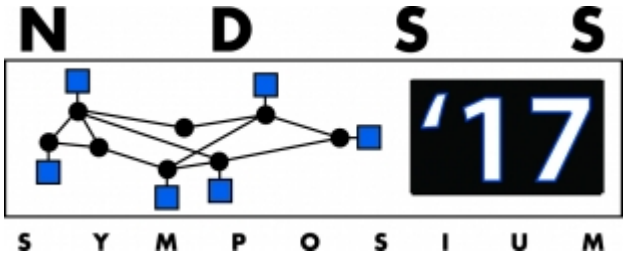


FBS-Radar: Uncovering Fake Base Stations at Scale in the Wild

Zhenhua Li, Weiwei Wang, Christo Wilson, Jian Chen, Chen Qian
Taeho Jung, Lan Zhang, Kebin Liu, Xiangyang Li, Yunhao Liu

Tsinghua University

百度移动安全 Mobile Security

UNIVERSITY OF CALIFORNIA SANTA CRUZ

lizhenhua1983@gmail.com
http://www.greenorbs.org/people/lzh/
Mar. 1st, 2017

Outline

1 Background

2 State of the Art

3 Our System

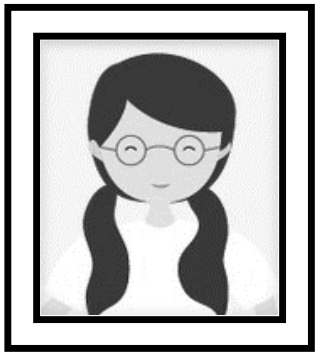
4 Locating FBSes

5 Summary

Story 1

SMS Text Message

From 95599 (Agriculture Bank of China):
We're processing the student loan you've applied for, and now requiring you to transfer a deposit of ¥9900 (≈ $1500) to the bank account XXXXXXXXX.



* Note: This is a simplified version of the actual story which involves more complex details.

Story 2

SMS Text Message

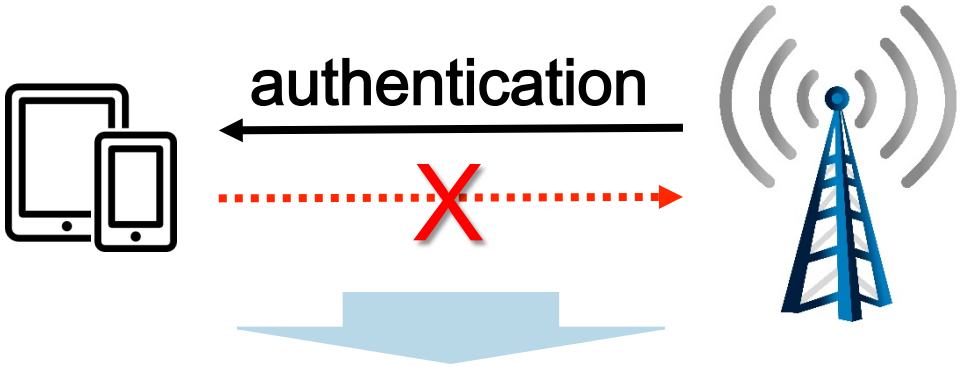
From 95566 (Bank of China):
We're processing the house mortgage for you. Please prepare ¥17,600,000 (≈ $2,600,000) ...

Fake Base Stations

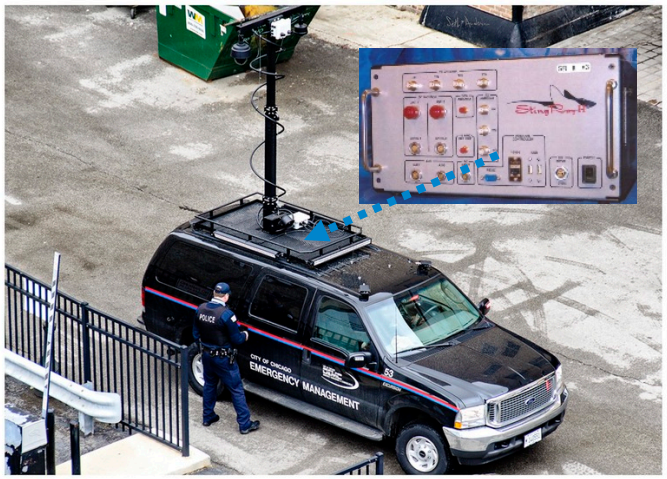
* Note: This is a simplified version of the actual story which involves more complex details.

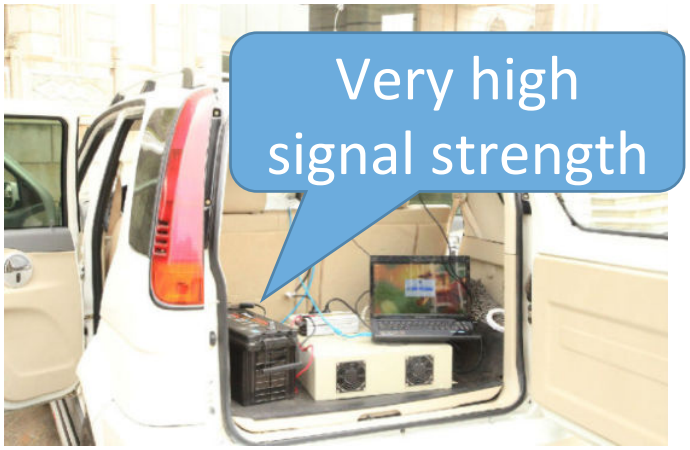
GSM (Global System for Mobile Communication)

	Birth Year	User Scale	Speed	Security
2G – GSM	1990	> 1 billion	Low	Poor
3G – CDMA	2008	< 2 billion	Middle	Middle
4G – LTE	2009	≈ 3 billion	High	Fine

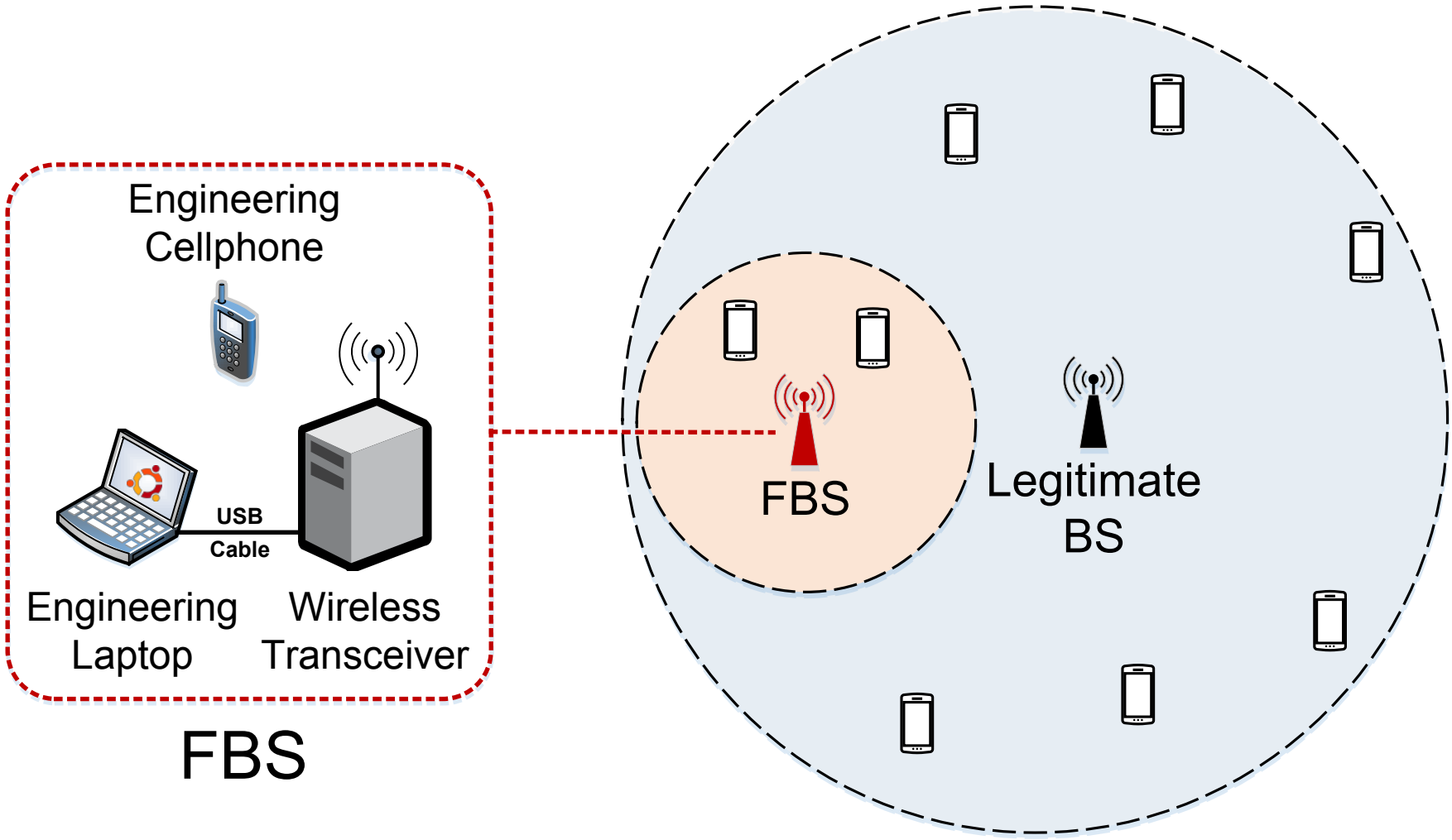


FBS Carrier

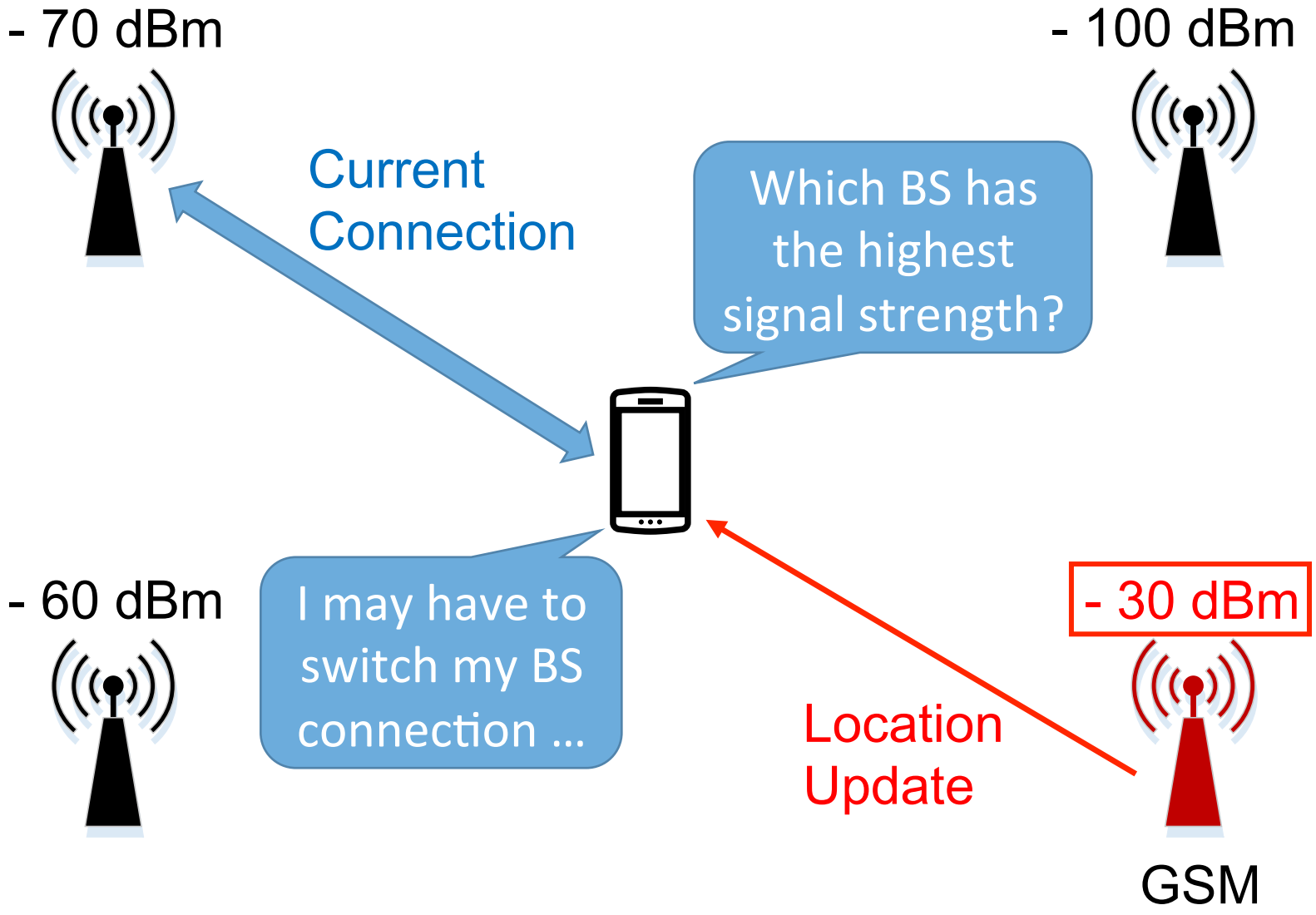




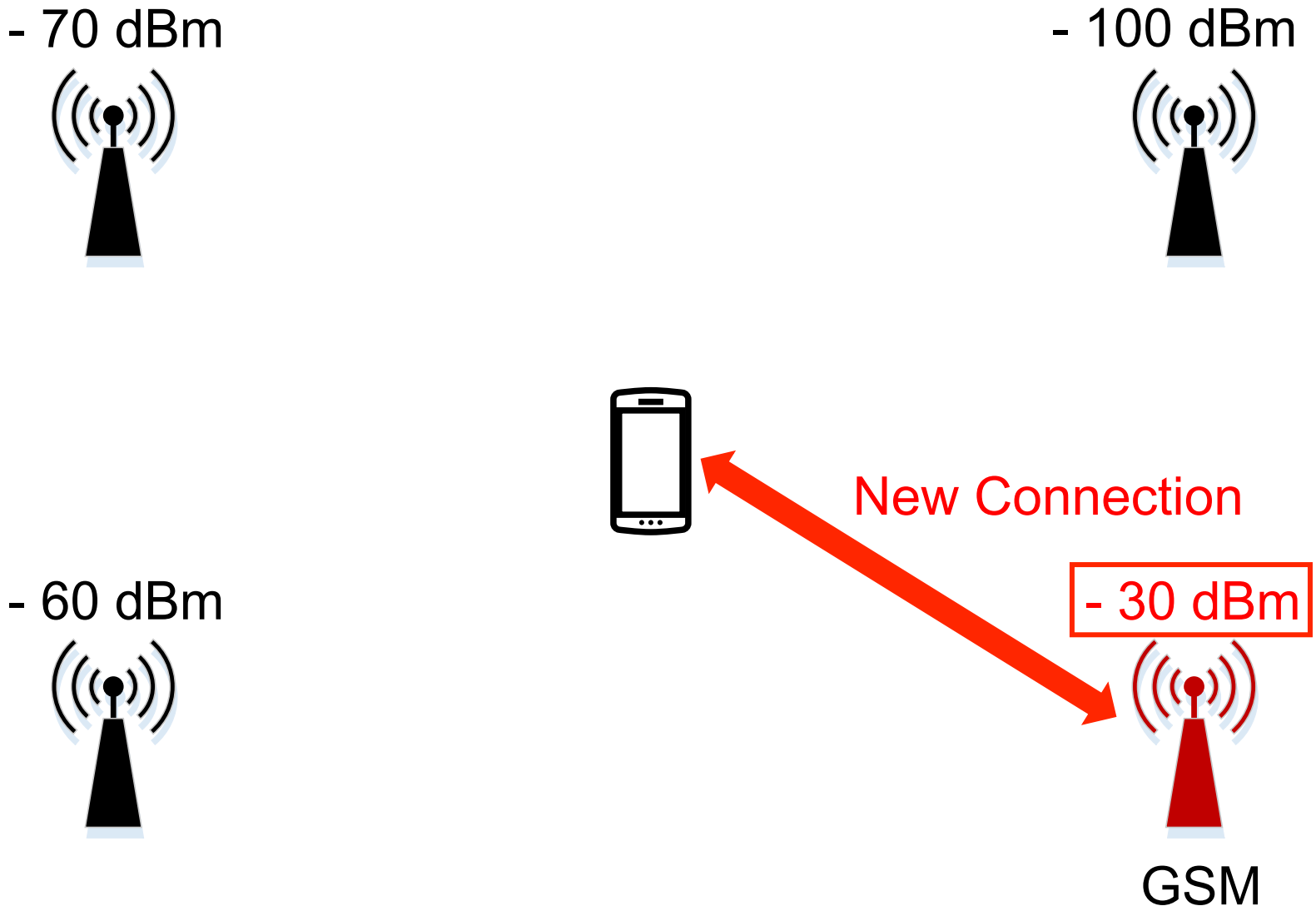
Fake Base Station (FBS)



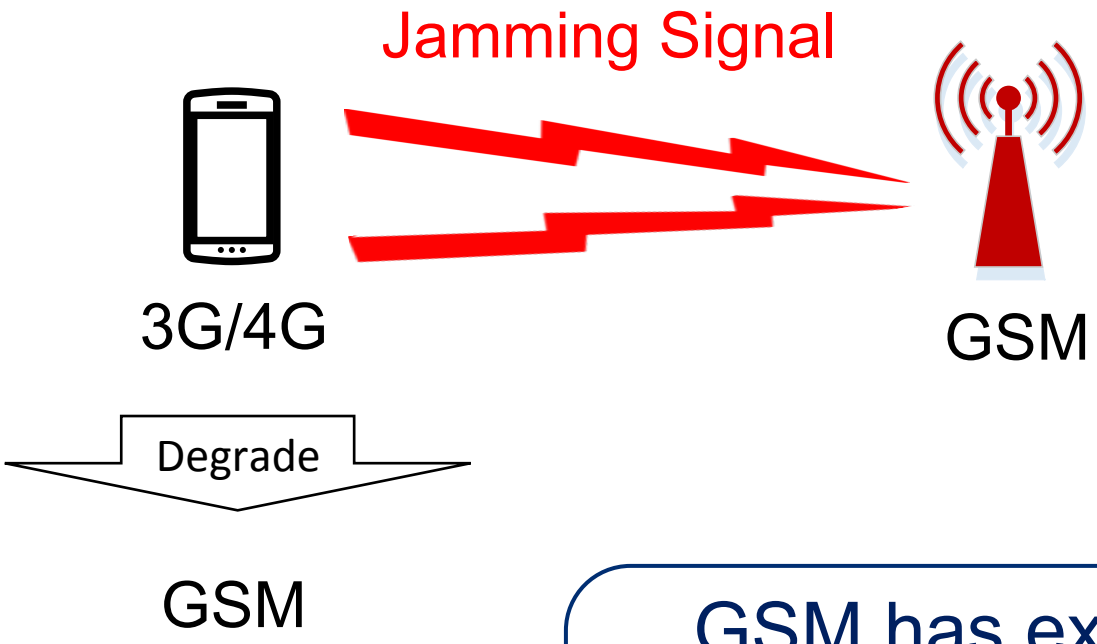
FBS Attack on GSM Phones



FBS Attack on GSM Phones

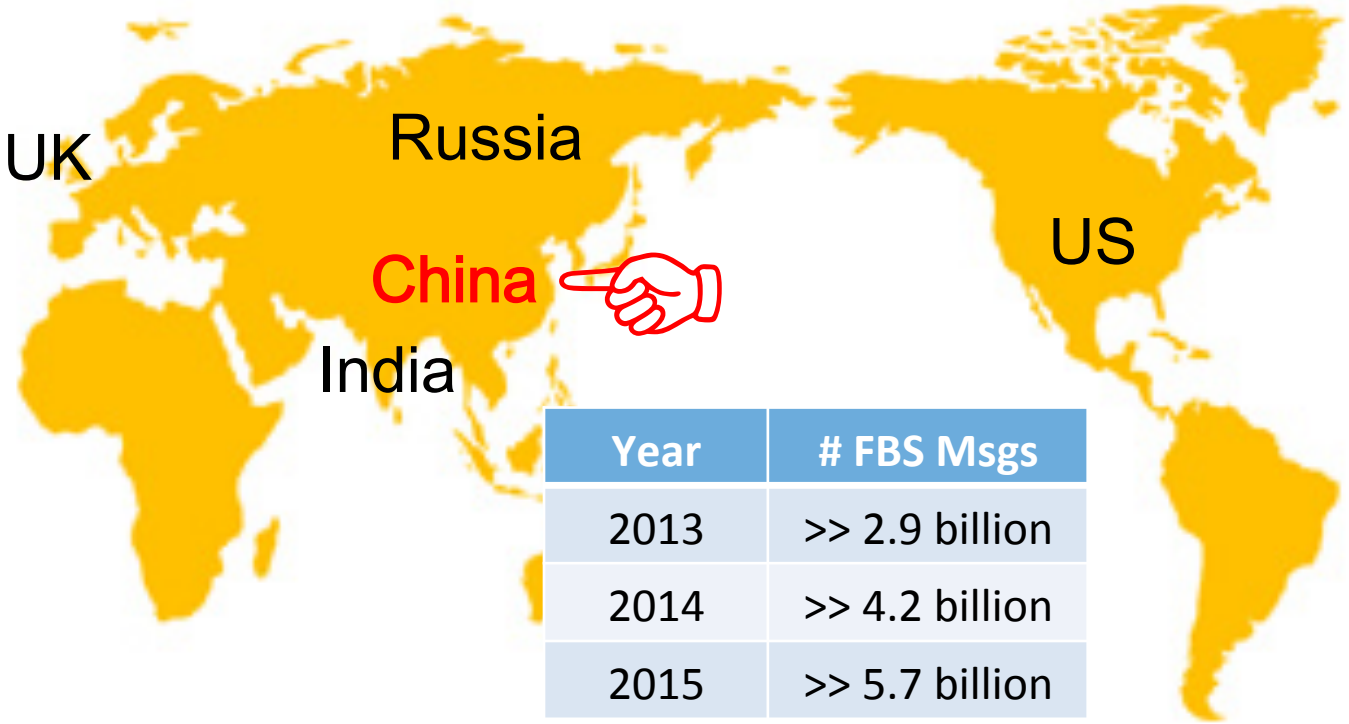


FBS Can Also Impact 3G/4G Phones



GSM has existed for many years, so abandoning GSM also needs many years …

FBS Attack Is NOT Hypothetical



Year	# FBS Msgs
2013	>> 2.9 billion
2014	>> 4.2 billion
2015	>> 5.7 billion

N * billion

FBS Industry in China

Device: $400

Daily income: $40

Device: $1000

Daily income: $70

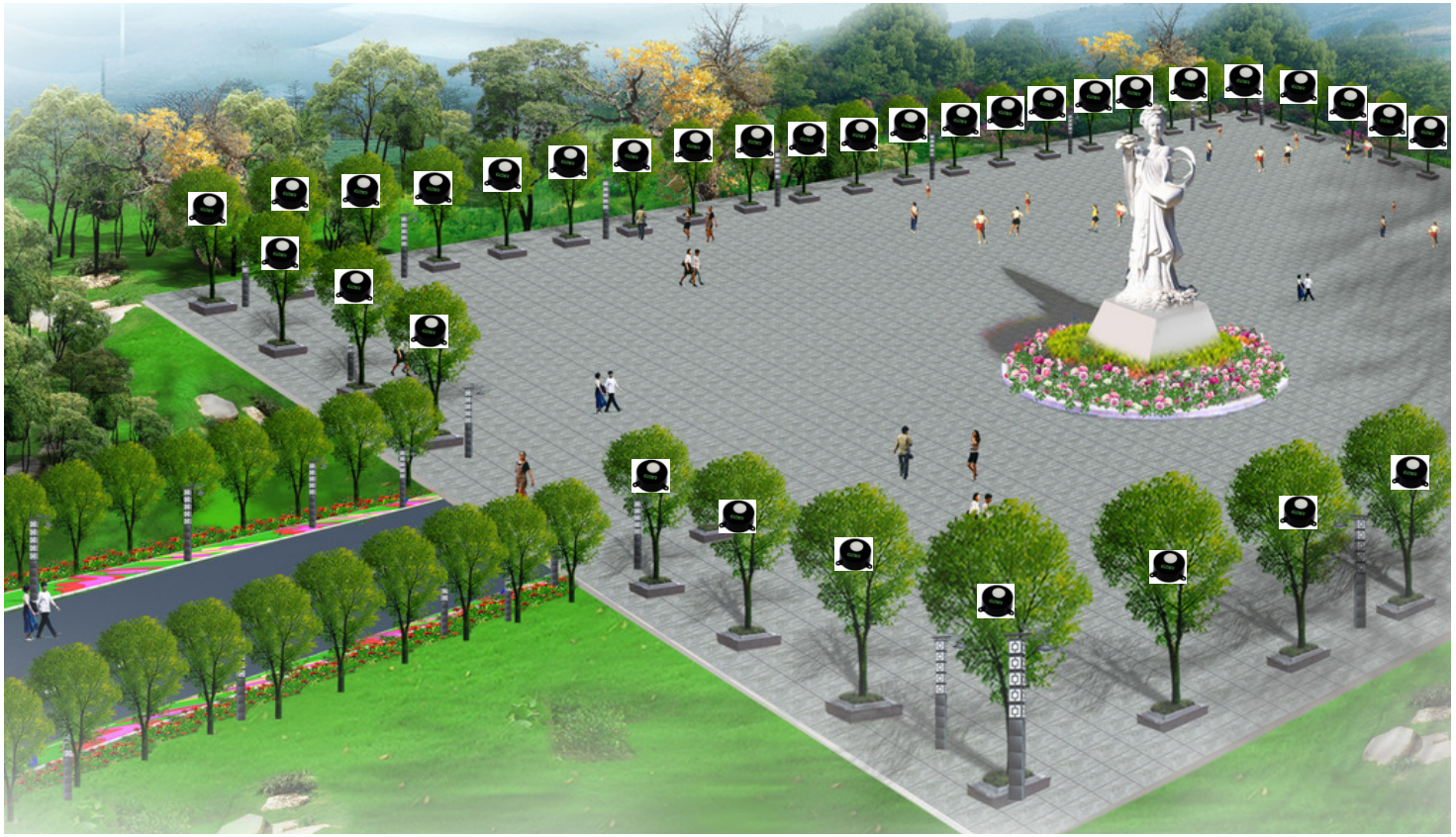
Device: $700

Daily income: up to $1400

FBS Industry in China

2 State of the Art

Electronic Fence



Huge infrastructure costs → Poor scalability

FBS-signal Detection Car

Random walk → Limited coverage & “dull”

User Reporting

Dial 12321

Most users don’t realize the existence of FBSes

Client-side Tools

SnoopSnitch

SnoopSnitch is an Android app that collects and analyzes mobile radio data to make you aware of your mobile network security and to warn you about threats like fake base stations (IMSI catchers), user tracking and over-the-air updates. With SnoopSnitch you can use the data collected in the GSM Security Map at gsmmap.org and contribute your own data to GSM Map.

CatcherCatcher

The CatcherCatcher tool detects mobile network irregularities hinting at fake base station activity.

Do they really work in large-scale practice? …

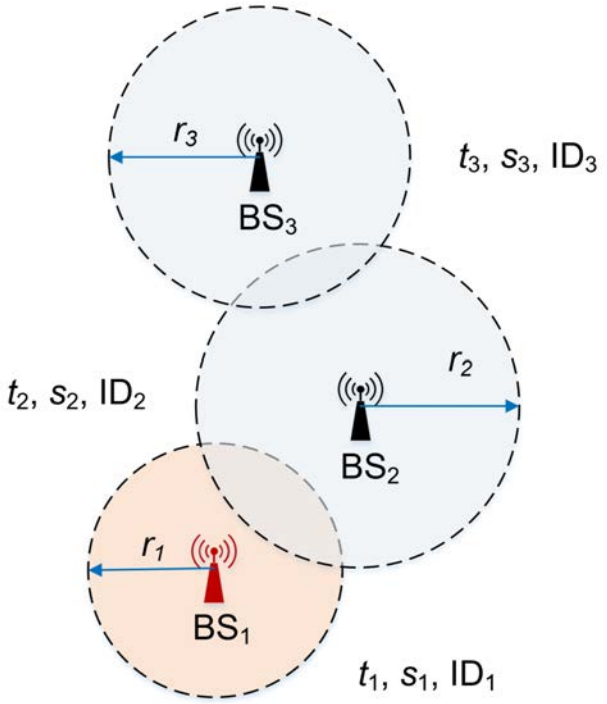
3 Our System: *FBS-Radar*

Baidu PhoneGuard Users Opt-in

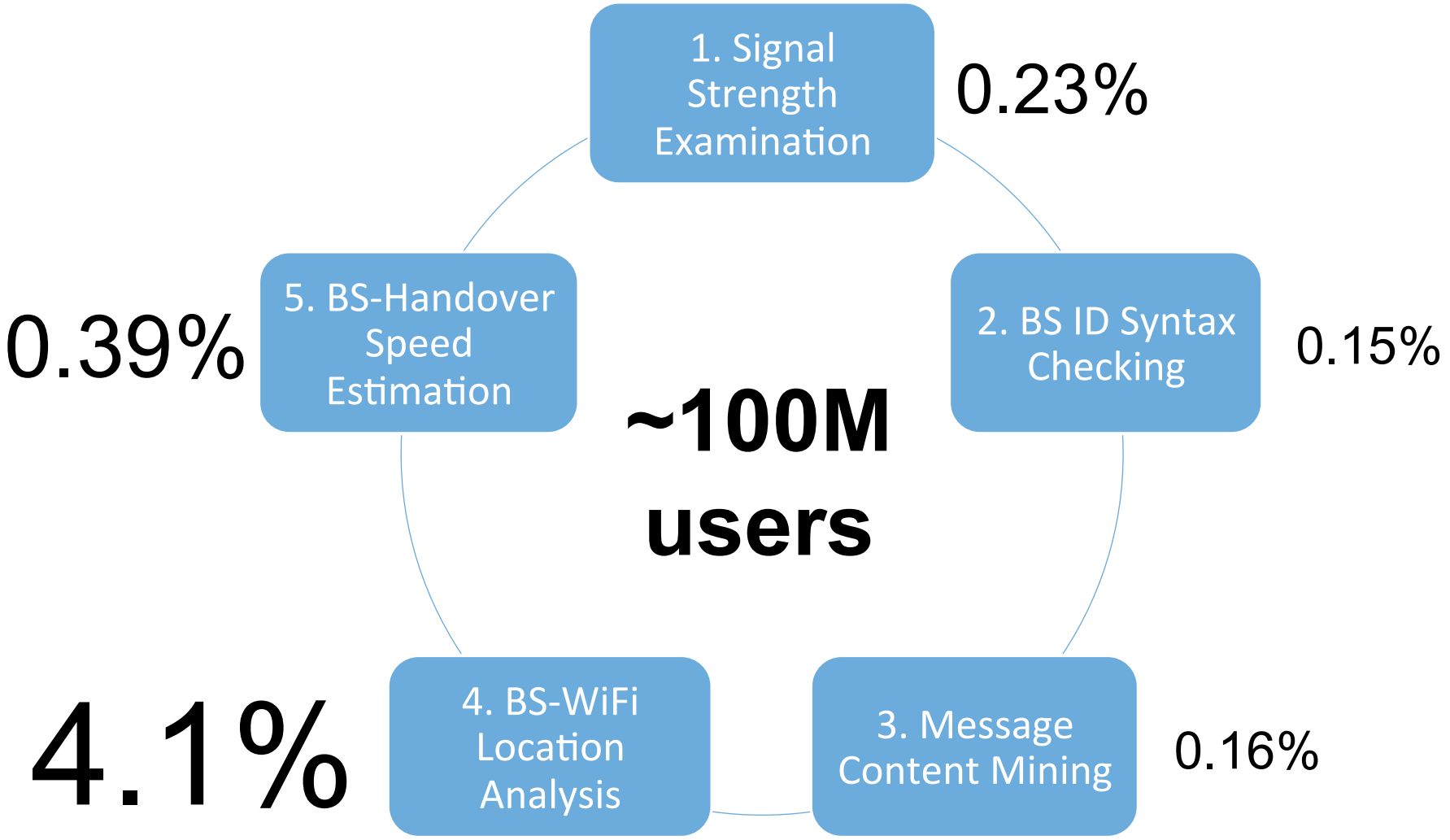
Report multiple fields of **suspicious** SMS messages

- Sender's number is not in the recipient's contact list
- Sender's number is an authoritative number

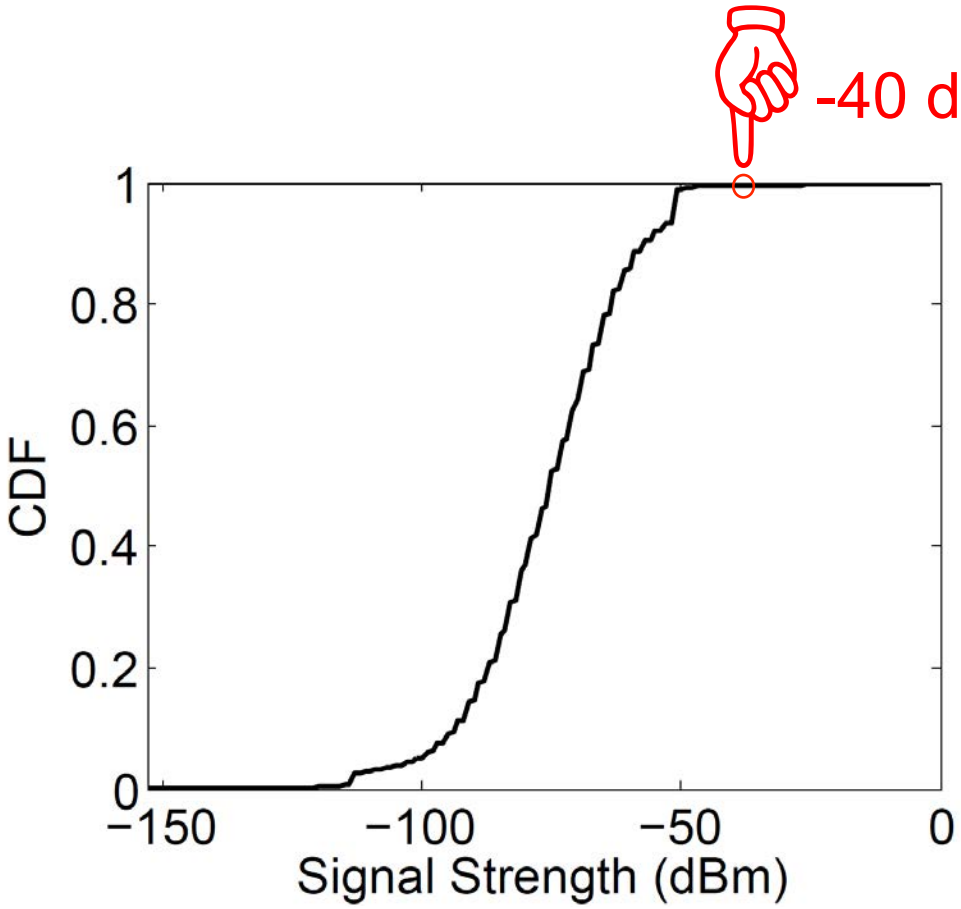
Field	Value
t_1	1452869570549
s_1	-79 dBm
ID_1	460-00-39185-21492
t_2	1452865343627
s_2	-84 dBm
ID_2	460-00-39185-52921
t_3	1452865278412
s_3	-95 dBm
ID_3	460-00-39185-52112
Sender's phone number	+86-135-5281-9836
Content of the message	$\leq$ 140 characters
MAC_1	ec:26:ca:26:f6:c0
MAC_2	d0:c7:c0:aa:6a:fc
...	...
MAC_n	6a:3e:34:03:d8:13

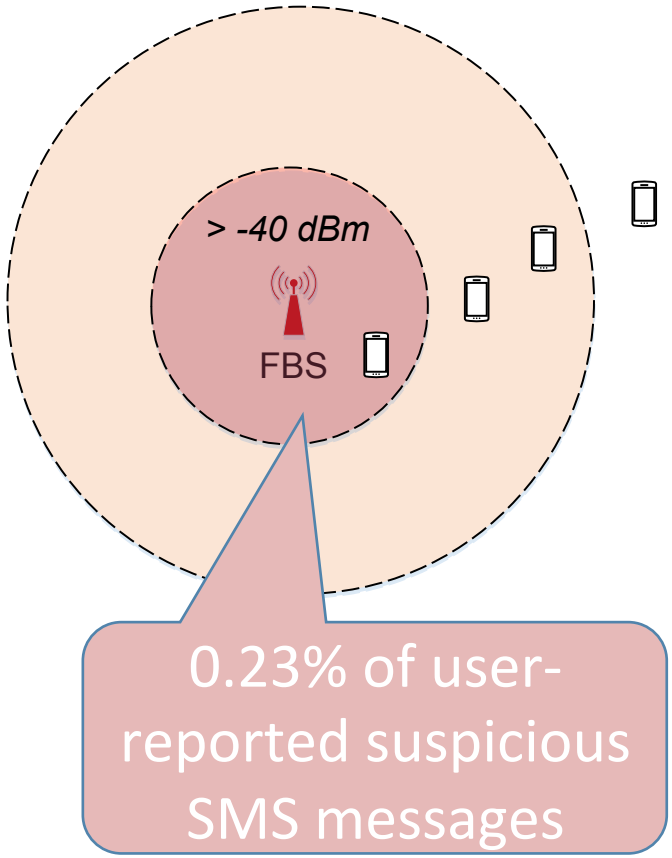


Five Methods



3.1 Signal Strength Examination





3.2 BS ID Syntax Checking

$$\text{BS ID} = \text{MCC} + \text{MNC} + \text{LAC} + \text{CID}$$

- MCC: Mobile Country Code, 3 digits
- MNC: Mobile Network Code, 2 digits
- LAC: Location Area Code, 16 bits
- CID: Cell Identity, 16 bits for 2G/3G and 28 bits for 4G

0.15% of suspicious messages were sent by BSes with syntactically invalid IDs

3.3 Message Content Mining

- **Bag-of-words SVM (Support Vector Machine) classifier** trained on 200,000 hand-labeled SMS messages.
  1. Labelling suspicious messages;
  2. Word segmentation;
  3. Feature extraction;
  4. Quantizing the feature vector;
  5. Training the SVM model;
  6. Preprocessing the test set;
  7. SVM classification of the test set.

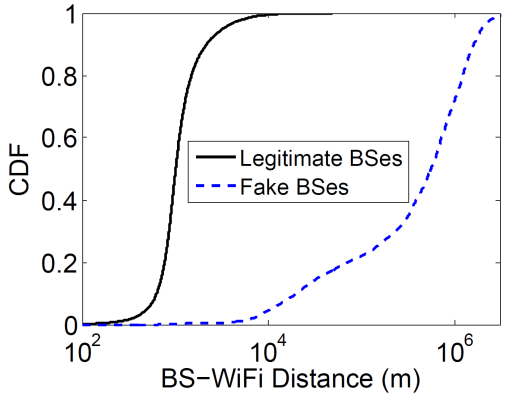
- Computation intensive
- Violation of user privacy

0.16% of suspicious messages came from authoritative phone numbers and were determined to contain fraud text content

3.4 BS-WiFi Location Analysis

Field	Value
t_1	1452869570549
s_1	-79 dBm
ID_1	460-00-39185-21492
t_2	1452865343627
s_2	-84 dBm
ID_2	460-00-39185-52921
t_3	1452865278412
s_3	-95 dBm
ID_3	460-00-39185-52112
Sender's phone number	+86-135-5281-9836
Content of the message	$\leq$ 140 characters
MAC_1	ec:26:ca:26:f6:c0
MAC_2	d0:c7:c0:aa:6a:fc
...	...
MAC_n	6a:3e:34:03:d8:13

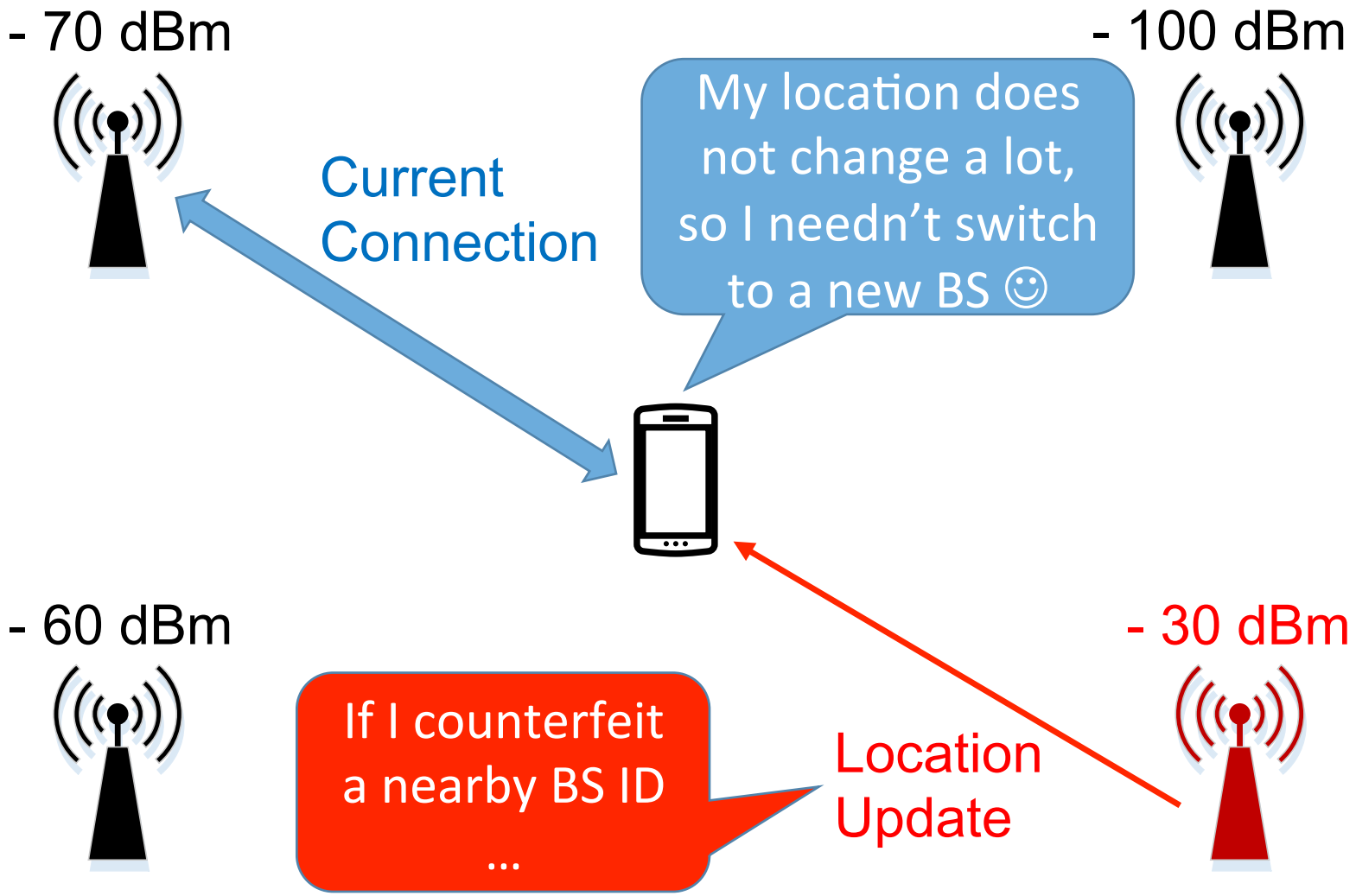
BS Location



User WiFi Location

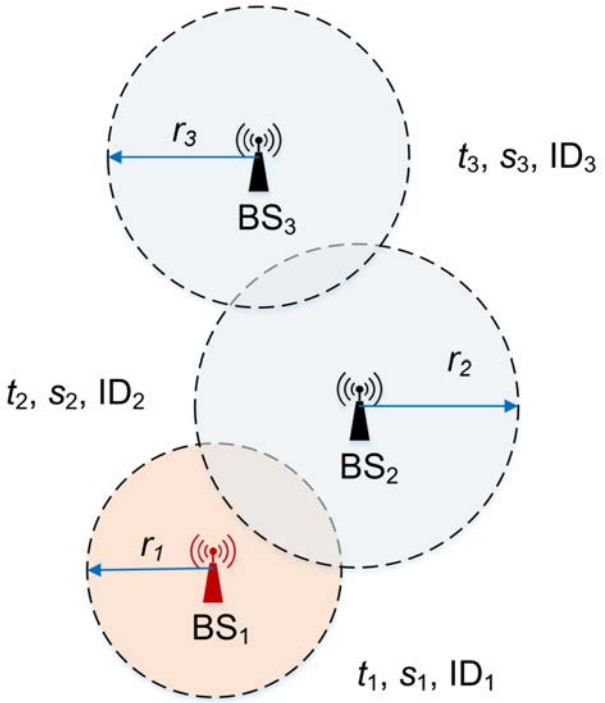
4.1% of suspicious messages were sent by BSes that were not in their correct geolocation, i.e., they were spoofing the ID of a legitimate but distant BS.

3.4 Counterfeiting a Nearby BS ID



3.5 BS-Handover Speed Estimation

- For BS-WiFi location analysis, what if the WiFi location information is not available?



$$V_{1,2-max} = \frac{d_{1,2} + r_1 + r_2}{t_1 - t_2},$$

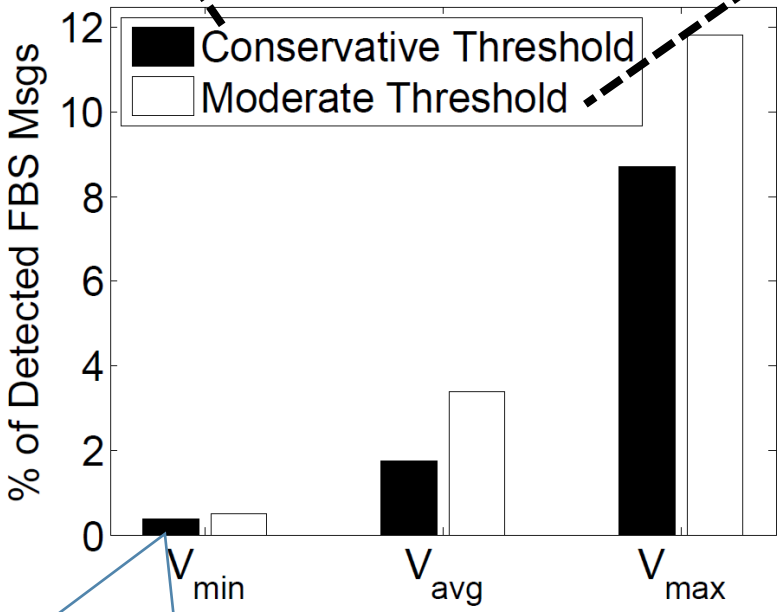
$$V_{1,2-avg} = \frac{d_{1,2}}{t_1 - t_2},$$

$$V_{1,2-min} = \begin{cases} \frac{d_{1,2} - r_1 - r_2}{t_1 - t_2} & \text{when } d_{1,2} > r_1 + r_2, \\ 0 & \text{when } d_{1,2} \leq r_1 + r_2, \end{cases}$$

4.5 BS-Handover Speed Estimation

$$threshold_{CRH} = 350\,km/h,$$

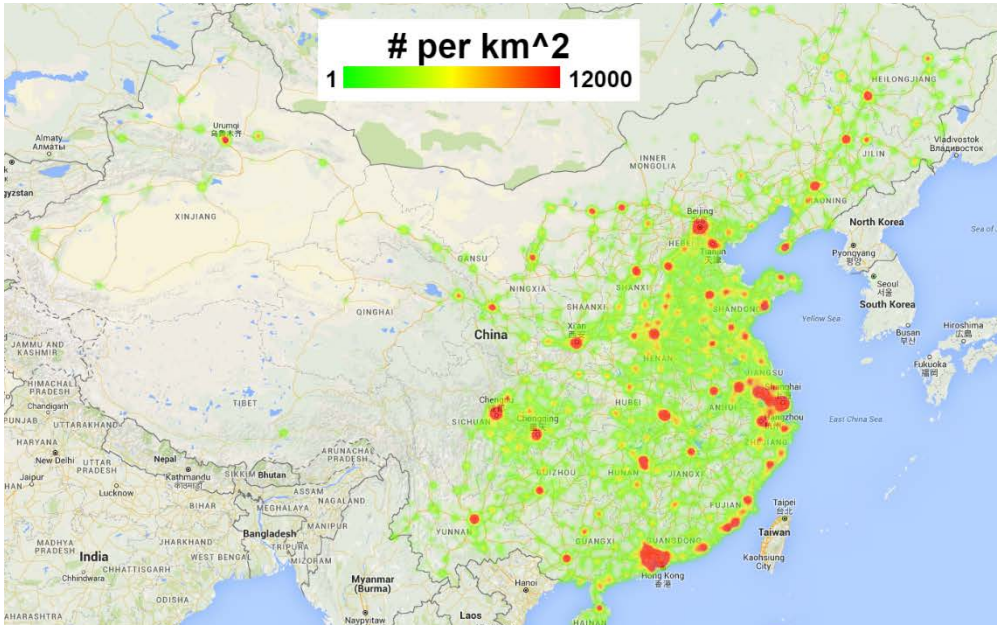
$$threshold_{Highway} = 150\,km/h,$$



>> 0.39% of suspicious SMS messages come from FBSes

Detection Performance

- **> 4.7%** of suspicious messages should have come from FBSes
  - False positive rate is only 0.05% (according to user feedback), mainly due to the inaccuracy of our WiFi database



- Set-3 (by message content mining) is >98% covered by the other 4 sets
  - **No need to collect the text content of users' messages!**

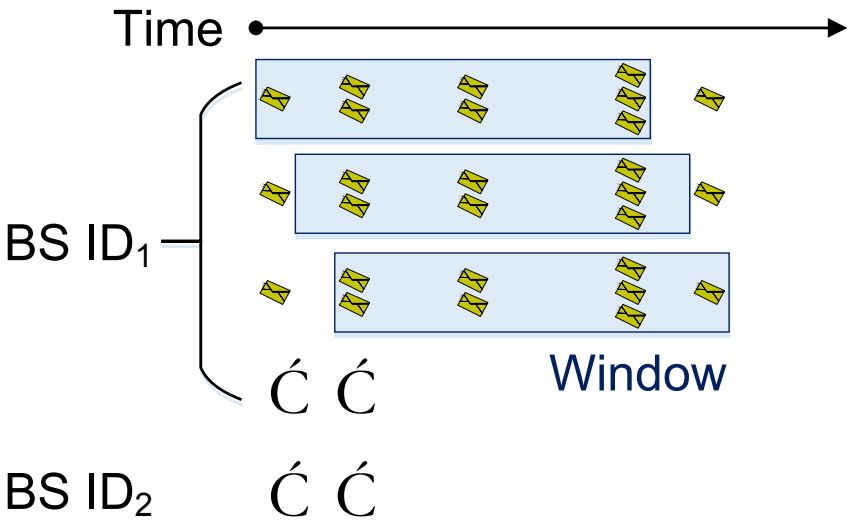
Arresting FBS Operators

- With the help of FBS-Radar, the police have arrested tens to hundreds of FBS operators every month

4 Locating FBSes

Locating FBSes based on User Device Locations

- FBSes frequently move and change their IDs
  - We take both **temporal** and **spatial** locality into account



Only those FBS messages

1) using the same BS ID,

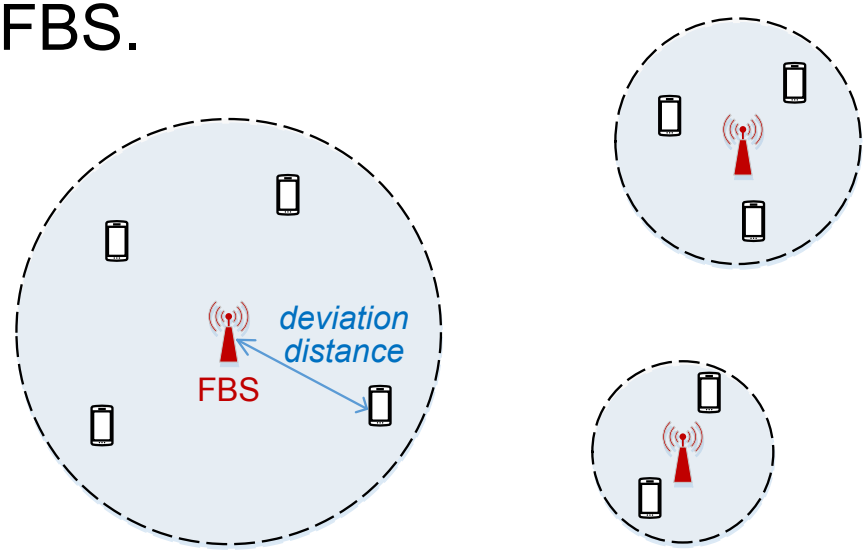
2) happening in the same **time window**,

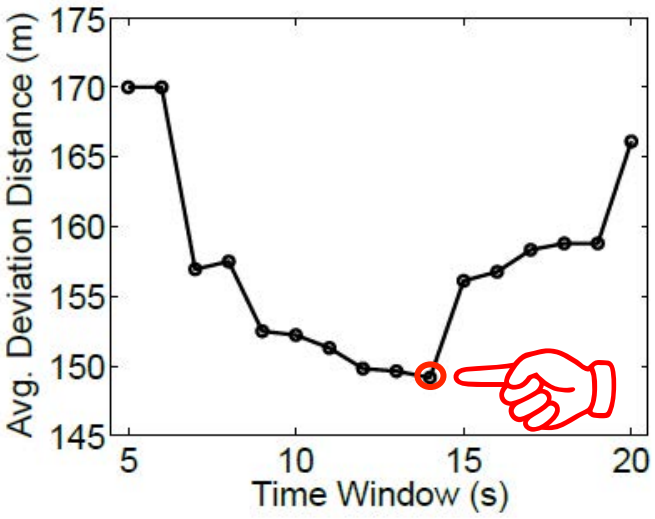
and 3) located in the same spatial cluster

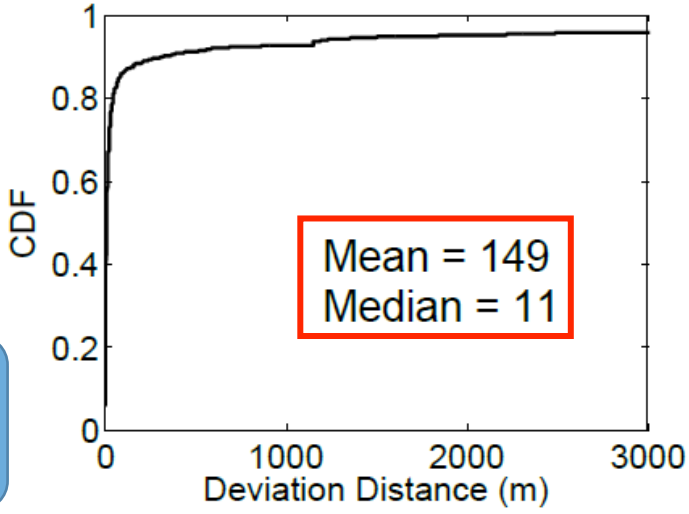
can be attributed to one FBS.

Locating FBSes based on User Device Locations

- The centroid of **every** cluster is the estimated location of an FBS.





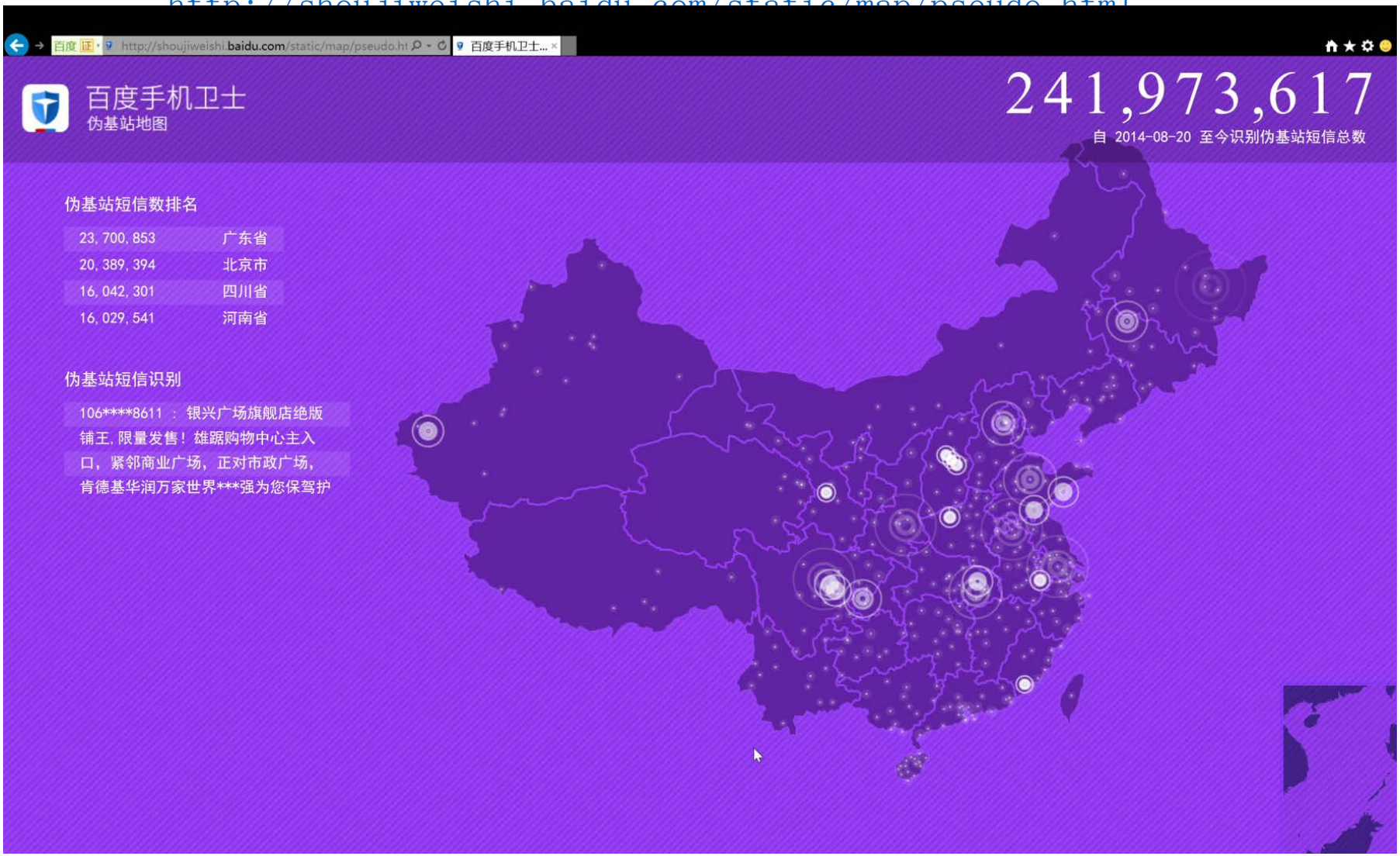


This location accuracy is sufficient for us to track FBSes!

Real-time Locations of FBSes

Public URL →

http://shoujiweishi.baidu.com/static/map/pseudo.html



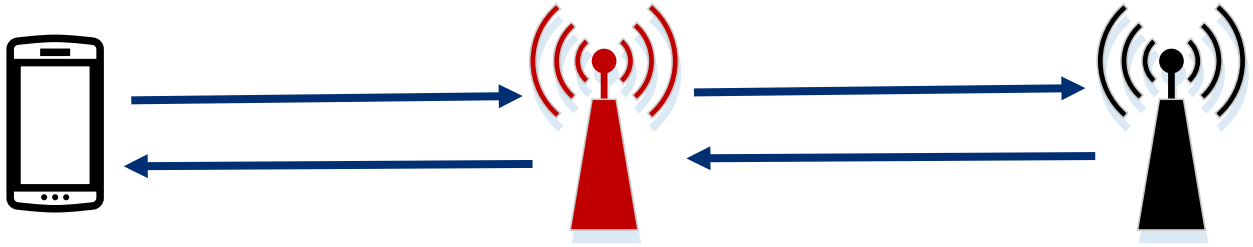
5 Summary

- Using extensive crowdsourced data, we evaluate five different methods for detecting FBSes in the wild, and find that FBSes can be precisely identified without sacrificing user privacy.
- We present a reasonable method for locating FBSes with an acceptable accuracy.
- FBS-Radar is currently in use by ~100M people. It protects users from millions of malicious messages from FBSes every day, and has helped the authorities arrest numerous FBS operators every month.

Backup slides

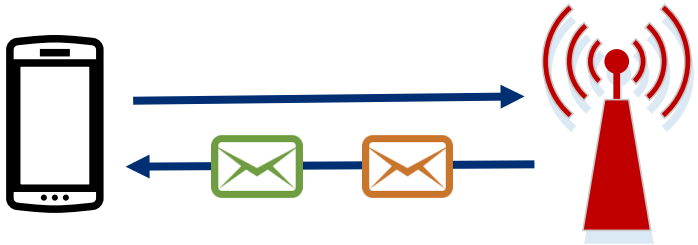
FBS Attack: Passive vs. Active

Passive: IMSI-catcher



Rarely reported in China, but sometimes reported in the US

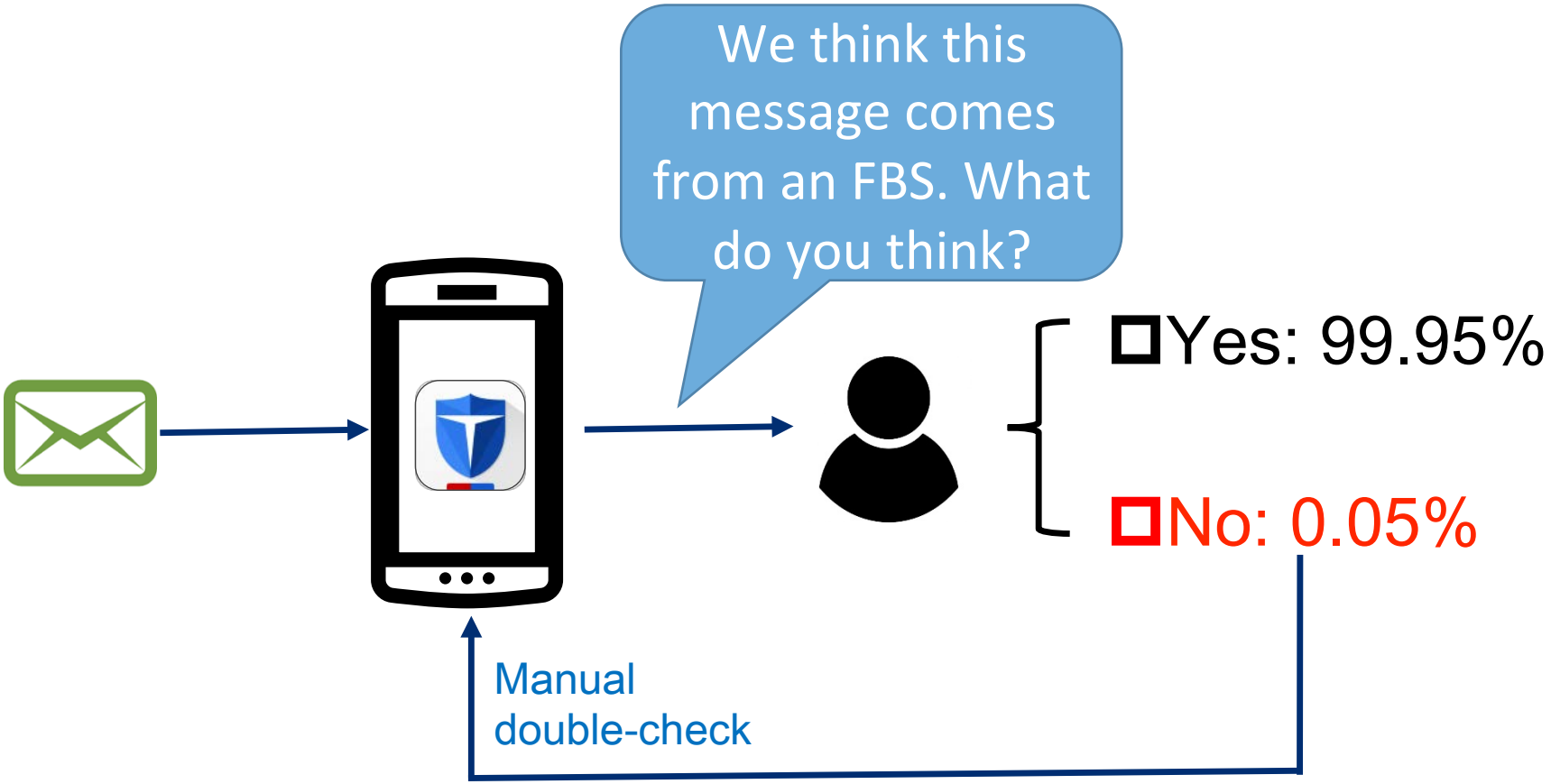
Active: Push spam/fraud SMS messages with spoofed phone numbers



Year	# FBS Msgs
2013	>> 2.9 billion
2014	>> 4.2 billion
2015	>> 5.7 billion

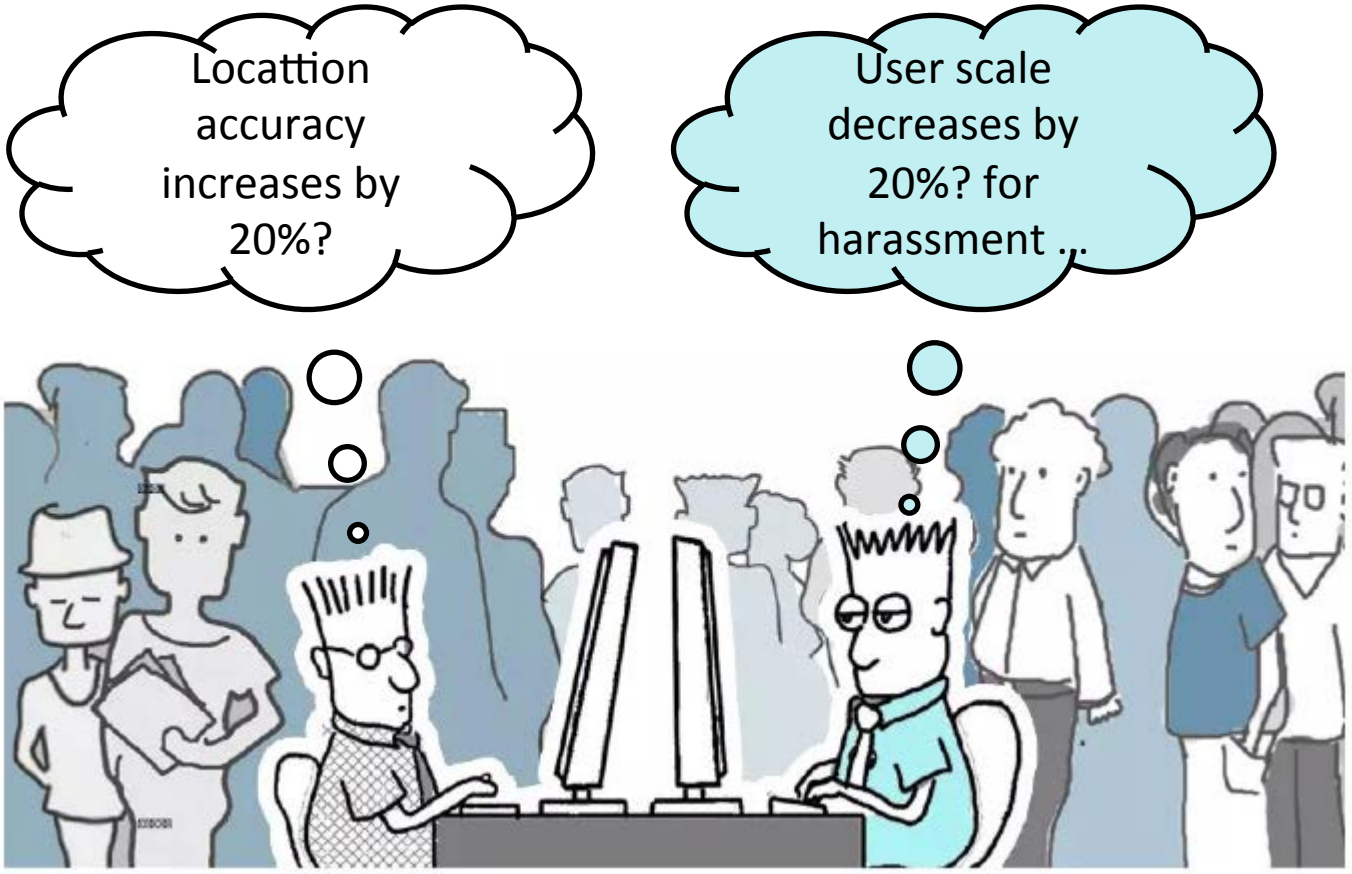
Ground Truth

- Our ONLY ground truth comes from users' feedback



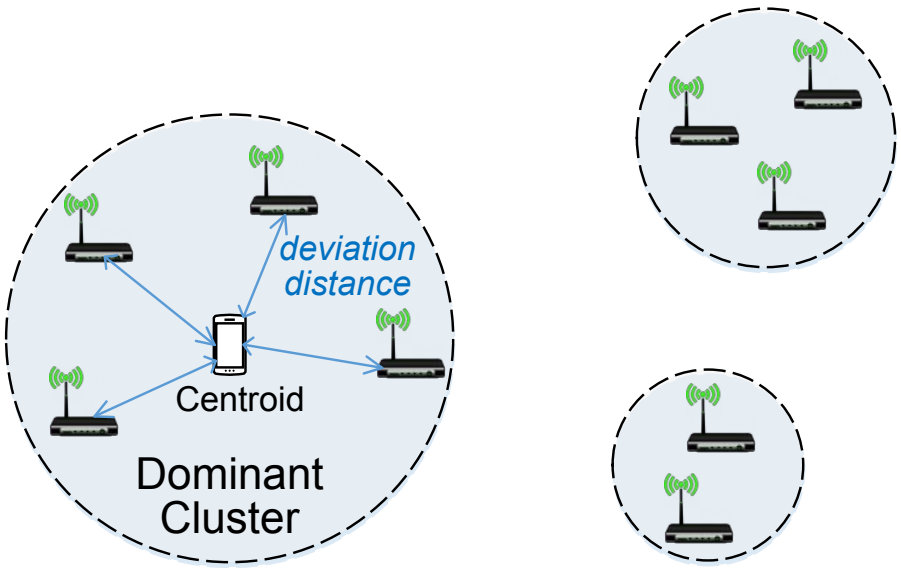
Why not use GPS?

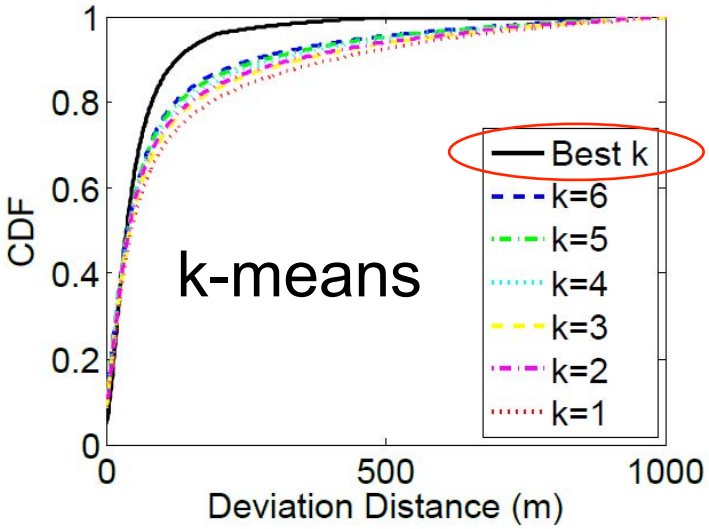
- Most people turn GPS off in most time to save battery, so we have to ask users for GPS privilege

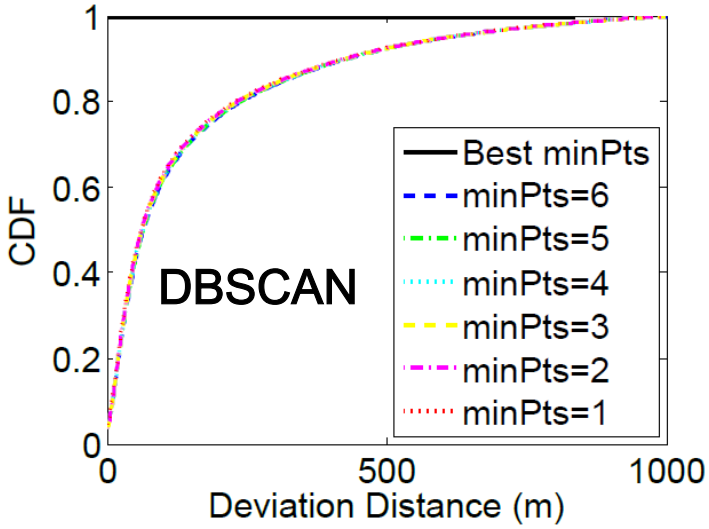


Localizing User Devices based on WiFi Information

- The centroid of the **dominant** cluster is the estimated location of the user device







Spam and Fraud SMS Messages

Fraud

"Dear user, you are lucky to be the winner of this month's big award! You will be offered 10-GB FREE 4G traffic by clicking on this URL: http://www.10086award.com." --- sent from 10086 (China Mobile).

Spoofed phone numbers

"Dear customer, you have failed to pay for this year's management fee of 100 dollars. If you do not pay for it before Jul. 30th, you will face a fine of 500 dollars. You should pay it by transferring money to the following bank account: ..." --- sent from 95533 (Bank of China).

Spam (Ads)

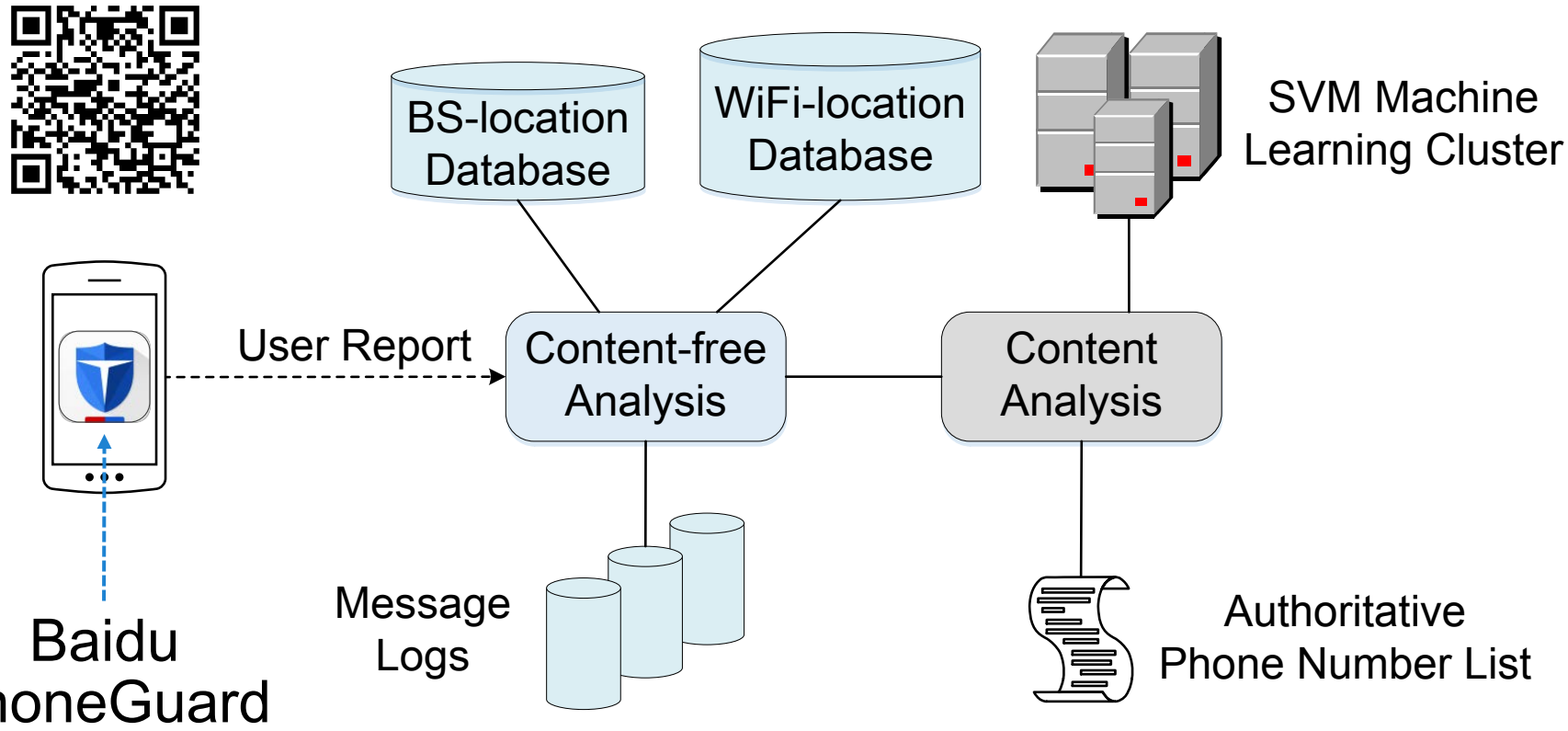
"We are selling excellent, cheap goods and food from Jul. to Aug. 2016. Visit our shops at the People's Square as soon as possible!" --- sent from a (usually not well-known) mart or grocery.

"We provide very cheap and legal invoices that can help you quickly make a big fortune. Don't hesitate, dial us via the phone number: 010-61881234!" --- sent from a (usually not well-known) company.

FBS-Radar: 4-fold Design Goals

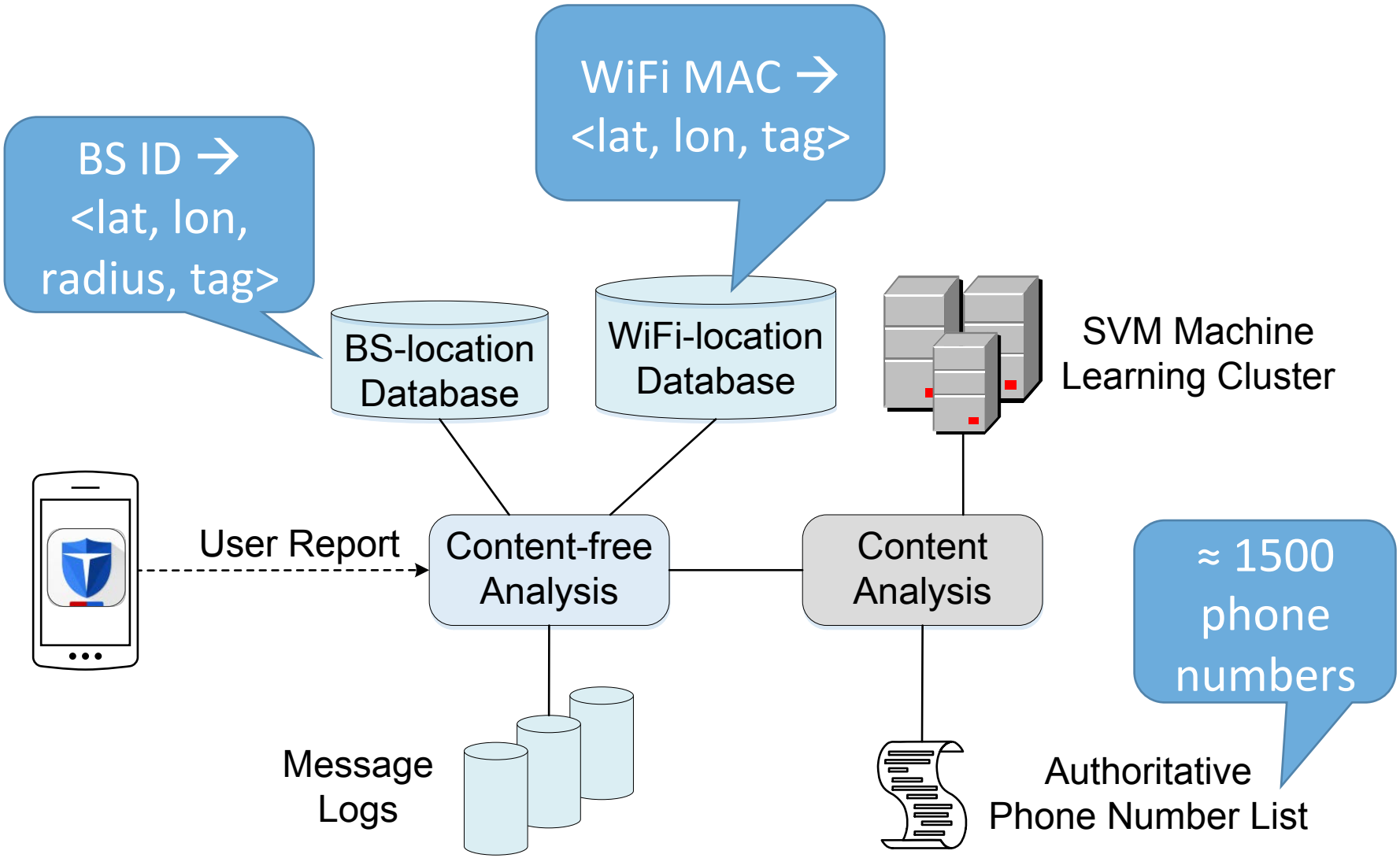
- Detect as many FBSes as possible with very few false positives, without specialized hardware
- Automatically filter spam/fraud FBS messages from user devices with a high precision
- Provide actionable intelligence about geolocations of FBSes to aid law enforcement agencies
- Use minimal resources on client side, minimize collection of sensitive data, and not require root.

FBS-Radar & Baidu PhoneGuard

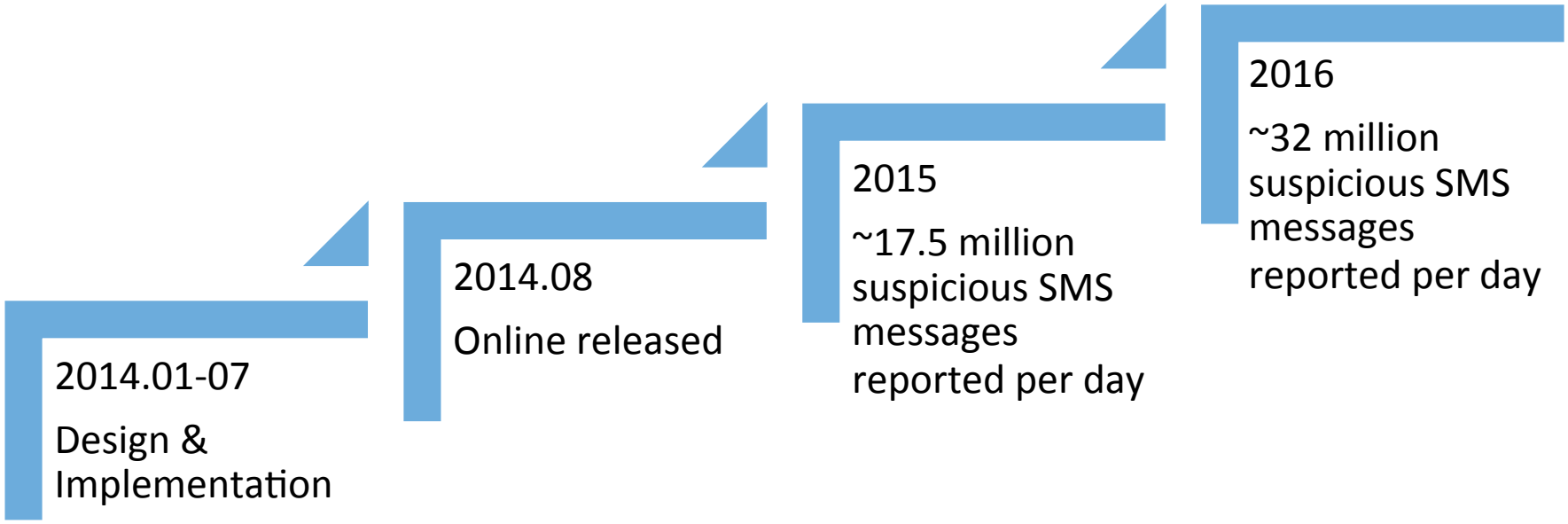


Crowdsourced data from ~100 Million Users

Database and List



FBS-Radar: Timeline



Informed Consent from Users

3.1 百度手机卫士软件及服务是百度公司向广大用户提供的安装在移动电话等移动设备终端上的提供全面安全保护的软件及服务，其提供的主要功能包括但不限于手机加速、垃圾清理、应用管理、防骚扰、防吸费、流量监控、病毒查杀、安全市场等。根据产品功能特点，百度公司可能收集以下数据：	3.1 Baidu PhoneGuard provides smartphone users with comprehensive security protections, such as smartphone acceleration, garbage cleaning, app management, anti-spam, anti-phishing, traffic monitoring, anti-virus, secure marketing, and so forth. To achieve specific functions and services, Baidu PhoneGuard may collect the following data from users:
……	……
3.1.4 防骚扰功能可以帮助您拦截垃圾信。在判断短信是否需要拦截时，百度手机卫士可能需要读取用户手机中的联系人名单进行比对。为了智能识别过滤垃圾短信，百度手机卫士可能需要对陌生号码的短信内容进行特征分析，若短信内容中包含垃圾短信特征，则对该短信进行拦截。	3.1.4 The anti-spam service (offered in part by FBS-Radar) can help users detect spam/fraud SMS messages. During the detection, Baidu PhoneGuard may need to scan the users' contact lists. In order to intelligently identify and filter spam/fraud SMS messages, Baidu PhoneGuard may need to analyze the features of SMS messages sent from suspicious phone numbers. If an SMS message is determined to be spam/fraud, it will be quarantined on the user device.
百度手机卫士不会未经授权记录任何为提供相应服务功能而读取的内容，同时，您可以在防骚扰功能设置中关闭骚扰拦截功能。同时，您可以举报电话和短信，百度手机卫士将会将您选择的电话号码上传至服务器，该上传行为仅在您的主动操作下进行。	Baidu PhoneGuard never collects data without user authorization. Meanwhile, users can opt-out of the anti-spam service in the app settings at any time. Furthermore, users can report wrongly determined spam/fraud SMS messages (to our team) through the app. The report will be uploaded to our servers, and this action is only performed after your active operation.
垃圾短信云拦截功能，可以提供更精准的拦截服务，有效降低垃圾短信误拦和漏拦概率。垃圾短信数据会通过联网加密的方式，上传到百度云安全中心进行识别，百度手机卫士将严格加固这些数据，不会与您的任何个人信息进行匹配，也不会将此信息提供给其他任何第三方（法律法规规定必须提供的除外）。	The cloud-side anti-spam function is able to further increase the detection precision and recall, as well as decrease the false positive rate. Data of suspicious spam/fraud SMS messages is encrypted and uploaded to the Baidu Cloud Security Center for analysis. These data is securely stored on Baidu servers, and will never be leaked out (unless required by law enforcement agencies). In addition, these data is never used to match with users' personal information.
3.2 本"软件"不含有任何旨在破坏用户移动设备数据和获取用户隐私信息的恶意代码。	3.2 This app does not contain malicious code aiming to undermine data on user devices or acquire private data of users.
……	……

Opt-in Options for Users

Detection Rules (for FBS-Radar)

Intelligent Detection ON/OFF

Cloud-side Detection ON/OFF

Content Detection of Suspicious SMS Messages ON/OFF

Suspicious Voice Call & SMS Message Detection ON/OFF

Contacts' Voice Call & SMS Message Detection ON/OFF

Baidu PhoneGuard App