [7], an observation which SAT builds on to use in the distributed scanning network. SAT does not rely on the cooperation of the tracked target which differentiates SAT from all other systems. Only Malnet [11] shares this feature with SAT, however it does not preserve privacy like SAT does.

3 SAT System model

The SAT protocol is based on three main Components: a DS (Data Storage) which is used to store the Geolocation Log Message (GLM) records, the Certificate Authority (CA) which provides the random pseudonym certificates for encryption and smartphones (nodes) which act as distributed detection network. A glossary of terms used in this paper can be found in Table 1.

For the SAT system model we make the following explicit assumptions. We assume that both type of nodes (sensor and target nodes) have their Wifi radios enabled continuously. The CA provides a Pseudonymous Public Key Infrastructure (PPKI). In which, the trusted CA acts as an authentication and authorization service for the sensor nodes, DS, and DC. The CA provides the sensor nodes with cryptographic private keys which will be used to encrypt the location data inside each GLM.

The smartphones are mobile devices distributed over a geographic area (e.g. metropolitan

Acronym	**Description**
AP	Wifi Access Point
BSSID	The Wifi MAC address of a mobile phone
CA	Certificate Authority providing public key infrastructure
ECC	Elliptic Curve Cryptography
DS	Data Store for the (encrypted) location reports
Delta	Amount of seconds used to aggregate GLMs for triangulation. Also referred to as Positioning Interval.
GLM	Geolocation Log Message
LEA	Law Enforcement Agency
Node	A phone which detects other phones
Range	Scanning range of nodes in meters
Report	Same as GLM. A report sent by a smartphone which detected another smartphone.
SAT	The Sense-And-Trace protocol
Scanning Interval	Time in seconds between nodes scanning for other nodes
Witness	Same as Node. A phone which detects other phones

Table 1: *Glossary of terms and acronyms used in this paper*

area). They communicate using their short range radios (e.g. Bluetooth or WiFi). Furthermore, they can pinpoint their own geolocation (e.g. using GPS, AGPS, or WiFi Location Service) using their embedded hardware. The smartphones detect other Wifi communications in their vicinity. We have two types of nodes: *sensor nodes* and *target nodes*. The sensor nodes voluntarily participate in SAT i.e. they run an application to scan their environment, and detect other Wifi devices in their communication range. The sensor nodes submit their logs on the DS using via a WiFi access point that the sensor node has access to, or by using the cellular data service (e.g. UMTS or HSPDA).

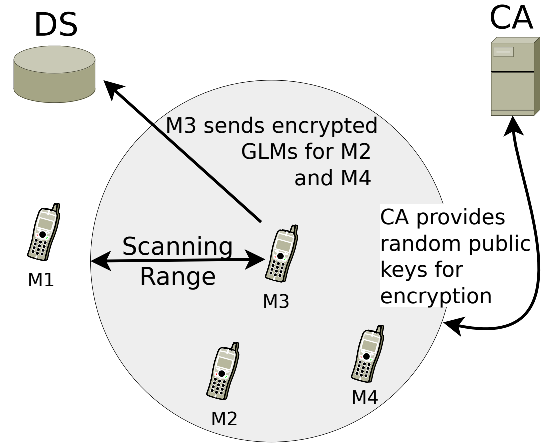
DS
CA
M3 sends encrypted GLMs for M2 and M4
CA provides random public keys for encryption
Scanning Range
M1
M3
M2
M4

Figure 1: *SAT protocol overview. M3 sends an encrypted location report for M2 and M4*

In Figure 1 we show an example for the SAT system model. The mobile phone M3 is within range of M2 and M4, therefore M3 will send a GLM for M2 and M4 to the DS. A GLM message includes the sensor nodes' location, the date & time, a public key identifier and the detected MAC addresses. The public key identifier is needed to be able to decrypt the GLM again using the correct private key. The location data inside the GLM is encrypted using random public keys provided by the CA for privacy preservation. The location information inside the GLM is the only content inside the GLM which is encrypted.

4 The SAT protocol

Sensor nodes detect other Wifi enabled devices in their vicinity using Wifi passive scanning. When a message is intercepted the detecting node sends a GLM to the DS which includes the targets MAC address and the detecting node's location. The DS collects and stores the GLMs for later tracking purposes. Each sensor node needs the SAT Application installed and Wifi enabled to be able to intercept surrounding Wifi traffic using passive scanning.

The CA provides the random pseudonym certificates which are used by the mobile phone nodes to encrypt the GLM records. For each GLM record the phone obtains a new random private key from the CA. The encrypted GLMs are sent to the DS which stores all records for later tracking use.

4.1 Target logging

A node detects all Wifi MAC (BSSID) addresses by passive scanning all Wifi communications every 15 seconds (the ScanningInterval) in its area. The node subsequently sends the detected MAC addresses as a GLM to the DS. A GLM report includes the following information:

- 32 bit integer as Latitude (encrypted)
- 32 bit integer as Longitude (encrypted)
- 46 bit Wifi BSSID MAC address of the target detected
- 128 bit integer as public key identifier
- 40 bit time stamp

Each GLM has its location information encrypted using a new random public key obtained from the CA (see Figure 1). Since the location information inside the GLM are encrypted the DS cannot use the GLMs for tracking without obtaining the decyption keys for the GLMs.

4.2 Target tracking

In order for the LEA to trace a target using SAT, they need to first obtain the target's GLM records and the neccessary decryption keys. This is due to the pseydonym public key infrastructure (PPKI) which is used to encrypt the position locatio inside the GLM. Figure 2 showcases the required communications for the LEA to track a target. The sensor node detects another smartphone and fetches a new private key from the CA (Step 1). Subsequently the sensor nodes submit an encrypted GLM to the DS.

In order for the LEA to trace a target they first need to obtain the GLM records for the target of interesst (Step 3). Since the location information is encrypted inside the GLM records, the LEA needs to obtain the decryption keys from the CA to be able to decrypt the records and trace the target (Step 4). The LEA then uses the GLM records to track the target's position.

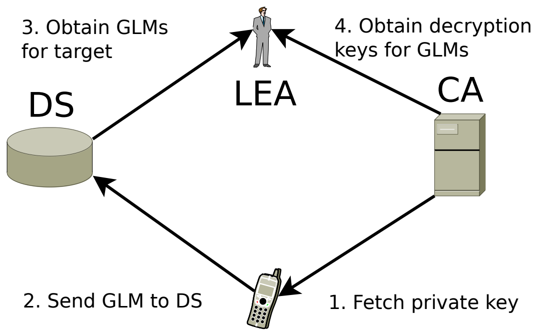

Figure 2: *SAT protocol communication overview*

This concludes our SAT protocol explanation. If a reader has questions about SAT we would like to refer the reader towards Canlar et al. [5] which is the original paper proposing SAT. Canlar's paper explains SAT in greater detail than required in this paper.

In summary the SAT protocol offers good privacy protection, requires no stationary infrastructure and is expected to provide better accuracies compared to current GSM network based tracking methods.

5 Simulation Setup

Currently no real world data sets exist that is suited to simulate the SAT protocol [11]. Such a data set would require complete and accurate positioning data for every person inside a city inside a 24 hour time frame.

We use the UDel Simulator [1] to generate the movements of 9056 people walking inside a 3x3 block area in downtown Chicago. "The UDel mobility simulator is based on surveys from a number of research areas including time-use studies performed by the US Department of Labor and Statistics, time-use studies by the business research community, pedestrians and vehicle mobility studies by the urban planning and traffic engineering communities. Based on these works, the mobility simulator simulates arrival times at work, lunch time, breaks/errands, pedestrian dynamics (e.g., realistic speed-distance relationship and passing dynamics), and workday time-use such as meeting size, frequency, and duration" [1]. These characteristics make UDel a good choice to generate the movements inside a city.

In order to be able to simulate SAT we have to make some assumptions. Most notably we do not simulate any detection success (or failure) rates. If a node is within two dimensional `Range` of another phone, detection is guaranteed. We use the `Range` between nodes very precisely. For example if the `Range` is configured to be at 30m (meters), then there will be no detection if the distance is 30,1m.

Our simulations are using 9056 walking pedestrians in a 9 block area from Chicago. Walking pedestrians inside a city are an ideal and realistic environment to conduct our SAT simulation study. Real world radio based connectivity issues are also not simulated as simulating such issues correctly without previous research out of scope for this thesis. All nodes can detect the target if the target is inside the scanning `Range`. Detection is immediate and guaranteed if the target is within the scanning Range. All witnesses (mobile nodes) are aware of their precise current position. We assume that the target and witness nodes all have Wifi enabled at all times, which is a necessity for the SAT protocol, as detection is based on the Wifi MAC addresses. The target localisation is computed using a two-dimensional centroid like algorithm.

We use the UDel Simulator Version 1 [1] and a 9 block area of Chicago to generate 24 hours of mobility data with 9056 walking pedestrians. The maximum walking speed of the pedestrians is 1,79 meters per second, the minimum walking speed is 0,70 meters per second, which are the default settings for the UDel simulator. The generated mobility data is then used as input to conduct our simulations using our own written SAT simulator.

The SAT simulation was developed with the following input parameters which have an influence on the outcome:

- ScanningInterval: How often do nodes scan for other nodes (seconds).
- Delta: All reports within a Delta time frame are aggregated, and a target triangulation is computed from all reports which are inside the Delta timeframe (seconds).
- Range: This is the detection range of nodes. If another node is within this Range it will be discovered (meters).
- Another input to our SAT simulator is the UDel mobility file, which contains all the movement data of the whole population.

These are the values which we used to conduct our simulations. For ScanningInterval we used {1, 15, 30, 60} seconds. For Delta variable we used 30 and 60 seconds. Furthermore for Range we use {15, 30, 45} meters. All combinations of the above settings are simulated and aggregated into our resulting data, which means that only *one* variable will change and all other simulation results are combined and shown. This gives the best overview on how a specific variable influences the tracking results. For all simulations we used a minimum of 3 witnesses to compute a triangulation. If there were only 2 witnesses reporting the target during a given Delta interval, then no triangulation is computed and the Delta interval is skipped creating a (small) tracking gap.

For each configuration we run 10 simulations on 10 different targets to ensure we receive a balanced set of results. Each simulation is a 24 hour simulation in which a specified target gets traced using our SAT protocol. As detection network we use 10% of the total population (9056). For each simulation run we pick a *random* 10% subset from the total population of nodes. The selected nodes act as distributed detection network to simulate the SAT protocol.

From each 24 hour simulation we compute the average and standard deviation from all tracking/triangulation results. This gives us 10 average and 10 standard deviation values for each simulation configuration. The 10 values are then averaged to receive the final values shown in the graphs (Figure 2-5).

We use one algorithm to compute the target position from the witness reports. This algorithm is often referred to as Centroid. Though the Centroid only averages the witness positions once. We took a slightly different approach since we average the positions twice. In Algorithm 1 we take the position average of each witness *distinct* pair (lines 5 – 13). Then as a last step we compute the average again to obtain the triangulation end result (lines 14 – 16).

Algorithm 1 Triangulation algorithm used during our simulations.
Averaging witness pairs, then average those to compute the final positioning

```
procedure TRIANGULATE($witnesses$)
    $n \leftarrow 0$                                          ▷ Initialise variables
    $x \leftarrow 0$
    $y \leftarrow 0$
    for $i \leftarrow 0$ to $(witnesses.size() - 1)$ do
        for $j \leftarrow 0$ to $(witnesses.size() - 1)$ do
            if $i \neq j$ then                 ▷ Continue only with 2 *distinct* witnesses
                $x \leftarrow x + ((witnesses.get(i).getX() + witnesses.get(j).getX())/2)$
                $y \leftarrow y + ((witnesses.get(i).getY() + witnesses.get(j).getY())/2)$
                $n \leftarrow n + 1$
            end if
        end for
    end for
    $x \leftarrow x/n$                         ▷ Compute the average of the temporary Data
    $y \leftarrow y/n$
return $(x, y)$
end procedure
```

6 Simulation results

6.1 Tracking accuracy results

The `Delta` variable is the time interval which is used to aggregate witness reports to compute the location of a tracked target. In other words it could also be called a Positioning Interval, because in these time intervals the target's position is calculated.

The `Delta` variable, for which we used 30 and 60 seconds in our simulations, has no influence on the tracking deviation results. For both `Delta` values the mean tracking deviation is 9.7 meters. This is the mean deviation from the target's actual (real) position. It is important to note that in our simulations tracking gaps *do not* negatively impact the mean tracking deviation. To give an exaggerated example: if during 24 hours a target was only traced once with a deviation of 10 meters, then the mean tracking deviation will show 10 meters as well. This is because whenever a tracking gap occurs there is no accuracy penalty. Additionally since we simulate slow moving pedestrians, the `Delta` has a smaller impact than if we simulated faster moving objects in our SAT simulations. For example if we simulated faster moving cars, then a `Delta` of 30 seconds would result in higher accuracies compared to a `Delta` of 60 seconds. This is because a car moves over a longer distance in 60 seconds compared to 30 seconds.

A higher `Delta` value decreases the tracking gaps (Figure 3). For each `Delta` time interval we aggregate all witness reports together to compute the target's location. If for a given `Delta` interval there are less than 3 witnesses, then no triangulation is computed and the `Delta` interval is skipped. Since increasing the `Delta` variable essentially requires less witness reports per minute, the reduced amount of tracking gaps using a `Delta` value of 60 seconds was to be expected compared to the lower `Delta` value of 30 seconds.

The `Range` variable in our simulation defines the scanning range of a sensor node. Our simu-

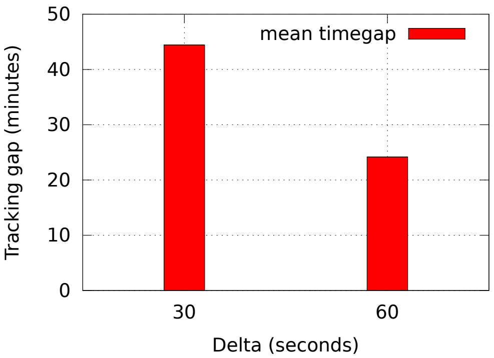

Figure 3: *Delta variable and average tracking gaps*

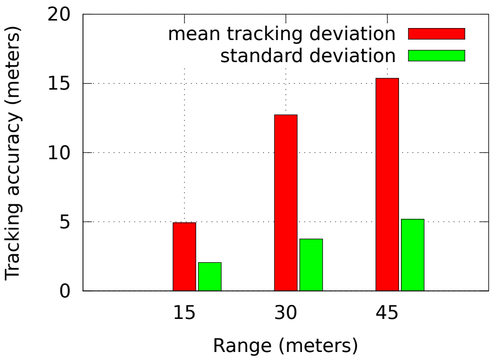

Figure 4: *Range variable and tracking accuracy*

lator uses the `Range` variable as a hard cutoff between detection and non detection. Pedestrians move slowly, so a `Range` of 15 meters will resulting in an accuracy of at least 15 meters. In our simulations we use the `Range` variable very accurately, which means that if a node is at a distance of 15,1 meters using `Range` 15 meters, then no detection occurs.

The `Range` variable has a direct impact on the tracking accuracy (Figure 4). The higher the `Range` the higher is the tracking deviation from the target's actual location. This is quite clear since we use the `Range` variable so strictly in our simulations.

A higher `Range` decreases the tracking gaps since with increased range the amount of GLMs sent increase as well. The more witness reports are available in a given `Delta` period the fewer tracking gaps will occur.

A `ScanningInterval` of 60 seconds reduces the tracking gaps (Figure 5). A tracking gap is the biggest gap between two computed target positions. A `Delta` of 60 reduces the tracking gaps, since it allows for more witness accounts to be used for each positioning interval. If for any given `Delta` there are 2 or less witness reports, the data is discarded and no triangulation is computed. This makes it possible for the tracking gaps to exist. The tracking gaps are at night when the simulated population is "at home". The UDel Model simulator simulates the typical urban commuting traffic. Which means during the day, due to the increased population amount inside the city, there are fewer tracking gaps.

The `ScanningInterval` is the time interval that the sensor nodes use to scan for other Wifi enabled devices. A higher `ScanningInterval` means less detection attempts per minute, so it does not come as a surprise that a higher `ScanningInterval` value increases the tracking gaps (Figure 5). The `ScanningInterval` setting has a direct influence on the amount of GLMs that are being reported, which influences these tracking gaps. These tracking gaps occur in our simulations at night time, when the lowest population amount is inside our simulated area. A `ScanningInterval` of 1 second provides the most witness reports (GLMs), which allows for the highest traceability with a minimum amount of tracking gaps (see Figure 5). However the bandwidth requirements using `ScanningInterval` of 1 are high, needing about 40 mbit of bandwidth in our simulations.

The `ScanningInterval` has no influence on the mean tracking deviation. Like we elaborated earlier this is due to the fact that, if no triangulation could be computed during a `Delta` interval, there is no accuracy penalty applied. This means that all triangulations that have been computed have the same degree of accuracy , regardless of the actual `ScanningInterval` used. Since we only compute the deviations between actual triangulations, the tracking deviation results do *not* reflect or include tracking gaps in any way.

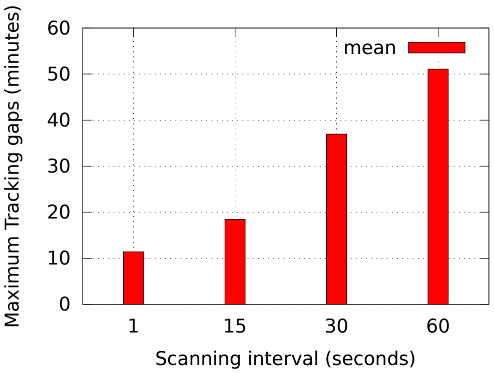

Figure 5: *ScanningInterval variable and average tracking gaps*

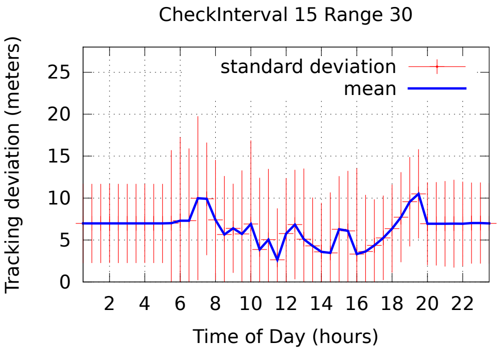

Figure 6: *24 hour tracking accuracy overview using ScanningInterval 15 Range 30 as configuration*

The potential tracking accuracies of SAT protocol can be seen in Figure 6. In our simulation the sensing smartphones are aware of their precise own location. Cheng et al. [7] showed that smartphones can use Wifi alone to determine their own position with an average accuracy of 25 meters in urban environments. As you can see in Figure 6 the configuration shown has an accuracy of under 10 meters. If we add another 20-30 meters deviation from the smartphone self-positioning, the potential SAT accuracies are likely 50 meters or better most of the time.

6.2 Bandwidth requirements

In this section we discuss the the bandwidth requirements of the SAT protocol. The biggest influence on bandwidth usage is the `ScanningInterval` variable. It directly relates to how many reports are sent to the DS and how much outgoing bandwidth is used by the SAT protocol. A GLM report sent by a node to the DS contains a total payload of 288 bits per message (see Section 3), excluding encryption.

The location information of the payload data is encrypted using the public key obtained from the CA and the actual payload size increases. Using Eliptic Curve Cryptography (ECC) together with 1024 bit keys results in a netto payload of 9 kilobytes after the GPS coordinates have been encrypted. The 9 kilobytes already include a 10% added overhead to account for TCP/IP overhead.

If phones are configured to detect every other communication device for *every second* the simulations show that the SAT protocol requires 40 megabit of outgoing bandwidth for 1000 sensor nodes (see Figure 7). Detecting every Wifi device in the vicinity within 1 second intervals is not desirable, not only due to the high bandwidth requirements. The power consumption would be higher compared to higher `ScanningIntervals`, like 15 seconds or higher.

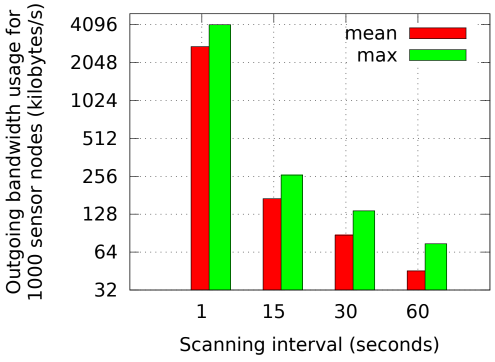

Figure 7: *Bandwidth usage in kilobytes per second and scanning interval. The data shown is for 1000 sensor nodes.*
Note: the Y-Axis uses log scaling.

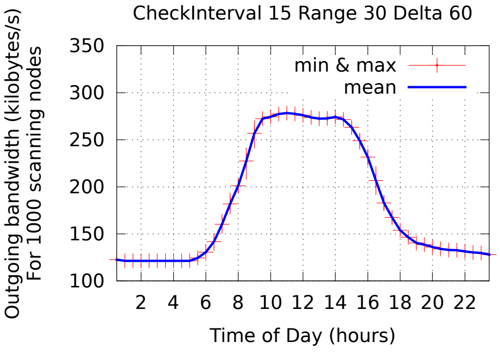

Figure 8: *24 hour bandwidth overview using Delta 60 ScanningInterval 15 Range 30 as configuration. The daily commute is visible, busiest time between 8 am and 4 pm*

The bandwidth requirements for a `Scanning Interval` of 15 seconds are 15 times less requiring only 3 mbit in comparison. This significant difference (40 mbit vs 3 mbit) makes the `Scanning Interval` of 15 seconds interesting. In Figure 8 we show the bandwidth for 24hours using 15 seconds as `Scanning Interval`. The daily commute into and out of the city is clearly visible, with more bandwidth used mid-day.

The SAT bandwidth requirements for configurations using `ScanningInterval` of 15 or higher are moderate, requiring less than 3 mbit of outgoing bandwidth per 1000 scanning nodes. It is our opinion that such bandwidth usage is already tolerable for current mobile phone networks, keeping in mind that the bandwidth capacity of mobile internet are steadily increasing due to high demand.

The SAT protocol traces a phone (device) with less than 15 meters accuracy in 30 seconds intervals. In 24 hours the SAT trace has a maximum average tracking gap of 10 minutes in an ideal simulated environment. Our simulations show that the results are all linearly connected. There is no threshold which drastically changes the results when reached. The opposite is true, the results degrade linearly if the configuration settings are changed towards less ideal settings.

7 Feasibility & open problems

In this section we present challenges that a real world implementation of our SAT protocol would face.

MAC address randomisation. The biggest issue is that the SAT protocol is designed to detect Wifi communications using the Wifi MAC address (BSSID) as unique identifier. This MAC address is static on current devices making it a suitable unique identifier for tracking. However the reliance of SAT on Wifi MAC addresses, make it vulnerable to MAC address randomisation or other techniques which prevent the MAC address from being sent over the air in plain.

Wifi protocol improvements have been proposed by Greenstein et al. [9] and Gruteser et al. [10] which would both directly counteract the SAT protocol by masking the MAC address, preventing it from getting sent in plain over the air. A user could also just change their Wifi MAC identifier and throw off the distributed SAT sensing network. As last resort the LEA can plant a probe which emits Wifi beacons to use for tracking if the tracked target changes their MAC address.

Listening on multiple frequencies at once. Current smartphones while powerful and versatile are unable to listen to all common Wifi channels at once. As such Wifi probing requests could be missed. If there is steady traffic flow between the target Wifi device and an AP then detection, if within reception range, is guaranteed. Canlar et al [5] state that scanning takes 550 milliseconds per channel, giving a total scanning time of just over 6 seconds.

We are unsure if Wifi devices looking for Wifi networks will send beacon requests at high interval to give a high chance of detection. Since a node would be only listening 550 milliseconds per channel it is unclear how high the chances are for detection. Further research needs to be done to find out how many beacon requests an idle Wifi device sends. The 801.11 standard [2] on page 421 explain that Wifi probes get sent less when other Wifi devices send probes.

A low level hardware approach needs to be taken to really find out how high the probability is that a scanning node detects another node during the 550 millisecond passive scan window. For our simulation we assumed that detection is guaranteed if within range, however this assumption may not hold true in the real world. Hence why we suggest to research this on a hardware level to find out how likely detection is given close proximity.

Battery Life. Until battery capacity increases significantly it can be hard to convince users to install an App to become part of the distributed sensing network. Due to restricted battery life on smartphones at the moment it would be hard to convince users to install the SAT application even with good incentives, as proposed in [5] and [11]. Technical users may be reluctant to install such an App due to the potential battery drain it can cause.

A hardware implementation on smartphones could force everyone to become part of the SAT network.

Intercepting Wifi channels. It is not clear if every mobile phone has the capability to *monitor* Wifi channels. For example we tried monitoring using a laptop running Ubuntu 12.04, however either the Wifi chip or its drivers prevented us from monitoring surrounding Wifi traffic.

Distribution of power. The privacy preserving aspects of SAT lie in the way the data and the witnesses are protected. While the security and privacy do not play a huge role in this paper it is an important design goal of SAT and deserves some explanation.

The location data inside the GLMs are encrypted using the random private key fetched. This encryption protects the witnesses privacy, ensuring the LEA cannot trace everyone since they would require the decryption keys.

The CA on the other hand has the decryption keys, which makes it important that the DS and the CA are controlled by 2 independent parties, to divide the power. The DS which contains the encrypted data are controlled by the LEA. The Judicary(Judges) control the SAT smartphone app implementation, and the CA infrastructure. Judges themselves won't be able to maintain it, but an independent employee who works on behalf of the judges and works in their interest has to maintain the CA.

It is important that the Judges (CA) and LEA (DS) do not conspire together, as this would effectively reveal the location from everyone, witnesses and targets alike. The boundaries of the LEA and CA have to be strictly adhered to, in the implementation, as otherwise there would be no privacy.

So as can be seen in Figure 1, the Judges literally hold the key (and the cryptographic keys too) to allow or deny the LEA's tracking requests. The LEA cannot use the data on the DS without the decryption keys, for which they need the Judges approval. This division of power using cryptographic protections gives SAT its privacy preserving qualities. If the division of power is not correctly implemented, then there is no privacy at all, so correct implementation is crucial.

8 Conclusion

The SAT protocol is a distributed tracking network alternative offering higher accuracies compared to GSM network based localisation tracking. Our simulation study shows that in an ideal simulated environment SAT can offer accuracies of under 15 meters. Smartphones have a self-positioning deviation of 25 meters on average, and even if we add the self-positioning deviation in full the SAT protocol will show accuracies of 40 meters or better.

The bandwidth requirements of SAT are reasonable, using less than 3 mbit per 1000 scanning nodes. Today's mobile phone networks should be able to cope with such a bandwidth consumption. As the mobile phone networks improve their capacities, in future a deployment of SAT will not significantly impact the mobile phone networks. Video or other media usage patters will consume a lot more bandwidth in comparison.

The feasibility of implementing SAT in a real-world scenario is unclear, even after our work. The implementation itself is not the concern. It is however unclear how high the detection chances are given close proximity of two smartphones. If both have Wifi enabled and one of the two smartphones has the SAT application installed and running, how likely is it that SAT detects the other smartphone? A Wifi enabled device, which is currently not logged into an AP may not send beacons fast enough for SAT to have a high chance of detection the other smartphone's Wifi communications. We suggest for further research to be done to find out how likely detection is on a low level hardware point of view.

The accuracies which SAT can offer are very interesting mainly because SAT relies on short range radio frequency detection (Wifi). GSM networks on the other hand have a higher communication range which makes it harder for them to compute a highly accurate position for a phone. The communication range of GSM is higher than the Wifi communication range, which makes Wifi the more suitable technology for positioning. Wifi-self positioning is a good example for this, achieving accuracies of 25 meters. If the same self-positioning technique were usable for GSM, the accuracies would be worse due to the increased communication range and reduced amount of Base Stations available compared to Wifi.

References

[1] *UDel Models simulator: http://udelmodels.eecis.udel.edu/.*

[2] *Ieee standard for information technology - telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements - part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications*, IEEE Std 802.11-2007 (Revision of IEEE Std 802.11-1999), (2007), pp. 1 –1076.

[3] S. Al-Kuwari and S. D. Wolthusen, *A survey of forensic localization and tracking mechanisms in short-range and cellular networks*, in Digital Forensics and Cyber Crime, vol. 31 of Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Springer Berlin Heidelberg, 2010, pp. 19–32.

[4] P. Bahl, V. N. Padmanabhan, and A. Balachandran, *Enhancements to the radar user location and tracking system*, Microsoft Research, (2000).

[5] E. Canlar, M. Conti, B. Crispo, and R. Di Pietro, *Sense-and-trace: A privacy preserving distributed geolocation tracking system*, Security Protocols XX, (2012), pp. 199–213.

[6] R. Cayford and T. Johnson, *Operational parameters affecting the use of anonymous cell phone tracking for generating traffic information*, 1 (2003).

[7] Y.-C. Cheng, Y. Chawathe, A. LaMarca, and J. Krumm, *Accuracy characterization for metropolitan-scale wi-fi localization*, in Proceedings of the 3rd international conference on Mobile systems, applications, and services, MobiSys '05, New York, NY, USA, 2005, ACM, pp. 233–245.

[8] X. Fu, N. Zhang, A. Pingley, W. Yu, J. Wang, and W. Zha, *The digital marauder's map: a wifi forensic positioning tool*, in IEEE Transactions on Mobile Computing, Volume: 11, Issue: 3, IEEE, March 2012, pp. 377–389.

[9] B. Greenstein, D. McCoy, J. Pang, T. Kohno, S. Seshan, and D. Wetherall, *Improving wireless privacy with an identifier-free link layer protocol*, in Proceedings of the 6th international conference on Mobile systems, applications, and services, MobiSys '08, New York, NY, USA, 2008, ACM, pp. 40–53.

[10] M. Gruteser and D. Grunwald, *Enhancing location privacy in wireless lan through disposable interface identifiers: a quantitative analysis*, Mob. Netw. Appl., 10 (2005), pp. 315–325.

[11] N. Husted and S. Myers, *Mobile location tracking in metro areas: malnets and others*, in Proceedings of the 17th ACM conference on Computer and communications security, CCS '10, ACM, 2010, pp. 85–96.

[12] A. Karlson, B. Meyers, A. Jacobs, P. Johns, and S. Kane, *Working overtime: Patterns of Smartphone and PC Usage in the Day of an Information Worker.*, Springer, 2003, pp. 398–405.

[13] K. Lorincz and M. Welsh, *Motetrack: a robust, decentralized approach to rf-based location tracking*, Personal Ubiquitous Comput., 11 (2007), pp. 489–503.

[14] Z. Zhu and G. Cao, *APPLAUS: A Privacy-Preserving Location Proof Updating System for Location-based Services*, in Proceedings of the 30th IEEE International Conference on Computer Communications, IEEE INFOCOM '11, 2011.