Protecting wireless computer networks by using intrusion detection agents

Dragan Pleskonjic

CEO & Security Architect at BEG Finsoft
Member of IEEE Computer Society, ACM and ACM SIGSAC
E-mails:
dragan@conwex.org | dragan@computer.org | dragan@finsoft.com

Introduction

- **Wireless networks are forecasted to expand rapidly in coming years**
- Wi-Fi networks defined by IEEE 802.11 standard family (IEEE 802.11a/b/g…) and also mobile networks

Some details and characteristics

- Covers an area i.e. not limited by wire connectivity
- Intruder can stay in covered area and access to network unseen
- Insider and outsider attacks definition used for wired networks should be redefined for wireless networks.
- There is no exact border between internal and external network, i.e. there is no clear perimeter security

The problem

- **Intrusion Threats and Attacks on 802.11networks**

- WLANs vulnerable on usual wired network threats plus some additional

Some wireless specific threats, attacks and vulnerabilities

- Easy access to 802.11 networks
- Unauthorized (“rogue”) access points
- Unauthorized use of service
- Denial-of-service vulnerability
- MAC spoofing and session hijacking
- Relatively easy traffic analysis and eavesdropping

Wireless network are usually targeted with various kinds of threats

- Attacks designed to steal the association and login credentials
- War Driving - Probe requests which don't have the ESSID field set in the probe
- Flooding - attempts to flood the AP with associations
- MAC address spoofing
- Monkey / Hacker jacks
- Null probes
- Null associations
- Floods etc.

Intrusion Detection

- Defined as problem in the early 1980s
- Anderson defines an intrusion as any unauthorized attempt to access, manipulate, modify, or destroy information, or to render a system unreliable or unusable.
- Intrusion detection attempts to detect these types of activities.
- We are going to establish foundations of intrusion detection techniques in order to determine where they are strong and where they need improvement.
- **With wireless networks intrusion detection system (IDS) should be carefully redefined**

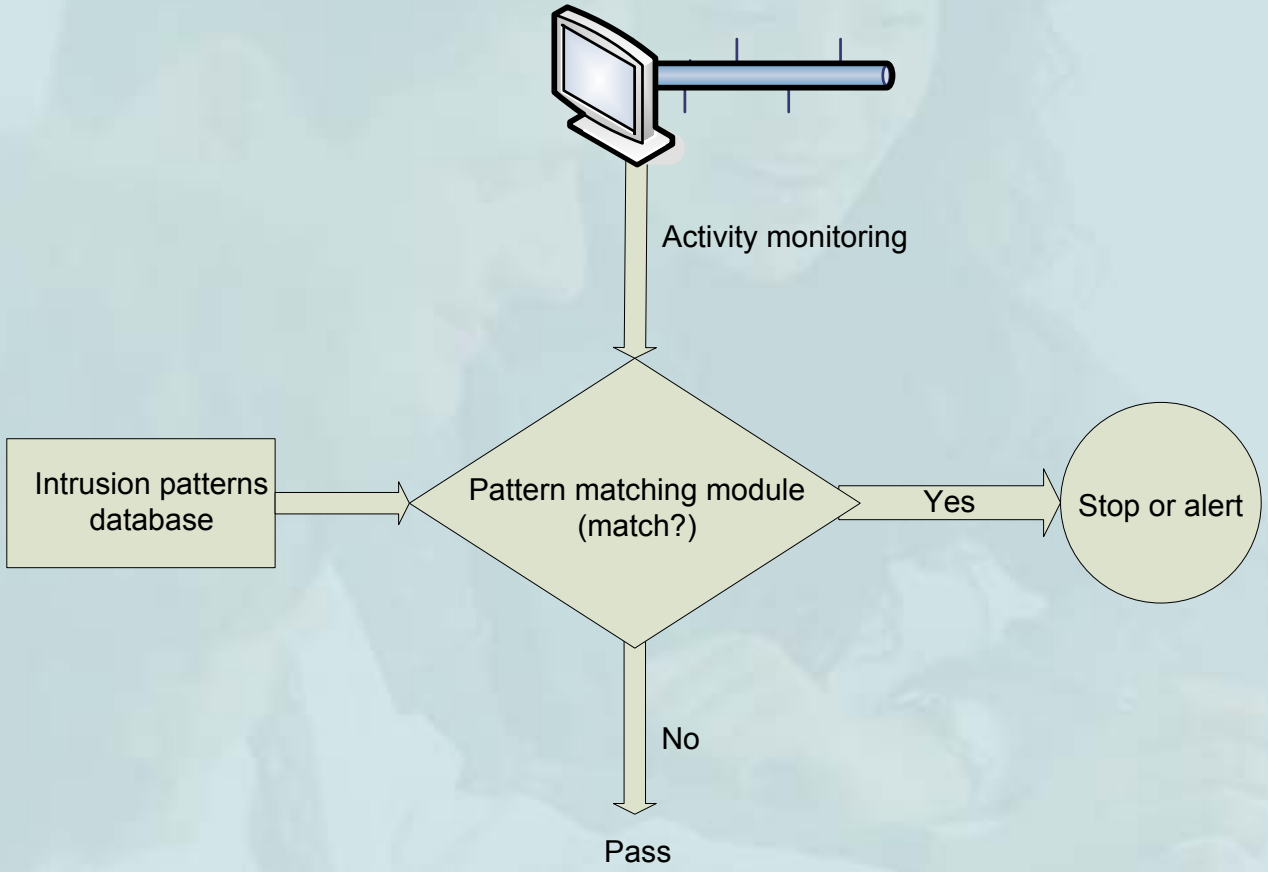
Existing solutions and their problems

- By detection model i.e. what is detected
  - Misuse detection i.e. signature based approaches
  - Anomaly detection
- By scope of protection (or by deployment) i.e. where detected
  - Network Based
  - Host Based
  - Application Based
- When attack is detected
  - Real time
  - After the fact

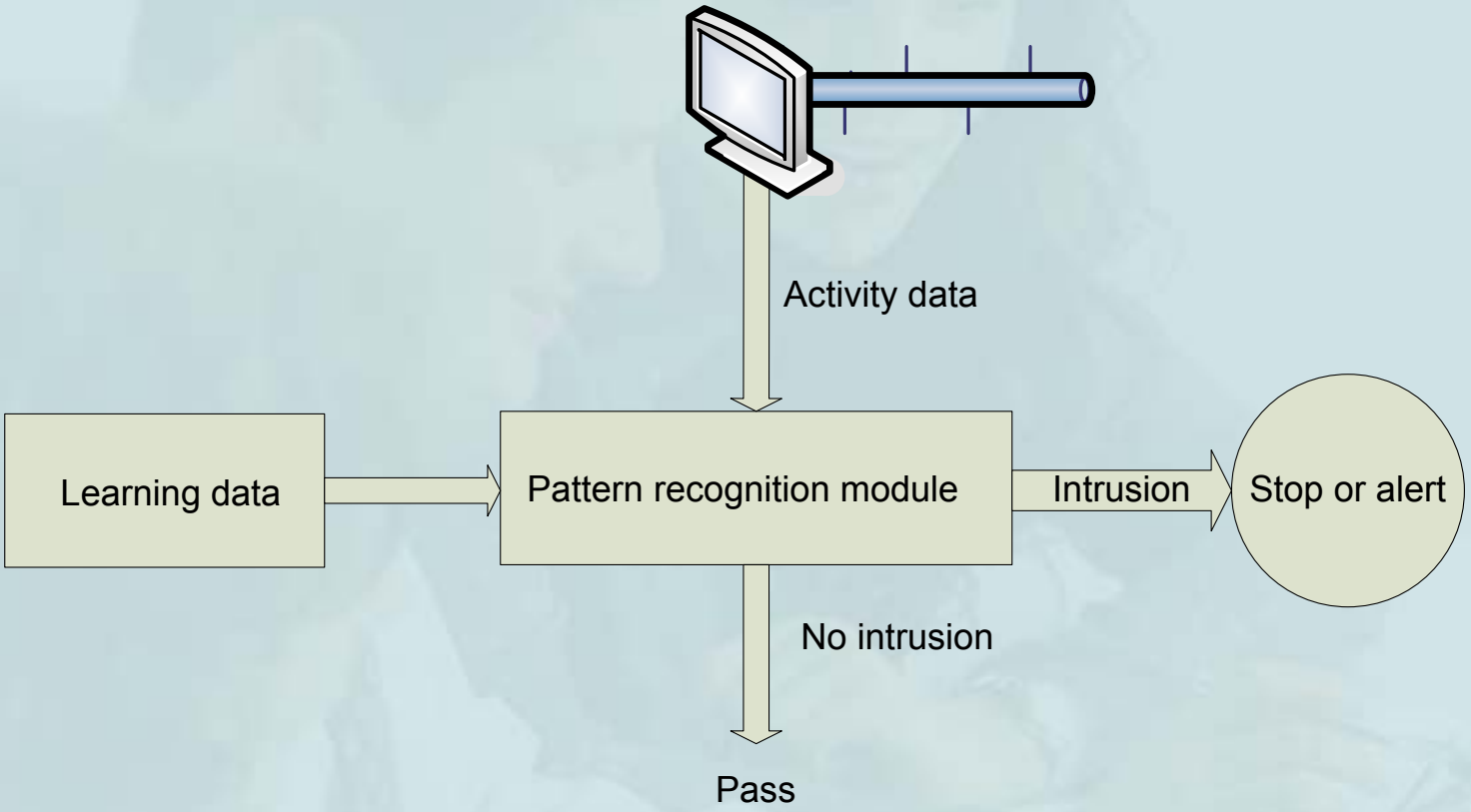
By detection model i.e. what is detected

- Misuse detection i.e. signature based approaches
- Anomaly detection

Misuse detection system



Anomaly detection system



By scope of protection (by deployment) i.e. where detected

- Network Based
- Host Based
- Application Based

When attack is detected

- Real time
- After the fact

Intrusion detection in wireless networks

- Inherent lack of security and experience
- WEP was broken pretty quickly
- Wired – physically attached: intruder / attacker needs to plug directly into the network
- Wireless – intruder can stay anywhere and intrude unseen
- No exact “border” between internal and external network => losing exact classification to insider and outsider attacks

The new idea and solution

- Multilevel and multidimensional architecture
- To make an efficient system to defend the wireless network
- Define attack and intrusion “axioms scope”
- Define conclusions mechanisms (“theorems”)
- Self learning system and anticipation – even if we fail to make a fully intelligent system we can accept some weaker decision points to get the system functional
- Implement attack recognition
- Launch response to defend system or network

Taken approach

- Neural networks and fuzzy logic
- Self learning system (AI - artificial intelligence, neural networks, fuzzy logic…)
- Automatic answer to intrusions
- Defend against new intrusion types (previously unknown or similar but different)
- Local and global answer on attack (intrusion)
- Wireless specific attacks detection

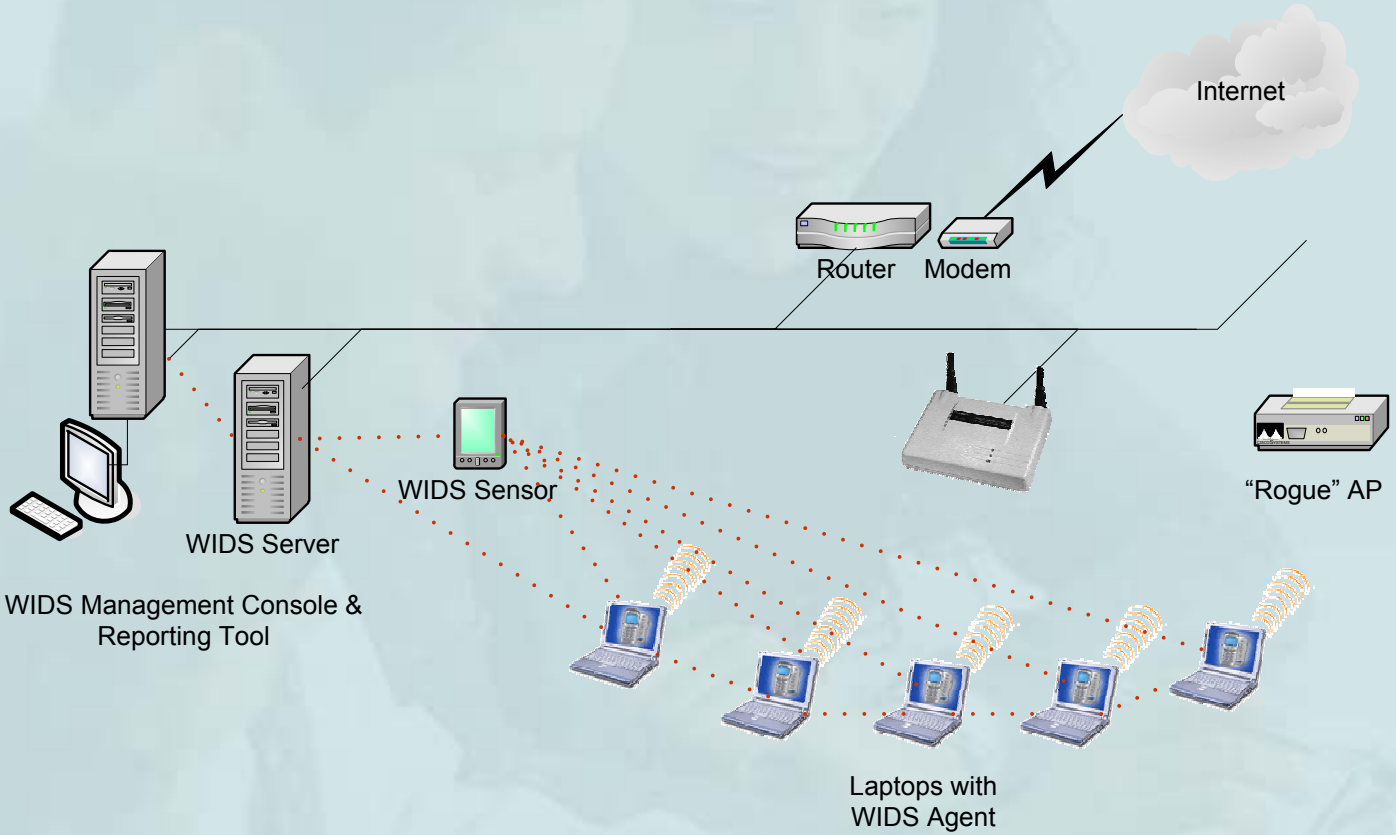
Approach… – continued

- Recognize more attacks
- Autonomy and cooperation of components
- Multidimensional system
- Level of autonomous decision and self defense
- Resistance and denial of new kinds of intrusions
- Providing two kinds of response: Local and global
- Elements of intelligent behavior etc.

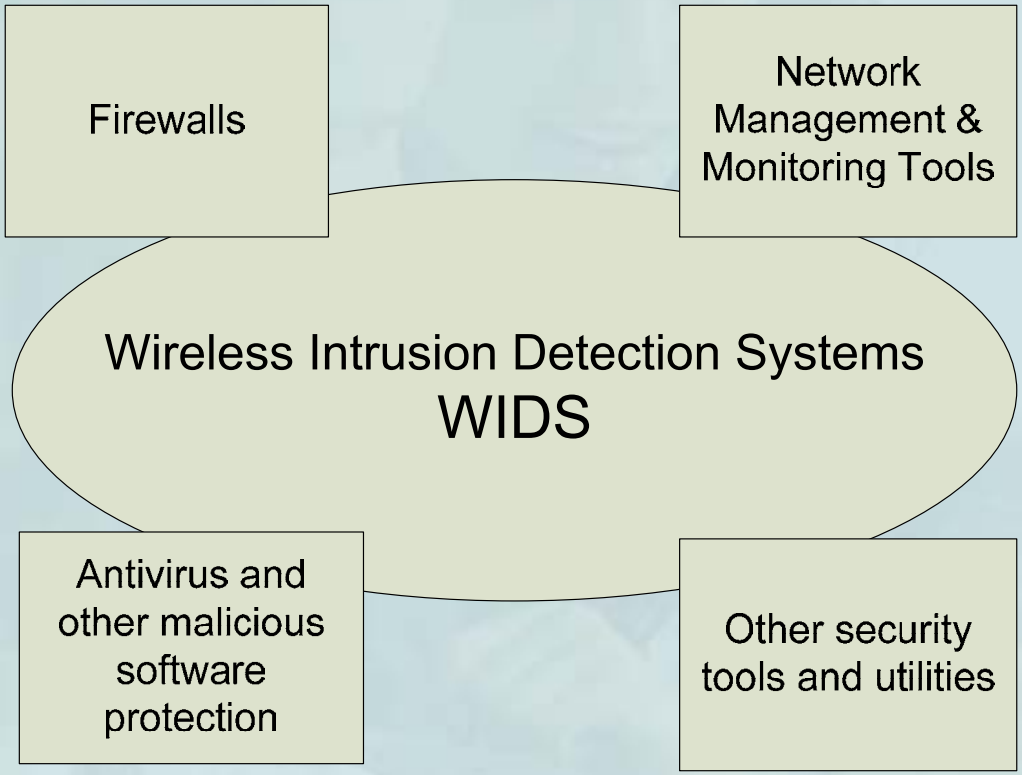
Proposed new system (WIDS)

- WIDS Agent
- WIDS Sensor
- WIDS Server
- WIDS Console & Management, Reporting Tools

WIDS



Relation to other network and security tools and utilities



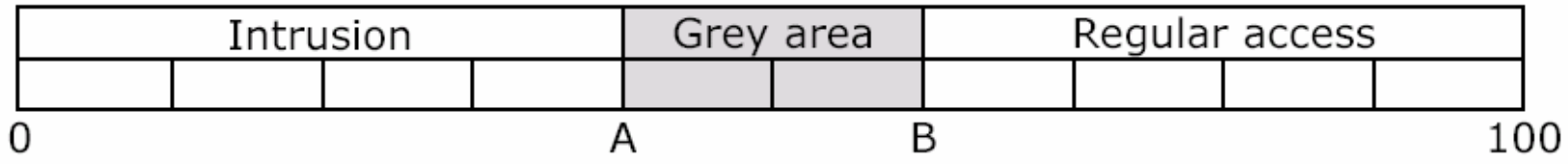
Example of decision scale

[0-A] is for deny access

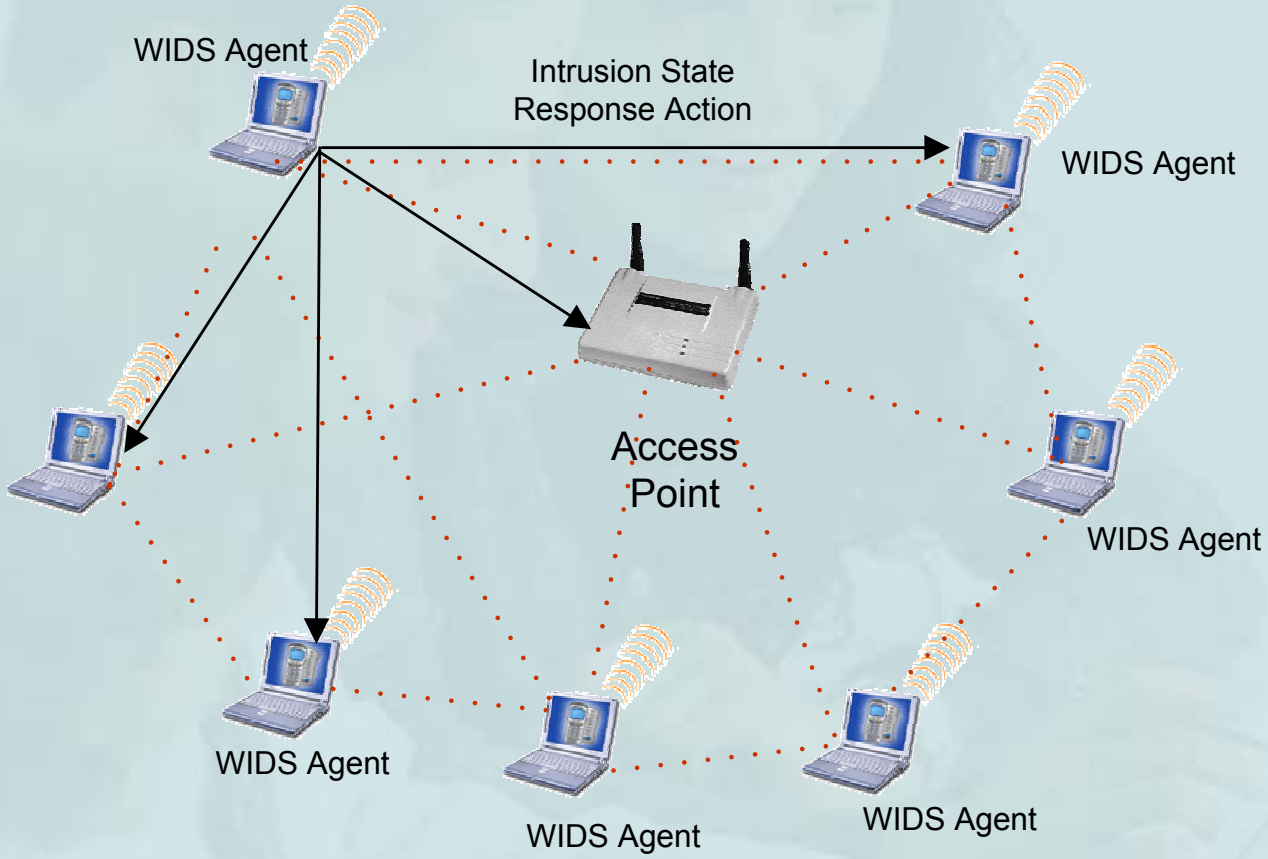
[A-B] requires human or artificial intelligence intervention

[B-1] is for allow access

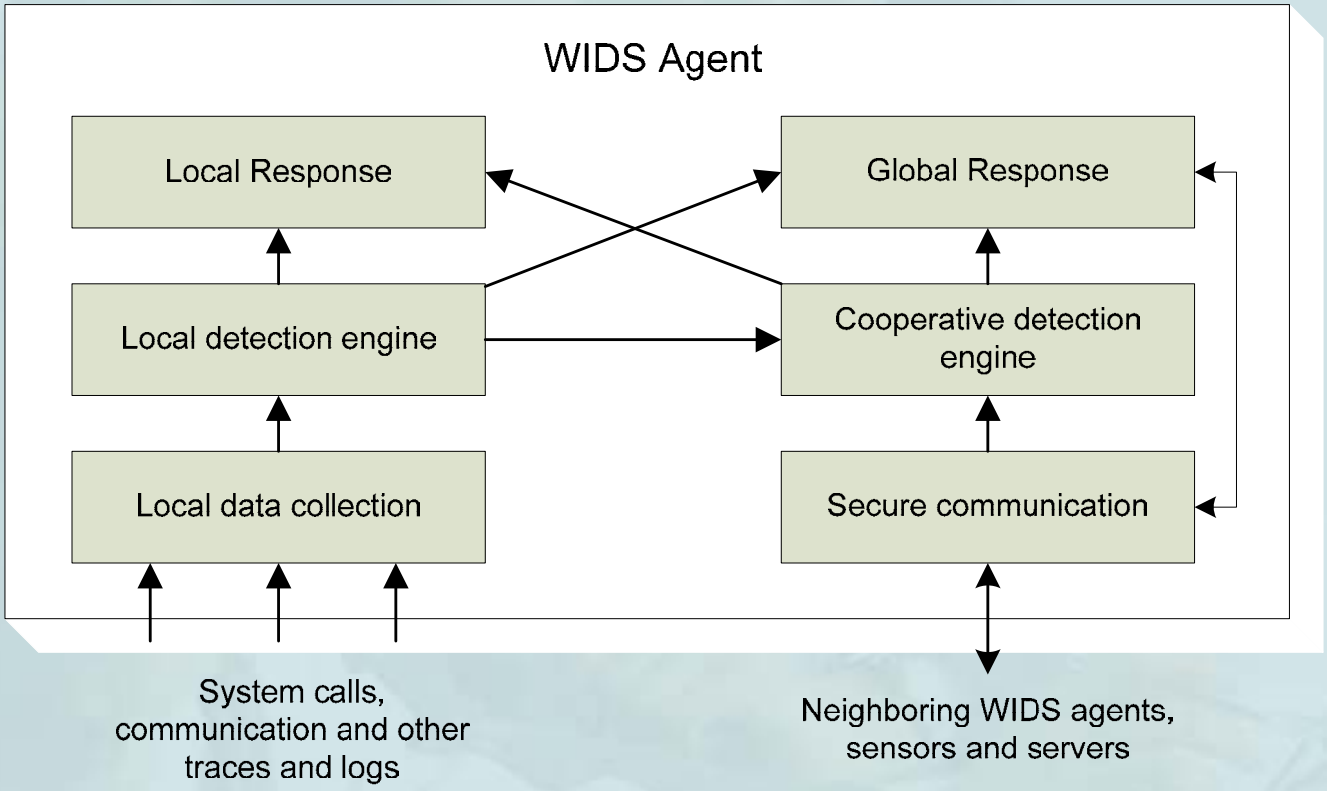
A and B are movable, A ≤ B



WIDS Agent



Conceptual model for a WIDS Agents in ad-hoc network [14]



Achieved results

- This methodology and system is currently under development. Work on developing methodology is done and some steps are completed:
  - Elements for multidimensional and multilevel concept and axioms scope, with defining “theorems” for decision and self learning scope.
  - Partially developed components and elements of system
  - Product family definition and implementation

Achieved results... continued

- Further work to be done:
- To define remaining part of system
- To make proof of concept implementation
- To test single components and system overall
- To gain understanding of the need and solution
- Example: WIDS Agent as part of Operating System (as personal firewall or antivirus tool is at present time)
- Additional work toward intrusion prevention and response

Next product lines / future development

- **WIPS** - Wireless Intrusion Prevention System
- **MIDS** - Mobile Intrusion Detection System
- **MIPS** - Mobile Intrusion Prevention System

- Bayesian probability and statistical theory
- Modal logic

Conclusions

- Wireless networks are growing very fast, but they are still vulnerable to different kind of attacks.
- This paper presents kind of new approach with usage wireless intrusion detection systems (WIDS) of components: agent, sensor, server and additional management and reporting tool.
- WIDS, as presented in this paper, is multilevel and multidimensional system and will include these components with built in neural network and / or fuzzy logic technology.
- This gives capabilities of autonomy, self-learning and decision about response against attacker.
- System is under development and some of parts are in early stage. There is further work to be done in order to achieve this goal.

Questions?

- Thank you for your patience
- Questions?

Additional info

- My security blog:

  http://www.conwex.info/blog/
- About me:

  http://www.conwex.info/Dragan_Pleskonjic.html