



UNIVERSITY OF
LIVERPOOL

Trust and Security Issues in Decentralised Wireless Networks

Professor Alan Marshall

Advanced Networks Laboratory

*Department of Electrical Engineering and
Electronics*

Cybercrime

“Any act which relies significantly or entirely on the use of one or more computers and gives rise to a result that is, or has a traditional counterpart that would be, subject to criminal sanction”

- **Performed by Computer**
- **Is already illegal**

Cybercrime

- Costs the UK economy up to £27bn each year (2013 UK report)
- Worldwide annual cost reaching around \$388bn (£253bn)
- Proliferation of mobile devices and cloud computing
- Growth of connected devices:
 - 2010: the number of devices connected to the Internet stood at around **12.5 billion**
 - 2015: grow to roughly **25 billion**
 - 2020: **50 billion**
- *A fertile ground for cyber criminals*

Cybercrime



Countries in which a breach was confirmed

***Breach:** Successful cyber attack

Growth of public WiFi Hotspots

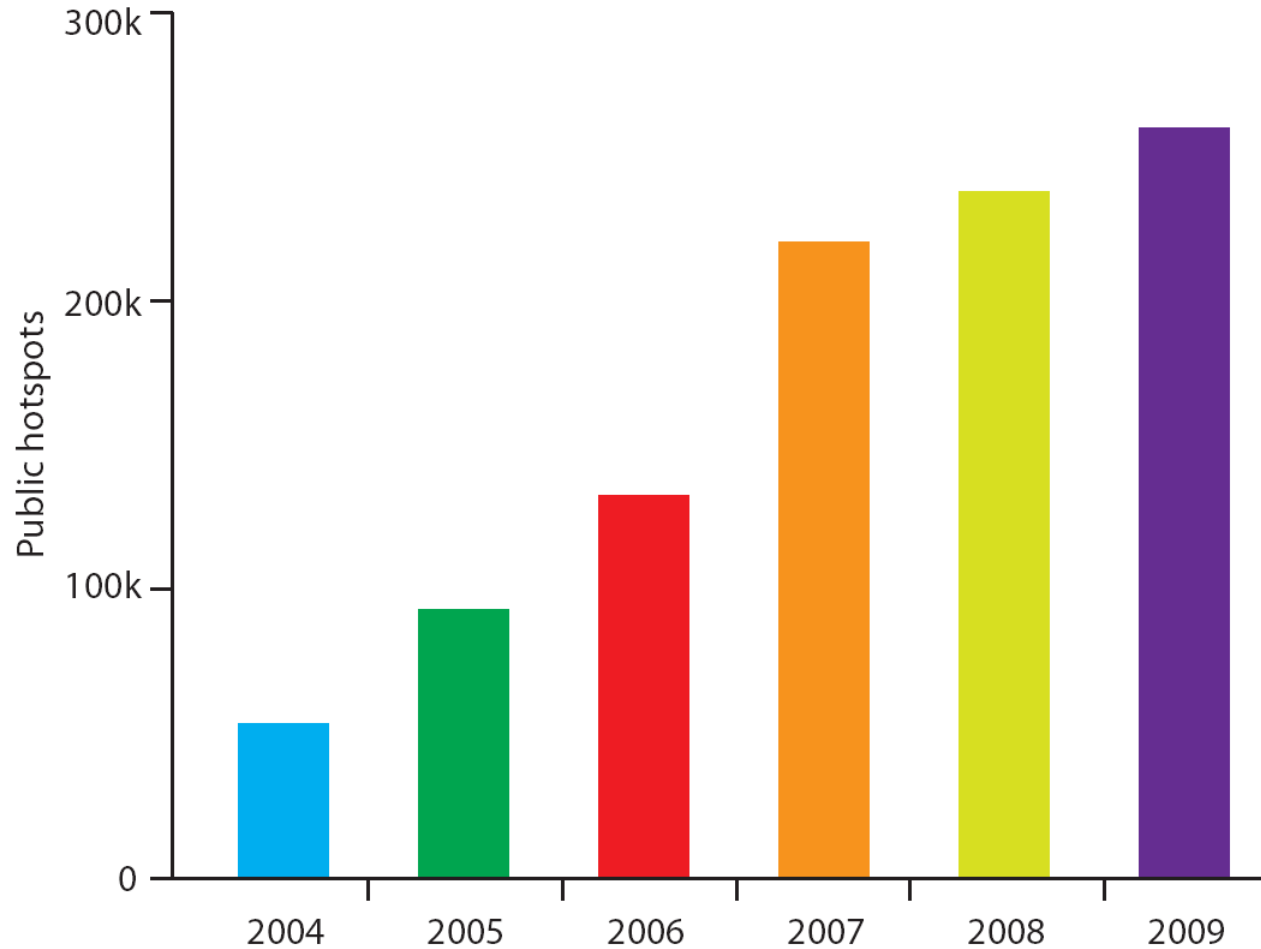
Wifi hotspots set to more than triple by 2015

- **Global growth from 1.3 million in 2011, to 5.8 million by 2015 – 350% increase!**
- **58% of network operators now believe wifi hotspots are “crucial” to their customers’ experience**
 - To offload busy mobile broadband networks
 - To provide value added services
- **China Mobile planning to deploy a million hotspots**
- **Japan’s KDDI planning to grow its 10,000 wifi hotspots to 100,000 within six months**

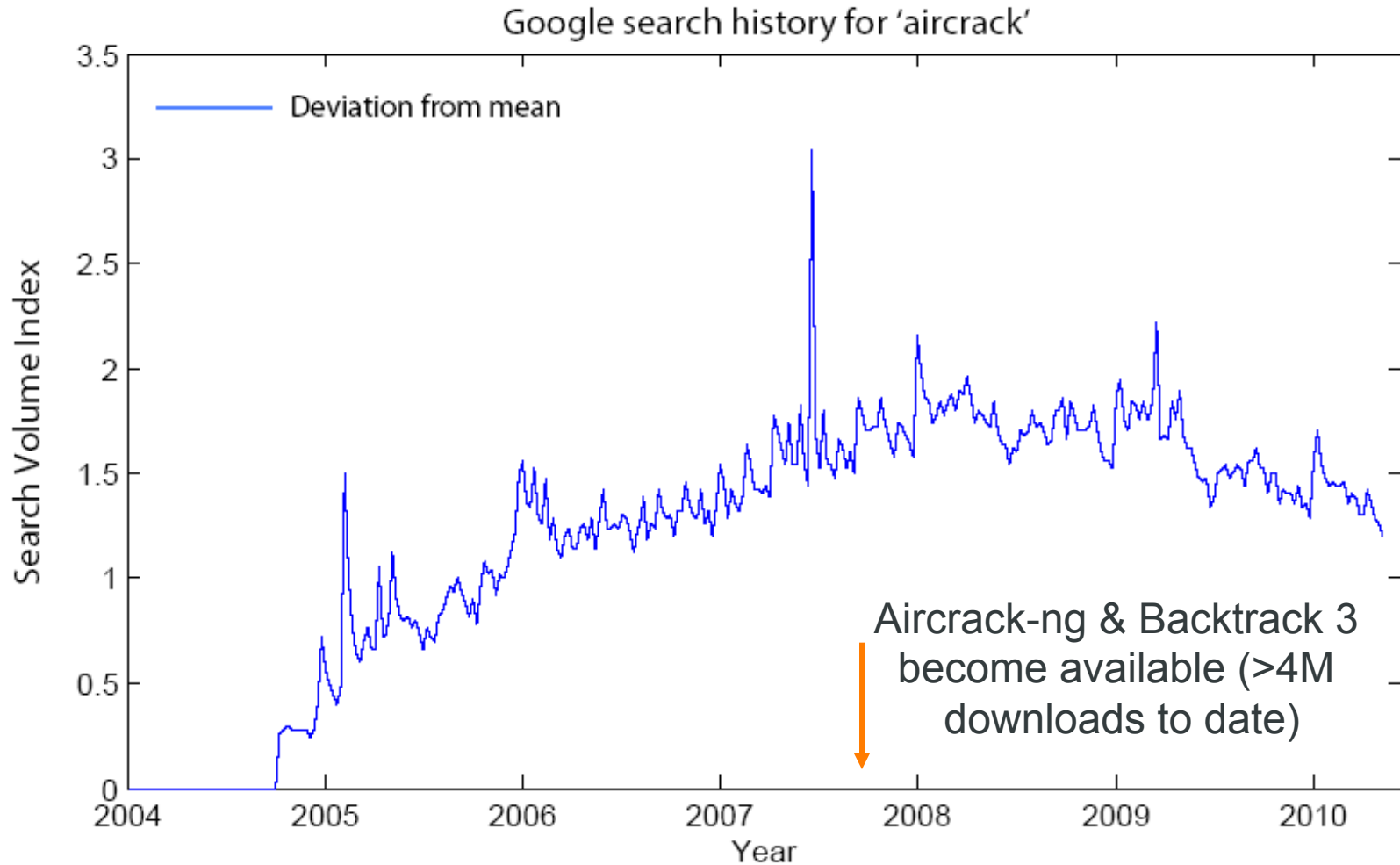
Growth of public WiFi Hotspots

(<http://v4.jiwire.com/search-hotspot-locations.htm>)

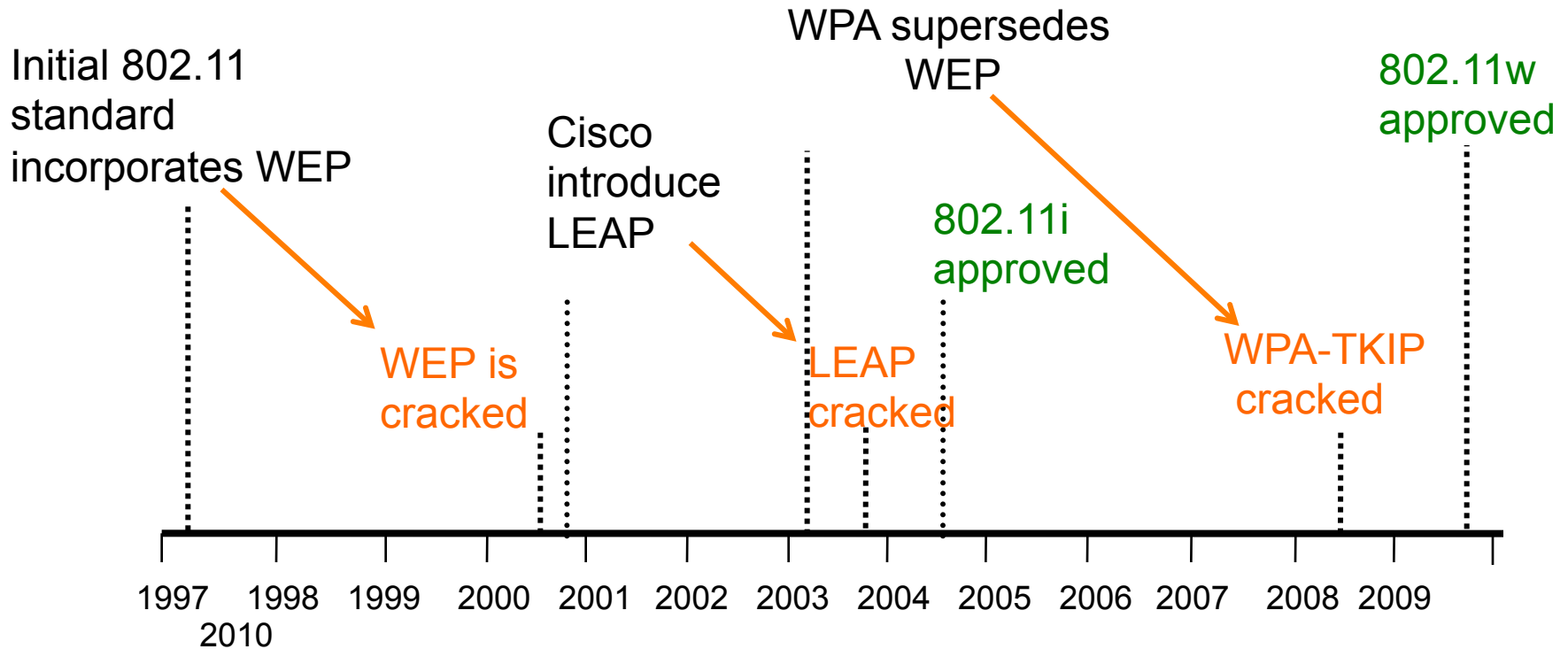
Growth in worldwide public hotspots



Availability of attack tools



Wi-Fi Security timeline



LEAP: Lightweight Extensible Authentication Protocol
TKIP: Temporal Key Integrity Protocol
WEP: Wired Equivalent Privacy
WPA: Wi-Fi Protected Access


The Open Access Dilemma


- Provide secure access to customers whilst limiting the constraints on client devices
- Authentication methods are limited
- Impractical to distribute encryption keys to clients
- Little if any, requirements can be imposed on the client devices
 - Clients don't want to have to install new software
 - No restrictions on device or operating system in use (e.g. Windows, Apple, Linux, Android)
 - Support a wide range of client devices (including legacy)



The Open Access Dilemma

App that attacks local WiFi networks

 Syorkan

 Jadilah kawan yang pertama memperkenalkan ini.

Posted: Jul 02, 2011 3:18 AM

Updated: Jul 02, 2011 4:24 AM



KYTX -- There is a quick and easy way for hackers to spy into your private

Key crack service



WPA CRACKER

about

run

faq

An Introduction

WPA Cracker is a cloud cracking service for penetration testers and network auditors who need to check the security of WPA-PSK protected wireless networks.

WPA-PSK networks are vulnerable to dictionary attacks, but running a respectable-sized dictionary over a WPA network handshake can take days or weeks. WPA Cracker gives you access to a 400CPU cluster that will run your network capture against a 135 million word dictionary created specifically for WPA passwords. While this job would take over 5 days on a contemporary dual-core PC, on our cluster it takes an average of 20 minutes, for only \$17.

NEW :: We now offer Germany dictionary support, a 284 million word extended English dictionary option, and ZIP file cracking.

Simply upload your network capture, start your job, and WPA Cracker will email you the results within minutes! [Run It](#) →

Wireless Threat Models: Basic types of attack

Three main categories of attack:

- Attacks against the **availability** of the network (e.g. DoS floods, resource exhaustion)
- Attacks against the **integrity** of the data (e.g. “poisoning” type attacks)
- Attacks against the **privacy** of the data (e.g. Encryption type attacks)

More complex attacks combine these

WiFi Attacks mainly target the Physical and MAC layers

Wireless Threat Models: Basic types of attack

Eavesdropping

Data Decryption

Message Modification

Traffic injection

Denial of Service (DoS)

Masquerading

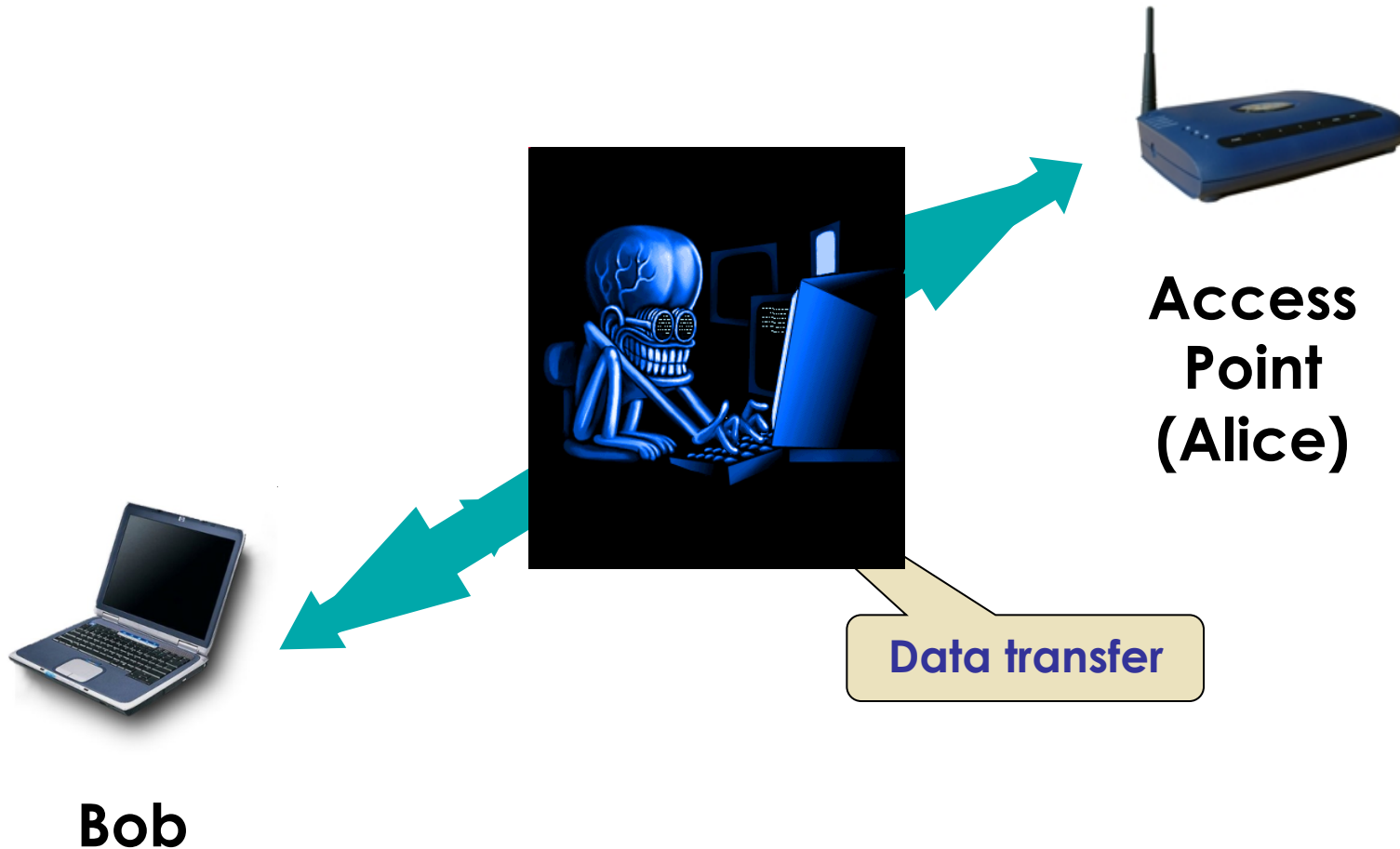
Man-In-The-Middle (MITM)

There are others

*.....Requirement for Wireless Intrusion Detection /
Protection systems*

Man-in-the-middle attacks

- This attack combines DoS and Masquerading attacks



Detection & Mitigation Strategies

Current detection strategies:

- Enterprise networks only, nothing for Open Access
- Overlays of “wireless sensors”
- Localisation techniques

Current mitigation strategies:

- Strong Encryption
- Security through Obscurity
- Access control (white) lists

None of the above are suitable to Open Access

Detection & Mitigation Strategies

We cannot stop forged frames being transmitted.

Hackers don't play by the rules of the protocol

Maybe physically take them out ;-)

Detection can be based on anomalous behaviours:

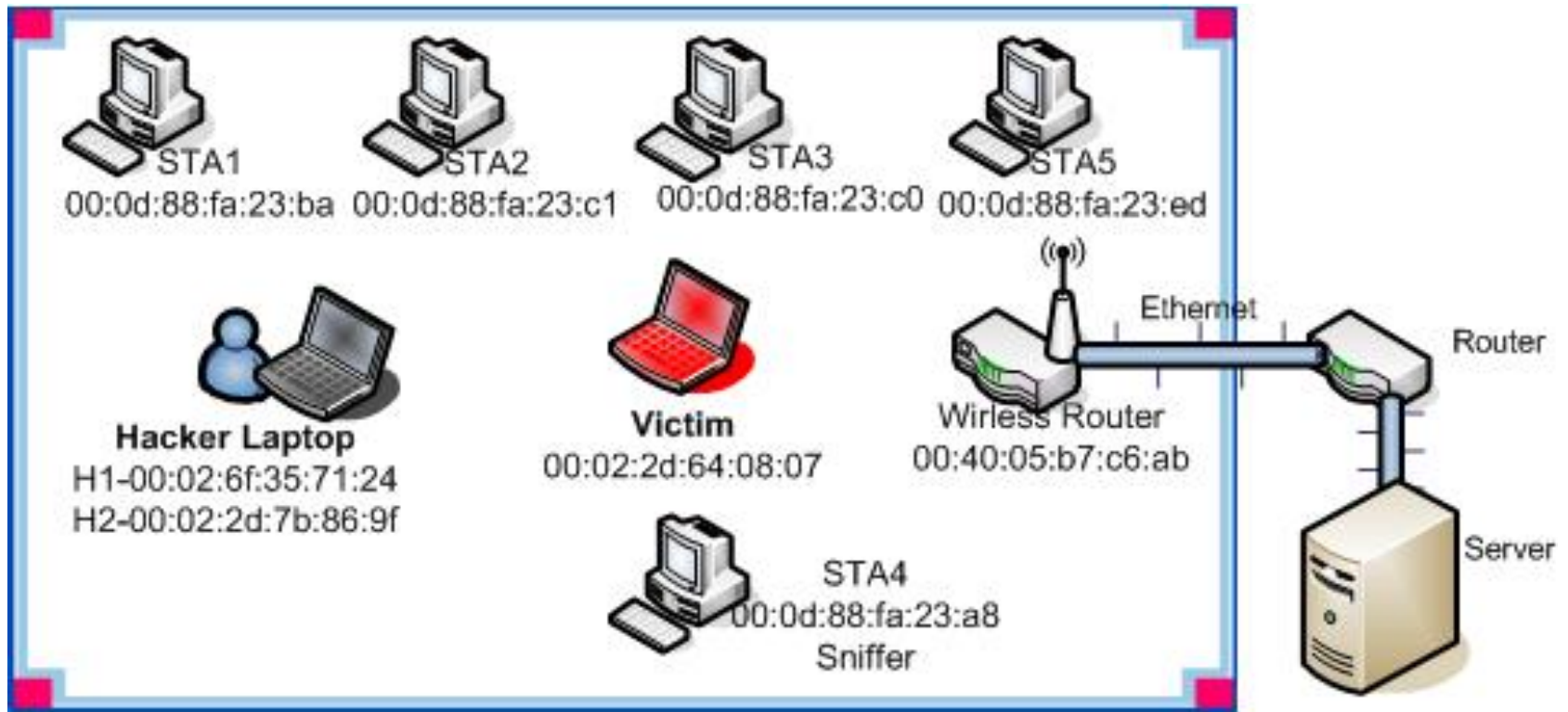
Network Parameters (RSSI, beacons, MAC addresses, etc)

Analysis of traffic patterns

Most likely require a combination of all the above

Let's Attack a WLAN/ Victim

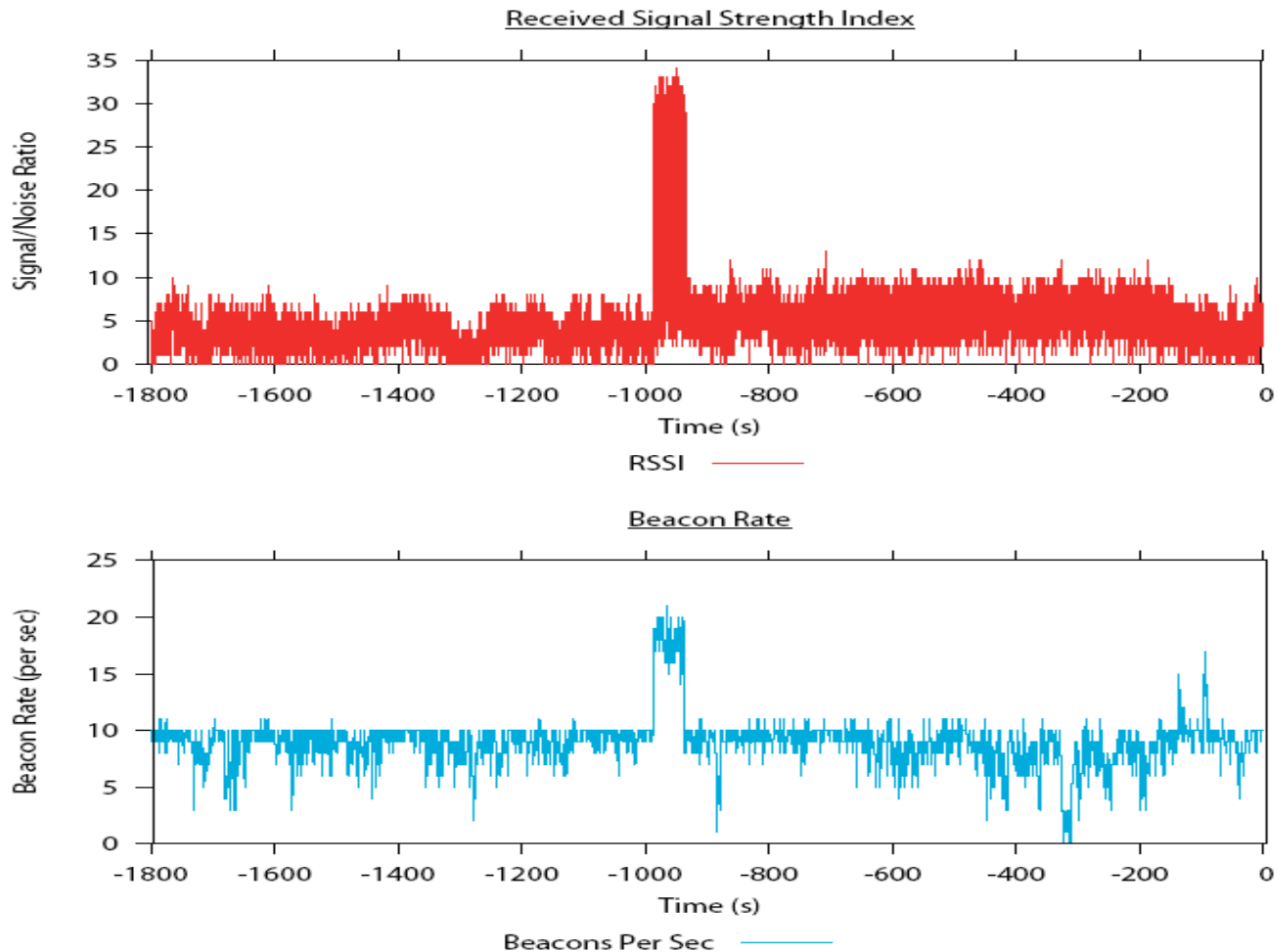
Hacker performs DoS & MITM attacks



Attack Detection

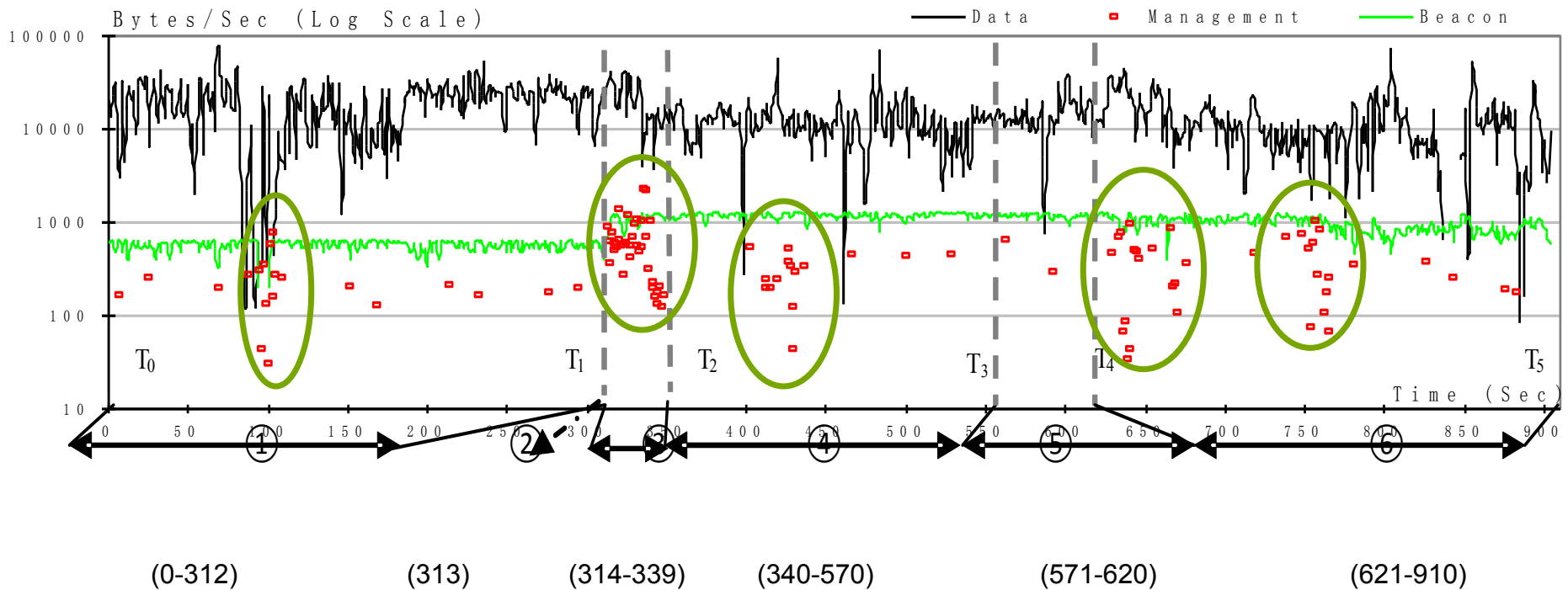
Discrimination using physical layer parameters

Comparing Metrics of 00:1A:70:EB:74:B9 for Rogue AP Detection



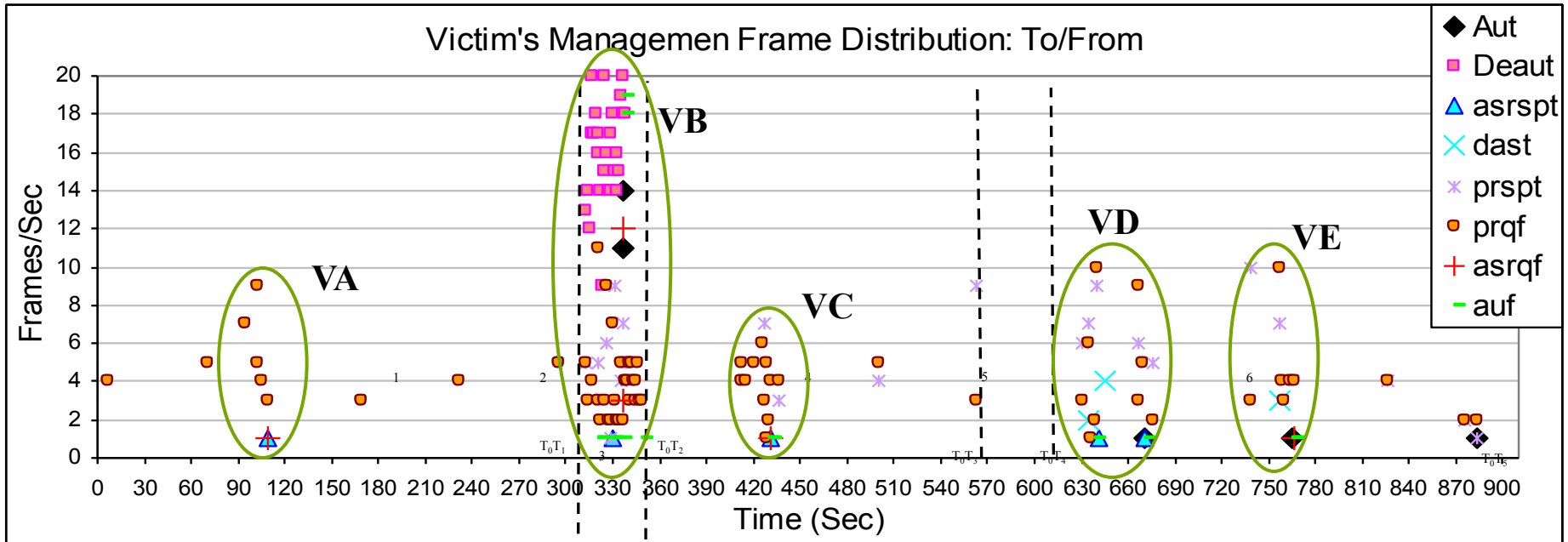
Attack Detection

WLAN Traffic Distribution & Management Frame Clusters



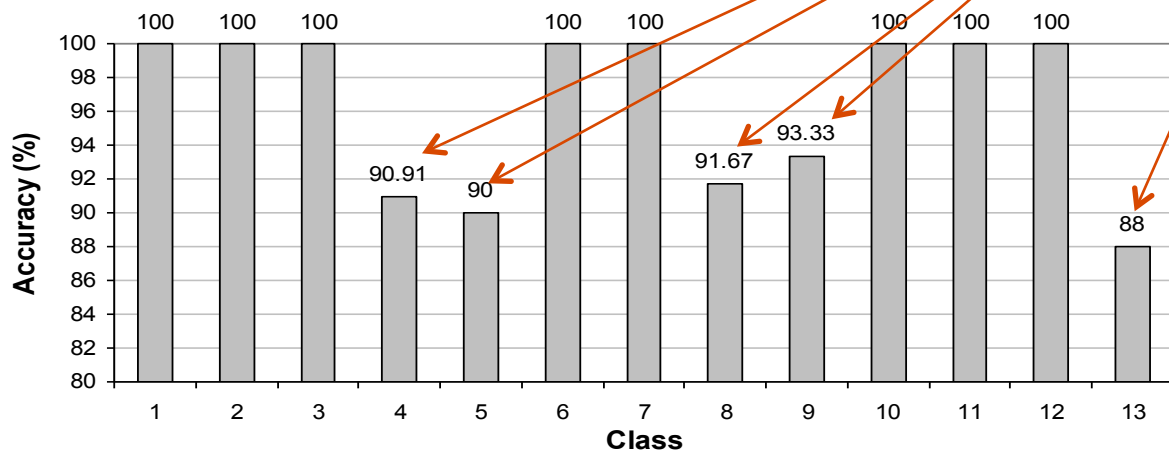
Looking into the Clusters

Victim's Management Frame Distribution: To/From Victim



Attack Classification Accuracy

Class Label	Type	Class Label	Type
1	Leave	8	DoS-Disassociate Flood
2	Leave & Rogue AP	9	DoS-Disassociate Flood & Rogue AP
3	Rogue AP	10	DoS-Disassociate Broadcast
4	DoS-Deauthentication Flood	11	DoS-Disassociate Broadcast & Rogue AP
5	DoS-Deauthentication Flood & Rogue AP	12	Join & Rogue AP
6	DoS-Deauthentication Broadcast	13	MITM
7	DoS-Deauthentication Broadcast & Rogue AP		



- In all cases anomalous network behaviour is identified.
- 100% accuracy can be obtained by adjusting false alarm/ missed events thresholds
- MITM classification is improved to 96% by employing a “likelihood score mechanism”.
A significant improvement in recognizing this type of attack - currently no accurate identification methods.

W.Zhou, A.Marshall. Q.Gu, “A Sliding Window Based Management Traffic Clustering Algorithm for 802.11 WLAN Intrusion Detection”, book chapter: *Network Control and Engineering for Qos, Security and Mobility*, Jan 2007.

Attacks against Trust



UNIVERSITY OF
LIVERPOOL

Trust

Merriam-Webster's Dictionary defines trust as
“assured reliance on the character, ability, strength, or truth of someone or something.”

Dictionary.com describes trust as

“the firm reliance on the integrity, ability, or character of a person or thing.”

We define trust as the degree of belief that an entity is capable of acting reliably, dependably, and securely in a particular case.

Trust

- When considering security threats, the design of many network protocols and applications must consider the possibility that some participants will not follow the protocols honestly.
- When trust information is produced, the designer can integrate the trust values them into the protocol design, without worrying about how to determine whether a node is trustworthy or not.
- **Therefore a related class of attacks include those that seek to compromise the trust levels of specific network elements**

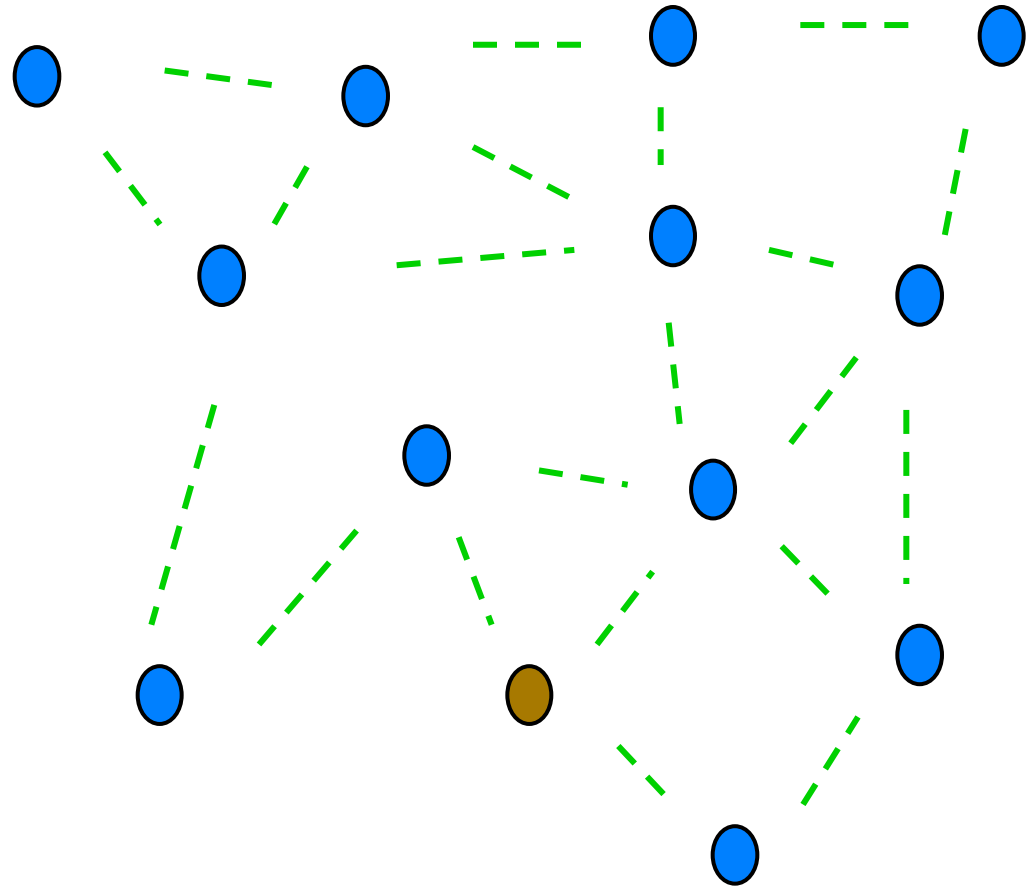
Trust

- Monitoring is used to establish trust among nodes in a network
- The basic idea is evaluating trust values to describe the trustworthiness, reliability, and capacity of individual entities
- Based on previous, direct or indirect observations on the behaviours of nodes
- This is particularly important for distributed systems:
 - **Peer-to-Peer**
 - **Ad-hoc Networks**
 - **MANETS**

Threats in wireless networks

Ad-hoc Wireless Networks

- PDAs, cell phones, laptops
- Distributed environment
- Limited resources
- Limited radio range



Selfish/malicious behavior

<i>Attack name</i>	<i>Layer or Area</i>	<i>Feature</i>
<i>Selective misbehaviour</i>	Network layer, Data forwarding	Behaving badly to one node and well to other (important) nodes
<i>On-off</i>	Network layer, Data forwarding	Randomly Behaving badly and well, in order to be undetected by maintaining a normal trust value
<i>Conflicting</i>	Network layer, Data forwarding	Behaving badly and well to different nodes, to conflict the trust values from various views among the network
<i>Bad mouthing</i>	Network layer, Data forwarding	Inflating the trust value of other nodes (boasting), or reducing it. Also called Slander.

Weakness of current TMFs

- **Based on Probabilistic Estimation**
- **Most use only a single parameter to determine the trust metric**
 - e.g. successful interactions or packet loss rate
- **Knowledge of this can be used by an attacker**
 - For example an attacker/selfish node can obtain a very high trust value by just interacting with close neighbours, while dropping or abandoning communications with nodes far away.
 - In comparison, normal behaving nodes communicating with all neighbours (near and far) will produce lower trust values (higher packet loss rates).

Proposed Approach

Based on Grey theory

1982 Deng Julong

Relational Degree

Use multiple parameters

transactions' times

ACK counts

etc

Advantages

Requires less samples



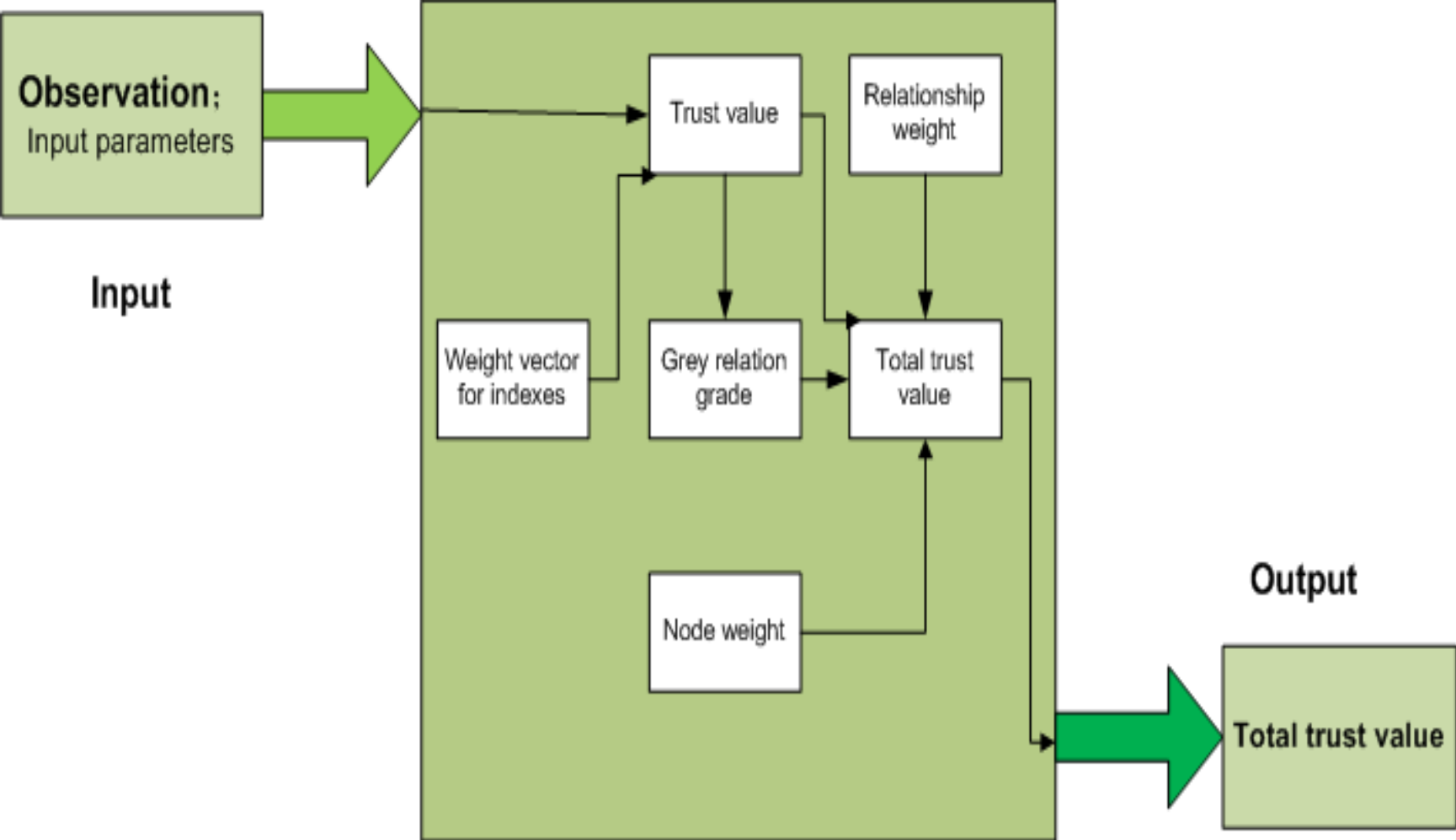
Grey Theory – Input Parameters

- Not only the *packet loss rate*
- But also: *signal strength, data rate, and other physical factors*
- The relational degree is based on a vector that describes the basic elements of the communications process

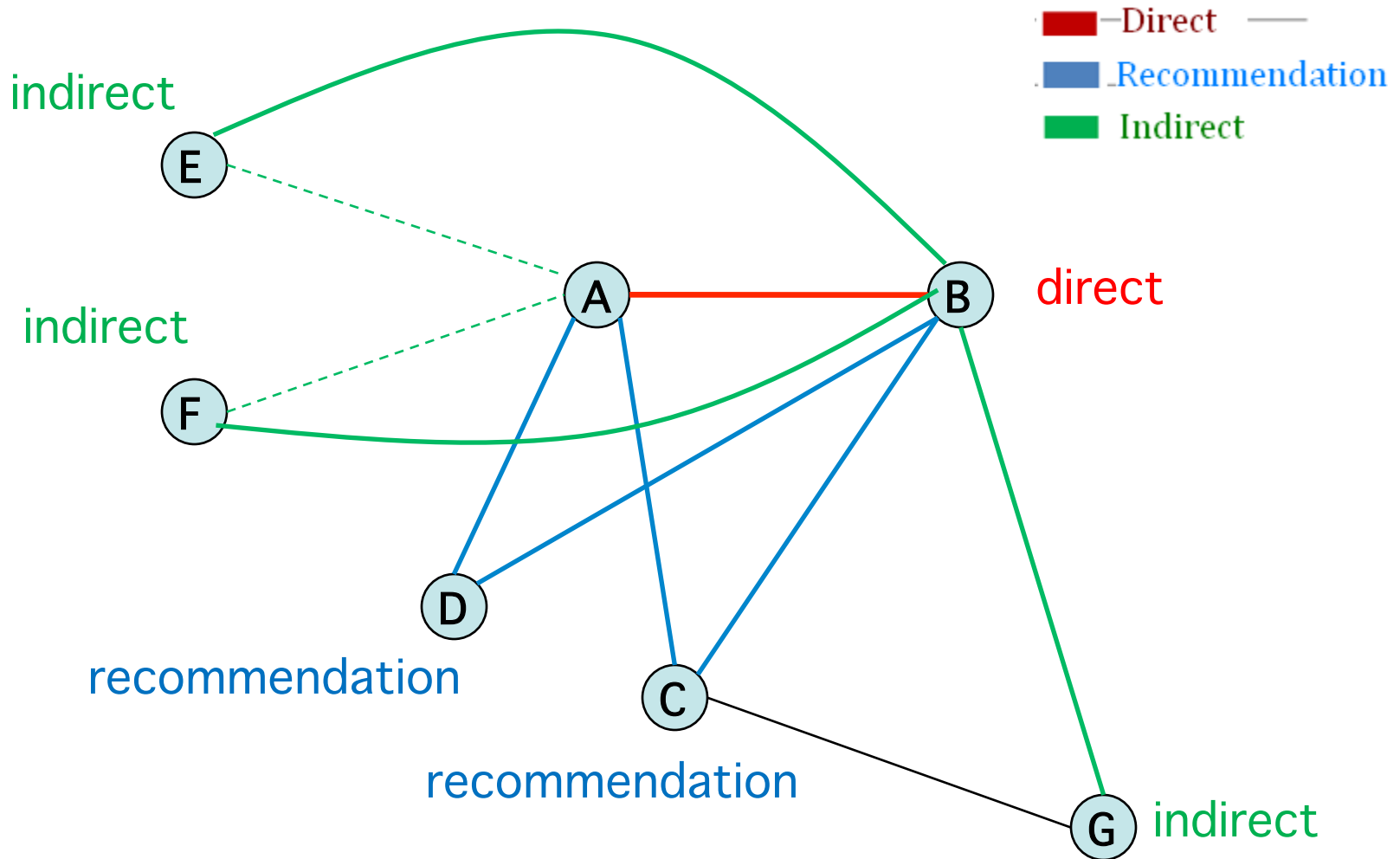
$X = \{\textit{packet loss rate, signal strength, data rate, delay, throughput}\}$

- This is applied to all observations

Grey Theory – functional blocks



Trust Relationships

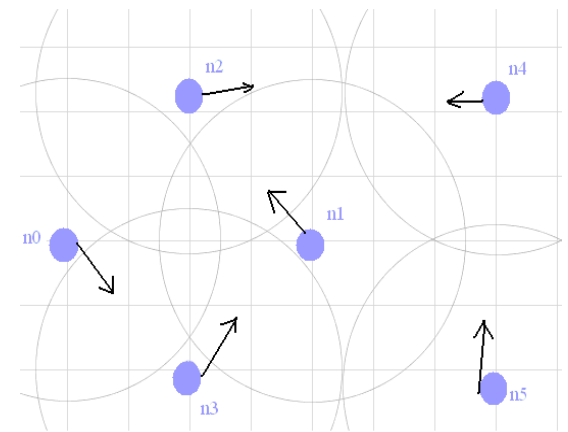
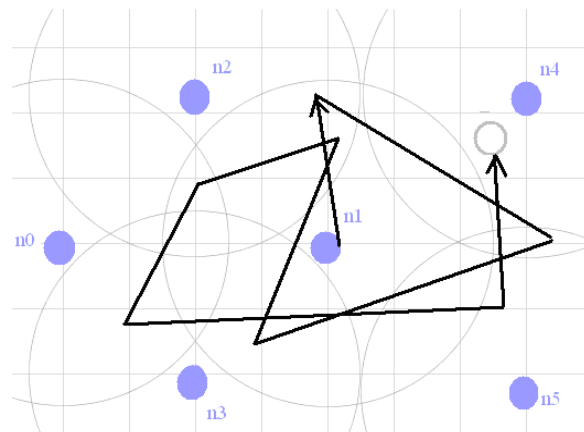
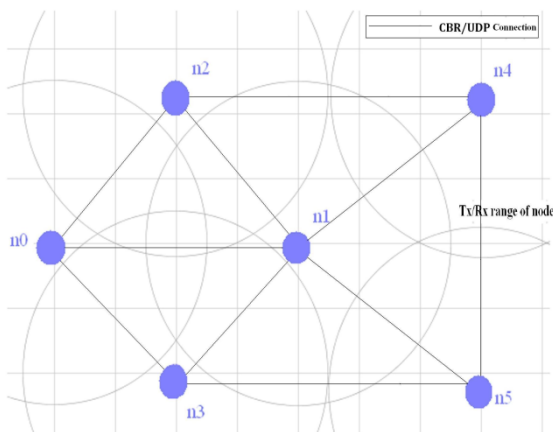


Trust relationships

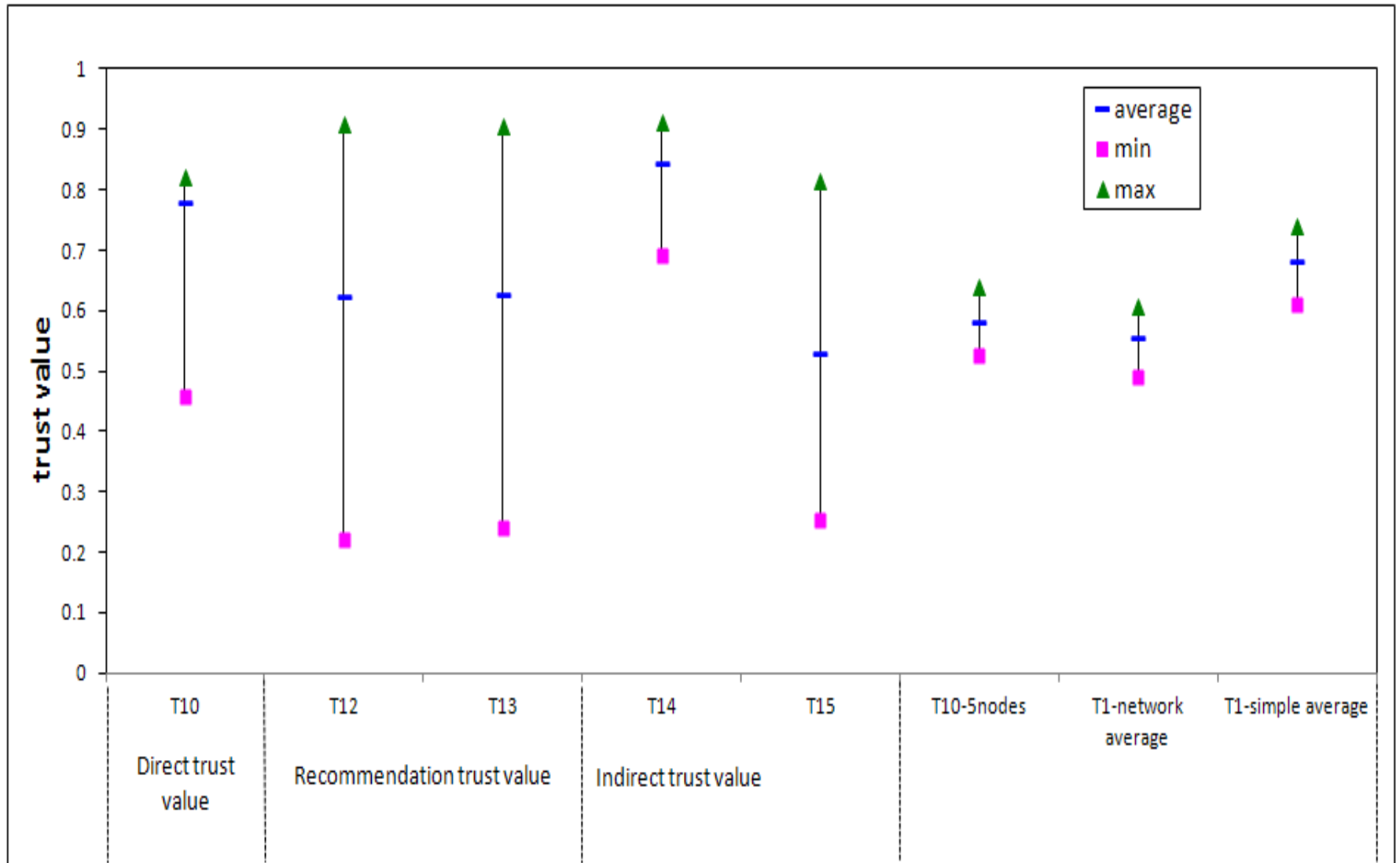
- **Direct trust**
- **Recommendation trust**
- **Indirect trust**

$$T_{BA-total} = \rho T_{BA-direct} + \alpha T_{BA-recommendation} + \beta T_{BA-indirect}$$

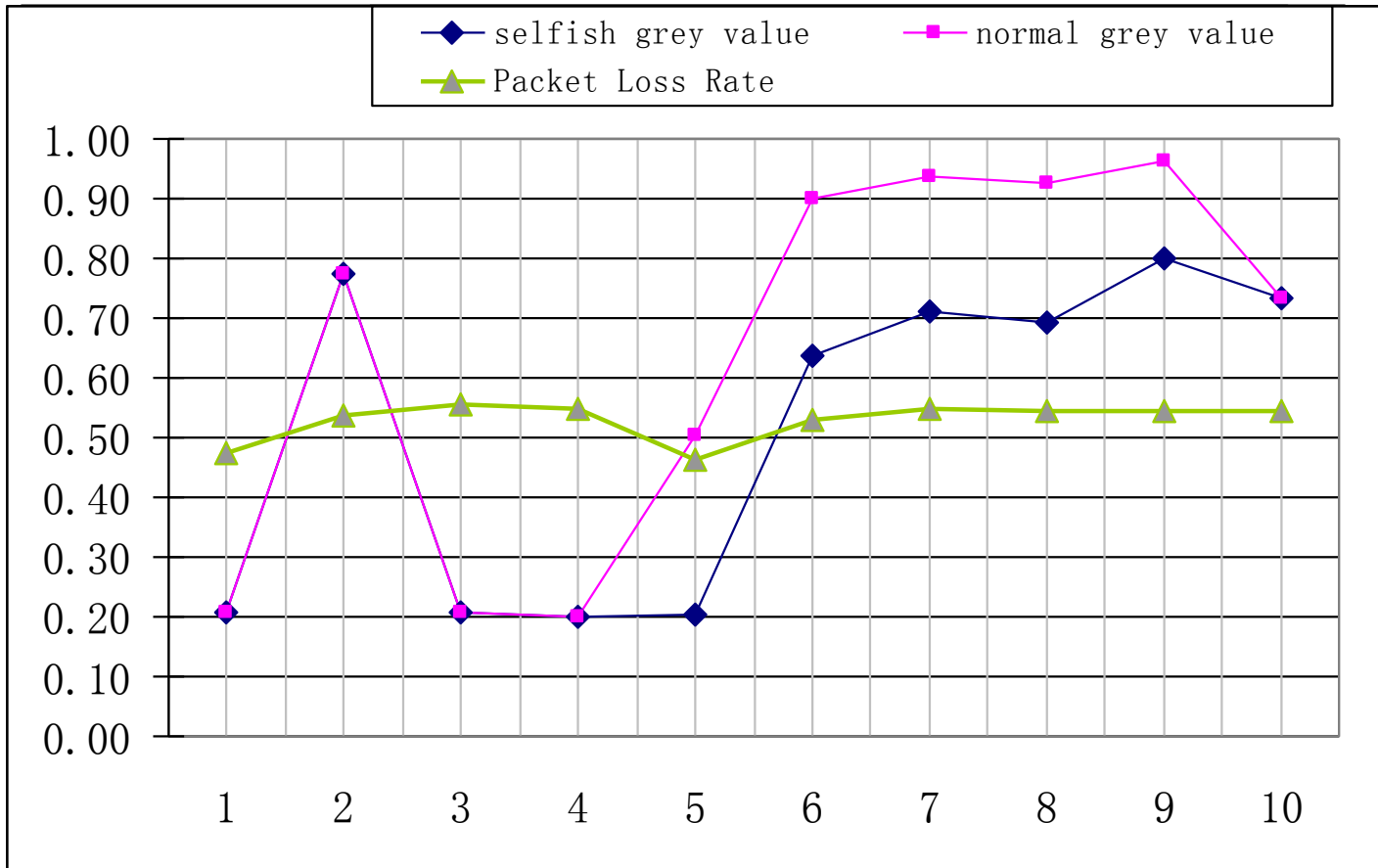
Mobility Scenarios



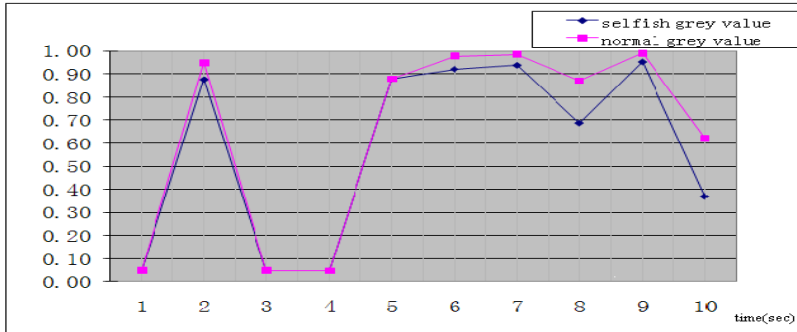
Trust values



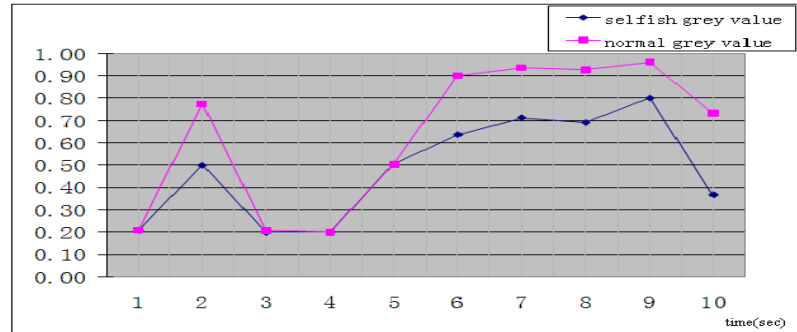
Trust values calculated by Grey Theory and PLR



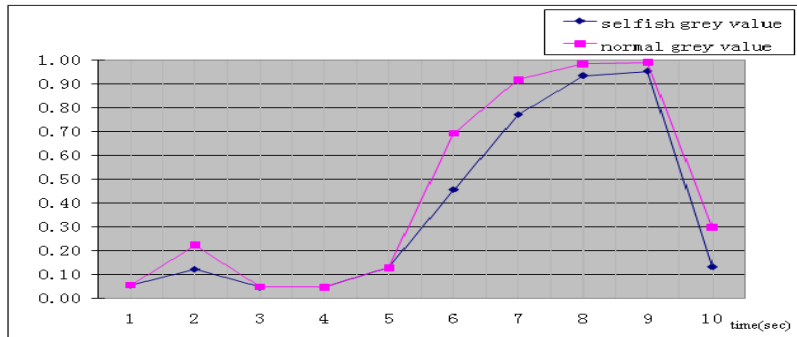
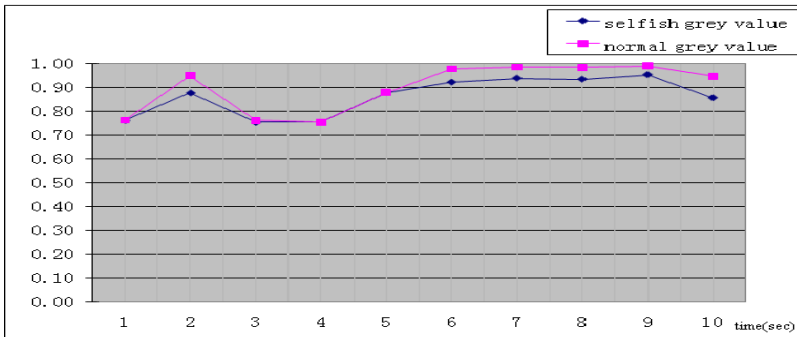
A selfish node's grey trust values (throughput behaviour)



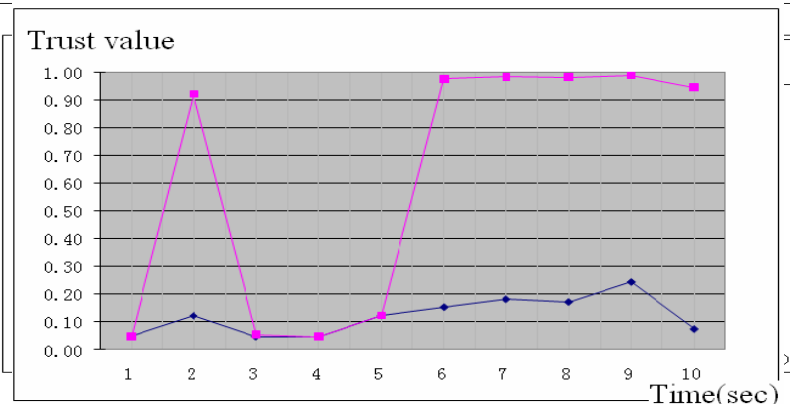
(a) equal weights



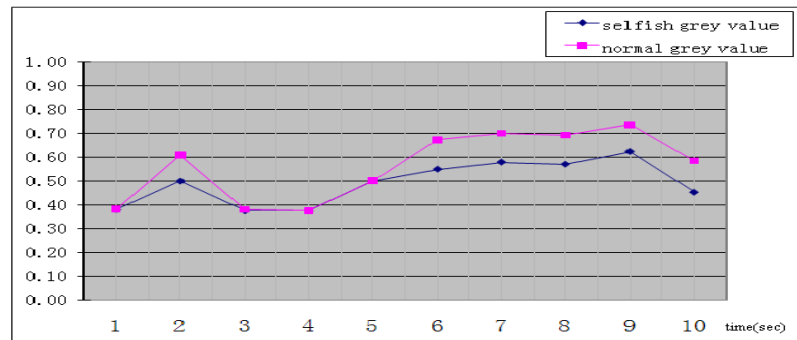
(b) emphasis of PLR



(d) emphasis of delay



(e)



(f) emphasis of data rate

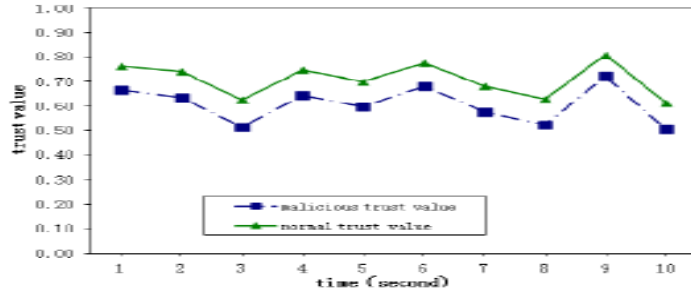
Detecting Attacks

- **The approach not only detects anomalous behaviour**
- **We can use multiple vector sets to discover the most likely strategy that an attacker is employing**
 - **e.g. by altering the signal strength or throughput to selected partners**

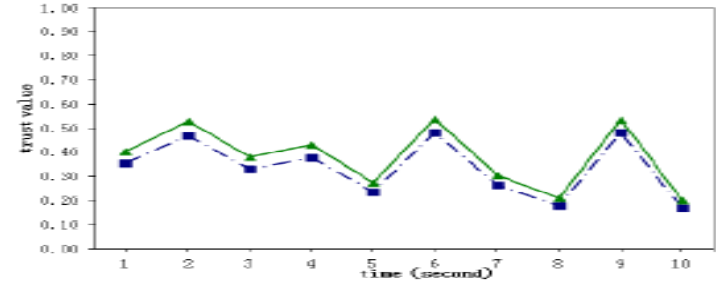
- J Guo, A Marshall, B Zhou, “A Multi-Parameter Trust Framework for Mobile ad hoc Networks”, book chapter: *Security, Privacy, Trust, and Resource Management in Mobile and Wireless Communications*, (IGI global), 2013
- J Guo, A Marshall, B Zhou, “Designing a prediction model as a complement of misbehaviour detection strategies in a multi-parameter trust framework for MANETs”, *Journal of Applied Science and Engineering* FCST-12 Special Issue, accepted for publication, 2013.

A selfish node's grey trust values (throughput behaviour)

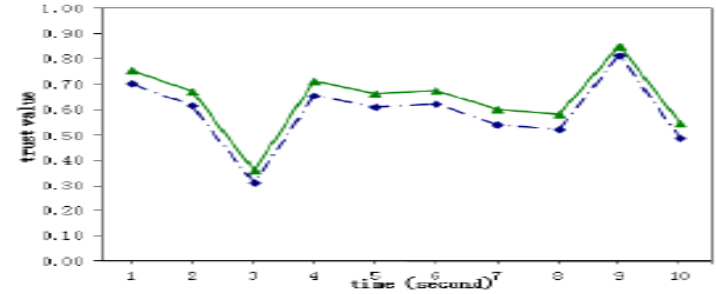
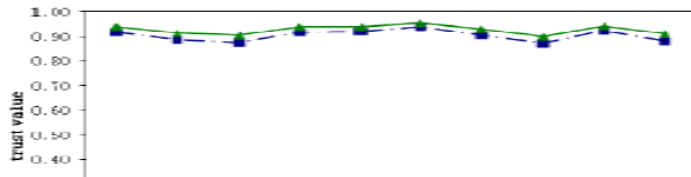
6 mobile nodes



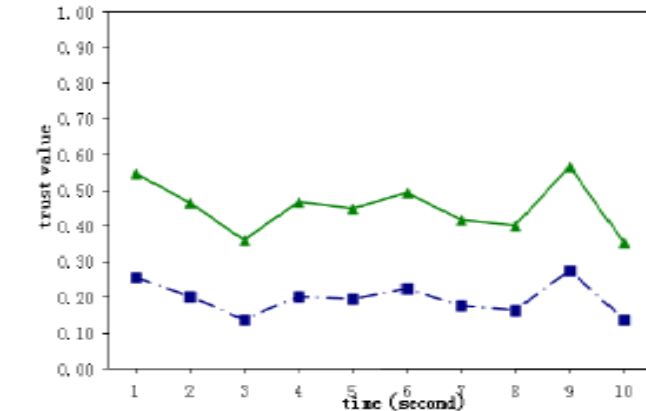
(a) equal weights



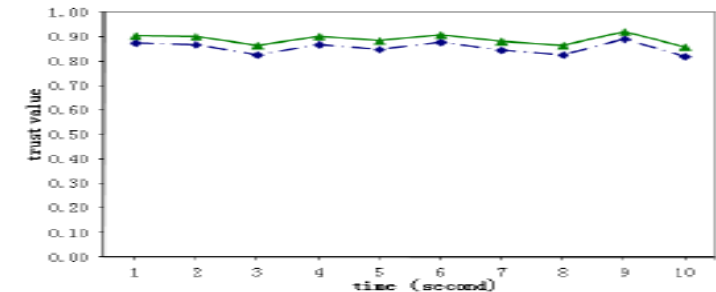
(b) emphasizing PLR



(d) emphasizing delay



(e) emphasizing throughput



(f) emphasizing data rate

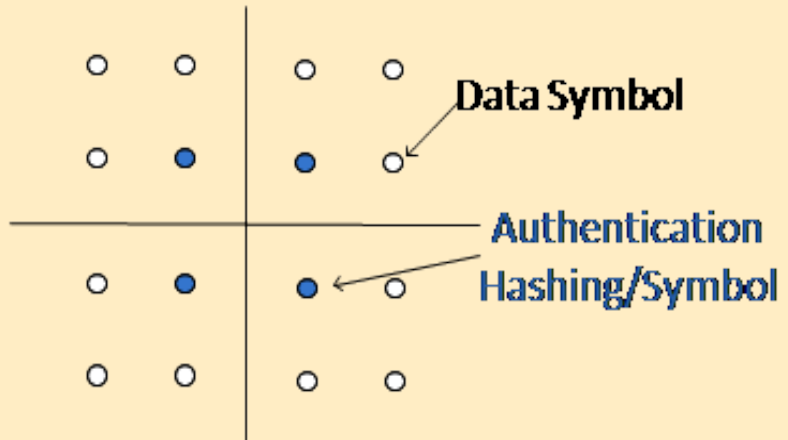
malicious trust values

normal trust values

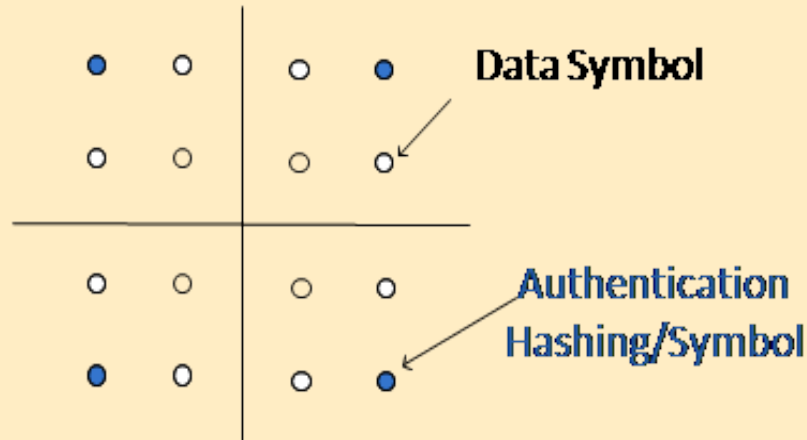
Summary

- **The new TMF employs multiple metrics to calculate a node's trust values**
 - sets a weight vector for each of the input parameters
- **The approach also uses Grey theory and Fuzzy sets to improve the trust value generation algorithms.**
- **Good Discrimination**
 - the simulation results clearly show the difference in the trust values between a normal and selfish node for each specific parameter results show it is resilient to mobility as well

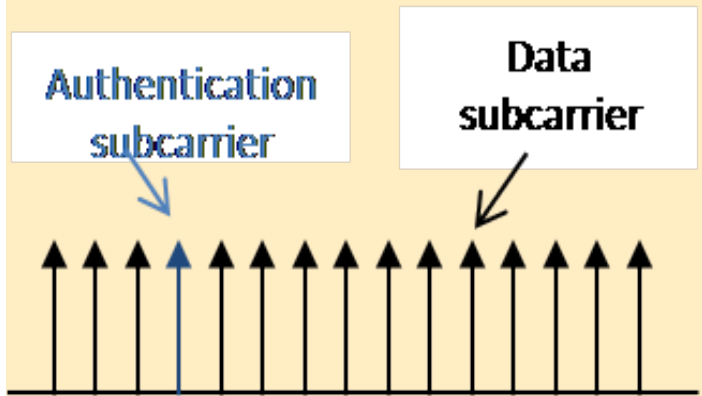
Ongoing Research: Physical Layer Security



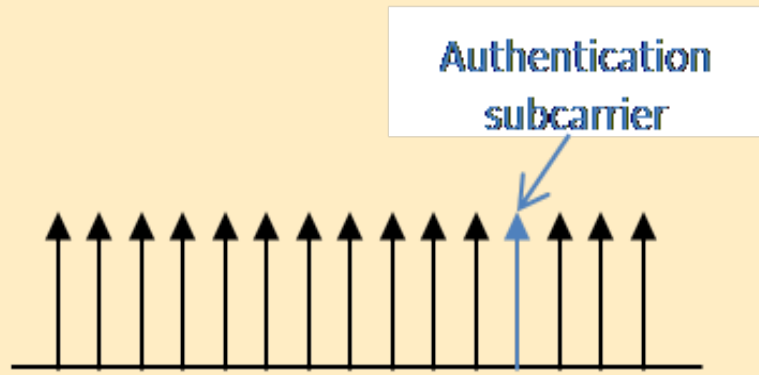
(a) - 16 QAM with symbols reserved for authentication/hashing



(b) - an alternative configuration



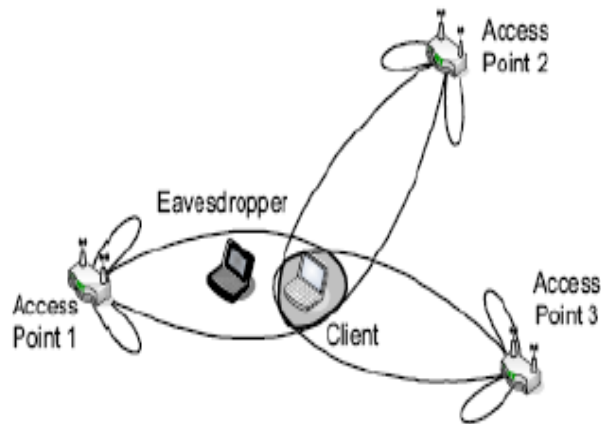
(c) OFDM Channel set (frame n)



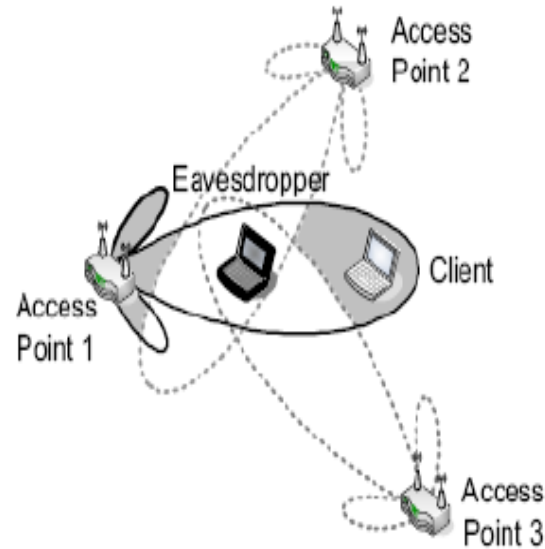
(d) OFDM Channel set (frame $n+1$)

Future Research: Physical Layer Security - Security without Encryption

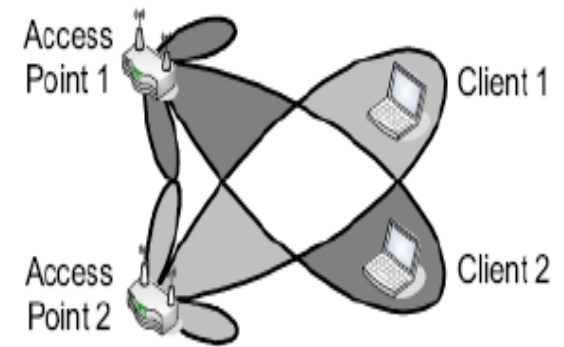
Three strategies



(a) Secret sharing



(b) Controlled jamming



(c) stream overwhelming

That's it, thanks for listening

- any questions?