

Alternative Security for WiFi Networks

Dan Cvrcek*, Petr Blahak⁺, Petr Hirs⁺, ...

*Computer Lab, Cambridge University

⁺Brno University of Technology, Czech Rep.

This is about a project we started in 2005 and implementations were carried as two MSc diploma projects. It is still running and the guys named are working on an implementation that can be easily deployed.

Introduction – WiFi Networks

- Securing WiFi networks is tricky
 - do we really need to secure WiFi?
- There is a number of WiFi security standards
 - WEP (64bit / 128bit or 40bit / 104bit + 24bit IV)
 - 802.1x
 - WPA
 - WPA2 / 802.11i
- Community Networks
 - the most common form of large WiFi networks in CR
 - weak security (if any encryption then WEP is used)
 - usually large number of users (like 200-300)

We hear a lot about WiFi security. It is important, a lot of studies of how many networks are not secured at all...

From home user point of view the security does not really matter much as long as the bandwidth is not consumed by someone else. There may be legal implications - someone is downloading sensitive content

disassociate or deauthenticate packets

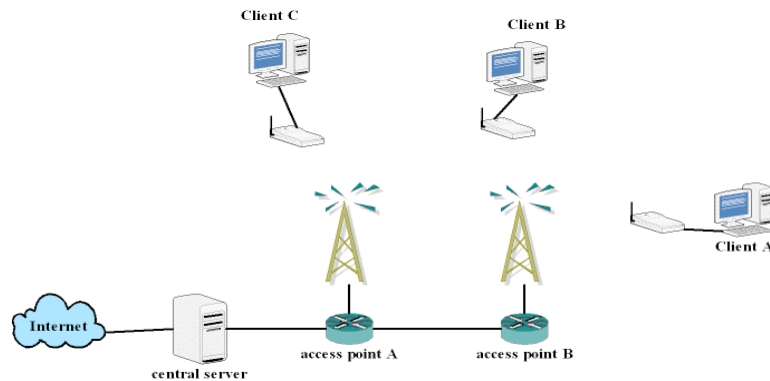
Community vs Corporate WiFi Network

- Hardware
 - company - can afford to buy only compatible hardware
 - community - each user buys its own WiFi card (price)
- Software
 - company - security software is installed by admin, easy access to all clients, central administration
 - community - each user is admin of their machine, various operation systems, "different flats"
- Policy
 - you can set-up policy but it cannot be much restrictive in community network
- Policy enforcement
 - very hard in community networks
- Threat model
 - **very strong risk of insider attacks in community networks**

Hardware community - AP for users to improve connectivity

Topology of WiFi Network

- Several (tens) of access points
- Each access point serves 20-30 users
- One (max two) gateways to Internet
- Internal services (shared disk space, VoIP, web space, ...)



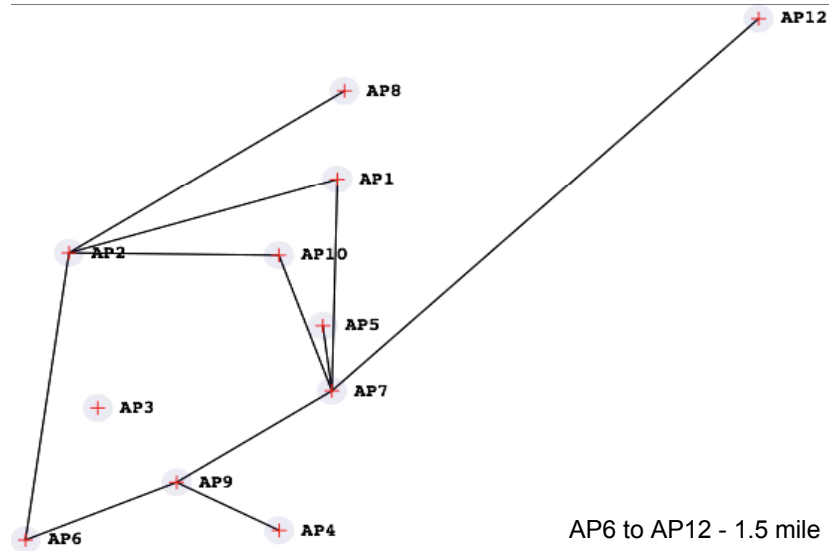
Alternative Security for WiFi Networks

www.buslab.org

Community network usually offer additional service - shared disk space for ISO images of various distributions of software, video, music, etc. Sometimes with reasonable access control

This allows use the surplus bandwidth (compared to Internet connection)

Topology of Our Testing Network



APs are sometimes connected by wires but only if money and environment allows.

AP5, AP10, AP1 cover a dense residential area



WiFi Security – Application Level

- List of possible security mechanisms is long
 - IPSec
 - SSH
 - SSL
 - VPN tunnels (Cipe, OpenVPN, Poptop, Openswan)
- Any additional mechanism increases demands on users
 - operating system
 - installation of new applications
 - configuration and maintenance (Kerberos, RADIUS)
- Users make mistakes

Reason to secure the network here - mainly financial (many more available resources) and possibly confidentiality (access to shared resources)

Clash of the security requirements and usability of the network

The selection of mechanisms is large but their applicability in community network is a problem. A lot of them is on application level

Why Alternative Approach

- WEP/WPA keys are shared
 - when compromised, WiFi network is unsecured
 - WEP attacks in minutes (some of our experiments - several seconds)
 - replacing shared key is difficult
 - *attacker is undetectable*
- Highlights (sort of) of reputation systems
 - we can pick users from crowd, they are with certain (non-negligible) probability attackers
 - topology of network remains intact, no additional wireless or active network devices, no SW for clients
 - unauthorised users can be eventually disconnected

Summary of why another approach is needed - second layer of defence
Attacker is virtually undetectable - one of several hundred users
How did she get access to the network?

Reputation Systems – Motivation

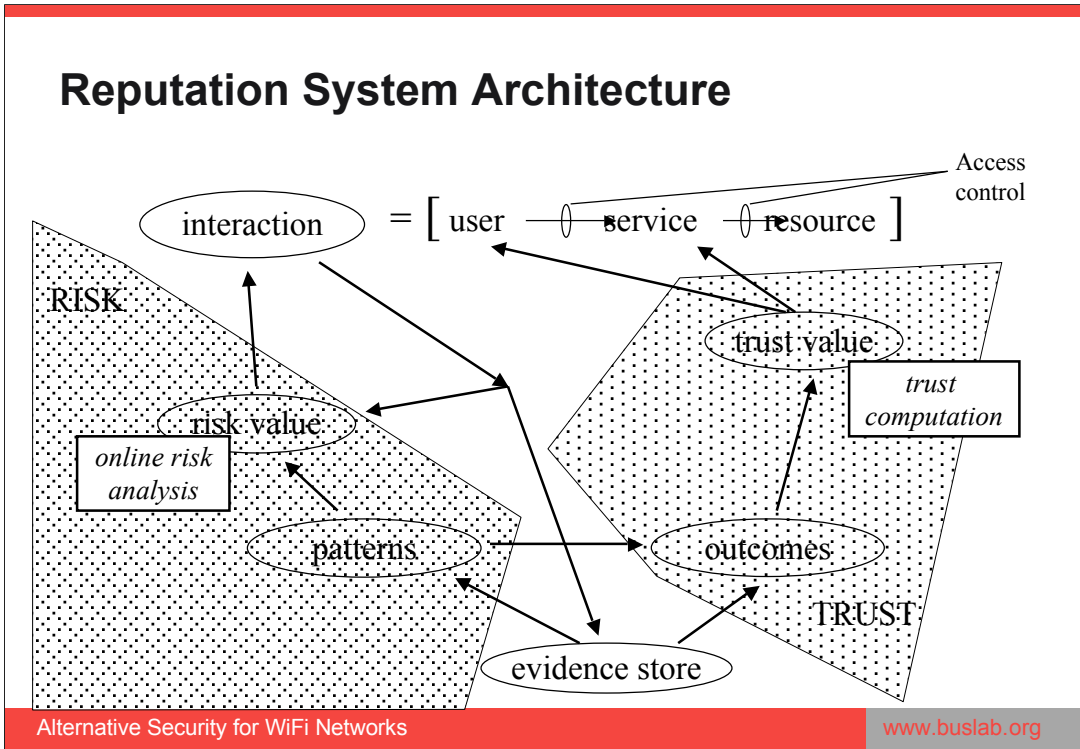
- There is no central administration
 - user cannot authenticate in each „domain“ <= expensive
- Servers/administration domains are heterogeneous but cooperating
- Systems are highly dynamic

- Interaction logs – basis for security decisions
- Knowledge is distributed among cooperating entities
- Potentially shorter reaction time
- Knowledge is imprecise, incomplete – mutual distrust, ...

Open problem – is reputation suitable for digital environment?

Why reputation systems - I was working on them some 2-3 years back and it seemed to be a sort of reasonable solution improving security

Something like typical environment, or typical application for reputation systems



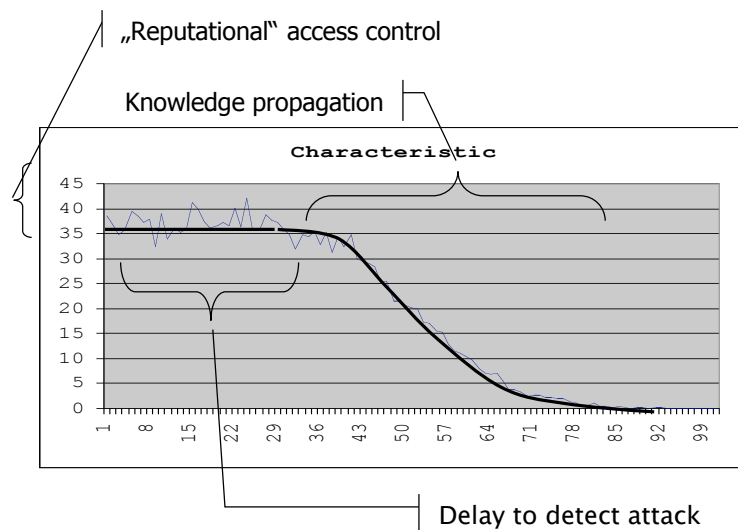
This is what I ended up with at the end of SECURE project I worked on with Ken Moody nad Jean Bacon in 2003-2004

Left-hand part is basically IDS system with an attempt to search for new patterns in real-time

Right-hand part influences access control and it is “orthogonal” to risk side of the model

This was my idea of implementation which we started with in Brno

Reputation Systems – Characteristics



Alternative Security for WiFi Networks

www.buslab.org

This picture is for distributed system where there is a number of entities working according to the previous schema

Ideal behaviour of reputation system in distributed environment - a lot of entities computing trust and searching for new risks

Costs incurred by attack

Reputation System for WiFi Network

- Reputation system evaluates user behaviour (measurable on APs central server)
- Reputation system structure
 - sensors – APs contain additional code keeping eye on active connections
 - central server – computes reputation from sensor data
- Reputation system processes
 - data logging on sensors
 - data collection on central server
 - data evaluation – computing reputation
 - feedback – selection and execution of security countermeasures

There is no distributed system in the moment and existence of something alike is not very probable.

Although if a system was deployed in more networks - there could be a feedback in terms of possible new types of attacks

Sensor Design (AP Extension)

- AP is a Linux machine and as such can be extended
- Following data are collected from all APs
 - user's IP address
 - user's MAC address
 - signal strength (standard units - dB)
 - noise to signal ratio
 - time
 - name of AP
- We also log amount of transferred data but it is not used in the moment
- Retrieved data are stored in database and ARFF files – data mining

dB - relative to 1 Watt of transmission power

Example of Statistics

- Variations from average level of signal - these are computed for AP and for particular clients
- Large variations are further investigated

MAC adresa	Průměrná síla odchylna prům.	Průměrná síla odchylna prům.	Průměrná síla odchylna prům.	AP	AP - min. síla odchylna	AP - prům. síla odchylna	AP - max. síla odchylna	Datum
00:20:4f:1f:83:39	3.84	9.94	15.16	1/1	0.42	1.43	6.99	2006-05-08 19:28:39
00:23:46:76:45:49	2.50	5.75	11.50	3/1	0.34	1.37	5.53	2006-05-08 19:28:39
00:40:19:c3:03:44	0.29	5.23	13.71	3/1	0.34	1.37	5.53	2006-05-08 19:28:39
00:4f:62:00:73:00	0.14	5.08	13.86	1/1	0.42	1.43	6.99	2006-05-08 19:28:39
00:90:4b:b6:af:33	0.29	3.73	15.71	3/1	0.34	1.37	5.53	2006-05-08 19:28:39
00:4f:62:00:73:3f	0.18	3.67	13.82	3/1	0.34	1.37	5.53	2006-05-08 19:28:39
00:4f:62:00:73:00	0.28	3.45	9.72	3/0	0.26	0.99	6.27	2006-05-08 19:28:39
00:60:b2:e4:91:44	2.00	3.44	5.00	3/1	0.34	1.37	5.53	2006-05-08 19:28:39
00:00:00:00:00:00	0.50	3.43	5.50	3/0	0.26	0.99	6.27	2006-05-08 19:28:39
00:02:28:a6:0b:10	0.19	3.40	27.81	1/1	0.42	1.43	6.99	2006-05-08 19:28:39
00:4f:62:00:7a:7b	0.07	2.92	9.93	1/1	0.42	1.43	6.99	2006-05-08 19:28:39
00:4f:62:00:31:90	0.47	2.73	11.53	3/1	0.34	1.37	5.53	2006-05-08 19:28:39

Example of Statistics

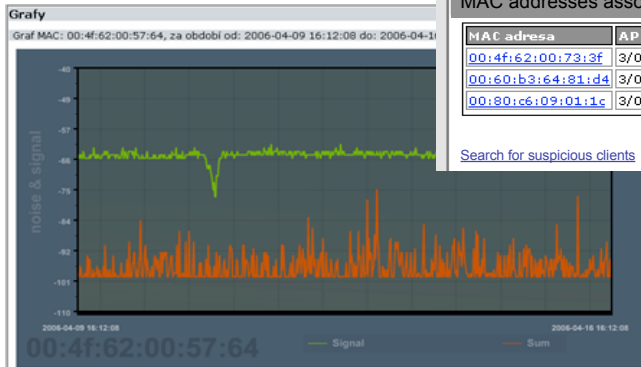
Signal variations on AP

Minimální	Průměr	Maximální	Datum	AP
0.30	0.73	3.86	2006-05-08 19:28:39	1/0
0.42	1.43	6.99	2006-05-08 19:28:39	1/1
0.26	0.99	6.27	2006-05-08 19:28:39	3/0
0.34	1.37	5.53	2006-05-08 19:28:39	3/1
0.29	0.79	3.58	2006-05-08 19:28:39	4/0

MAC addresses associated with more APs

MAC adresa	AP
00:4f:62:00:73:3f	3/0, 3/1
00:60:b3:64:81:d4	3/0, 3/1
00:80:c6:09:01:1c	3/0, 3/1

[Search for suspicious clients](#)



Evaluating Reputation and Reaction

- Evaluation
 - computing signal strengths variations from average on AP
 - MAC and IP address check
- Countermeasures against potential attacker
 - limiting bandwidth
 - restrictions on TCP ports
 - disconnecting from WiFi network
- Evaluation results must be confirmed by administrator
- Risk of user disconnection is more important than risk of undisclosed attacker

Implementation

- Sensors
 - PC (MikroTik, MIPS 175 MHz, 70-120USD) + OS Linux
 - WiFi card Zcom xi626 / CM9 (Atheros chipset) + driver for HostAP
 - *SNMP protocol*
- Central server
 - Database PostgreSQL => Oracle (limited DB size)
 - Web-based GUI
 - Computation of reputation
 - Analysis is directly in DBMS (PL/pgSQL)
- Reaction
 - Scripts updating firewall rules on all APs

Data Processing – Reputation

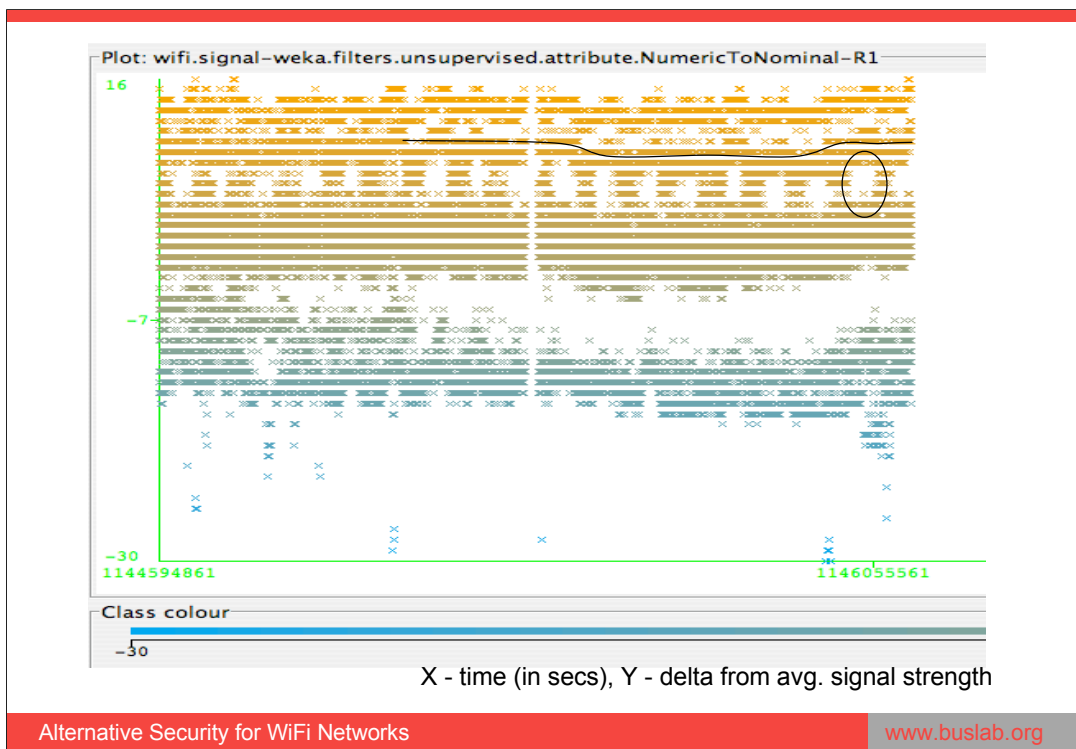
- Existing implementation – RepuNET
 - computes average values
 - for AP as a whole
 - separately for clients of AP
 - defined trigger conditions - signalisation
- Revised system
 - users of AP split into clusters with predefined relative sizes
 - cluster intersection
 - assumption is that attackers are in minority
 - goal - universal functions applicable on several types of data

Data Mining

- Search for analytical functions to be implemented in the system
- Initial enthusiasm is gone :-)
- Data from APs must be pre-processed
 - one has to know what is looking for
 - ... as we do not know what we are looking for
- Output from RepuNET (thousands of files per week)
 - a file per AP
 - a new file every 15 mins (on the edge of our needs)
- Weka system
 - takes ARFF files
 - but needs different content

We do not want to make it part of the system but use it as a tool to find interesting information in data.

Second step - implement appropriate analysis functions in the system

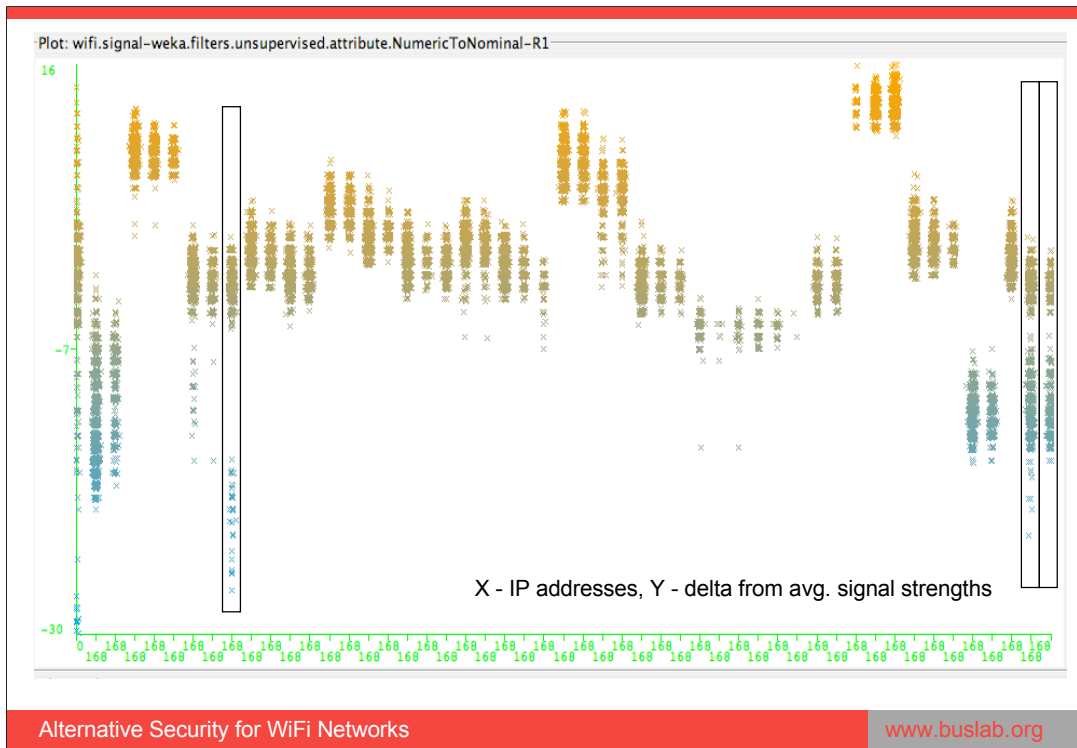


Just to show what sort of plots you can get from Weka - initial visualisation of input data

White line in the middle - drop-out of the system.

Total time span here is about 17 days.

Windows is disconnection of some clients during day. The curved line depicts change in weather conditions

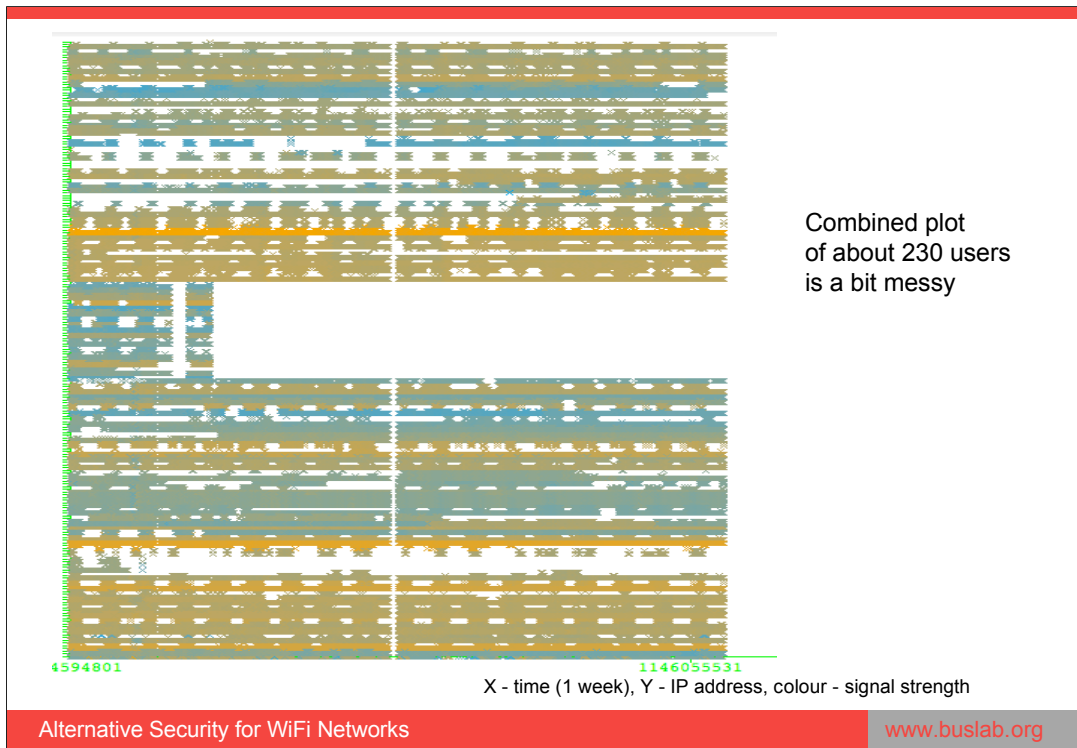


Variation of signal strength per clients.

Suspicious clients are in black rectangles, each has two intervals clearly confined.



One client changes strength of signal in a way that makes her potential attacker



This is a plot combined from four APs, it is much harder to visually find any interesting information.

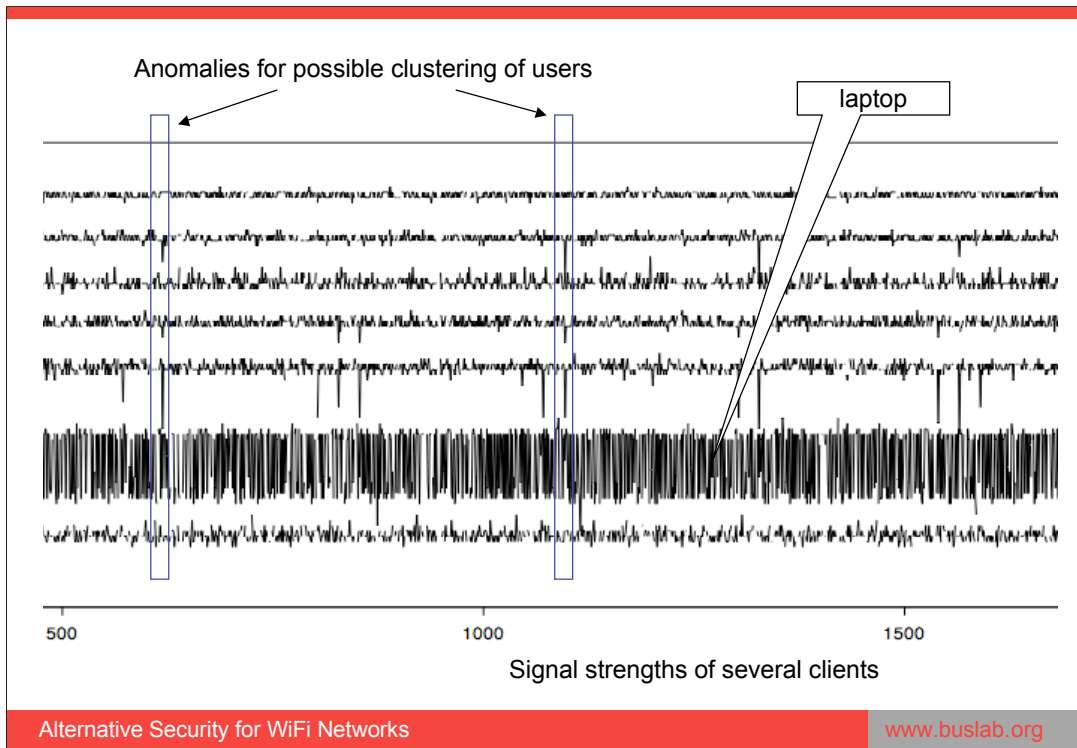
One AP was used for a shorter period of time - (middle of the plot), again a drop-out of the system - vertical white line across.

Conventional Analysis

- We know what we want to find
 - two clusters of IP addresses
 - Roughly relative size of clusters (attackers vs users)
 - what may be an interesting information
- We make a list of candidate functions (patterns from schema)
 - test them on data we have
 - select most promising
 - implement in system
 - use it to analyse new data

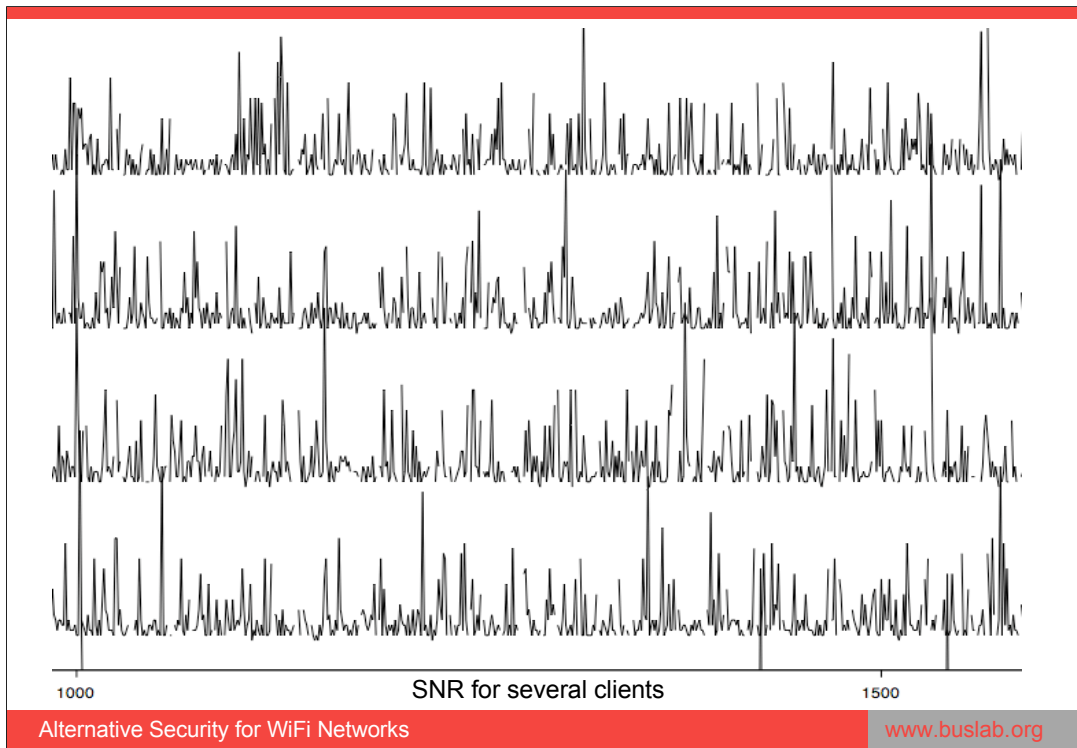
Or just hand-held analysis of data, implementation in programming language

24 -> 10



All values are a mean of about 20 measurements taken with 15 seconds intervals

Large variations in signal strength



All values are a mean of about 20 measurements taken with 15 seconds intervals

Traffic Data

- We have data about traffic
 - Four types of data: FTP, web, mail, other
 - each group: in and out
- Two major problems with analysis
 - one-time events strongly influence user profile
 - applications not respecting ports (BitTorrent)
- We collect the data but that is it

This is something we want to take a look at.

There are no expectations regarding results but it may give some hints

Conclusions

- Reputation system
 - will never ensure 100 % detection of attacker
 - is not limited on threats known in advance
 - suitable for distributed environment
- Initial implementation of RepuNET found in 2 months
 - 12 unauthorised users - attackers
 - problems with connection at several users - non-standard connection behaviour
 - errors in user database;-)
- It turned out as suitable to categorise attackers and for network diagnostics
 - side effect – automatic feed-back/reaction is questionable

Thanks for you attention!