A robust SNMP based Infrastructure for Intrusion Detection and Response in tactical MANETs

Sascha Lettgen
University of Bonn, Germany
Inst. of Computer Science IV

Marko Jahnke, Jens Tölle, Uwe Weddige, Michael Bussmann
FGAN/FKIE, Wachtberg, Germany
Computer Networks Dept.

July 2006

Outline

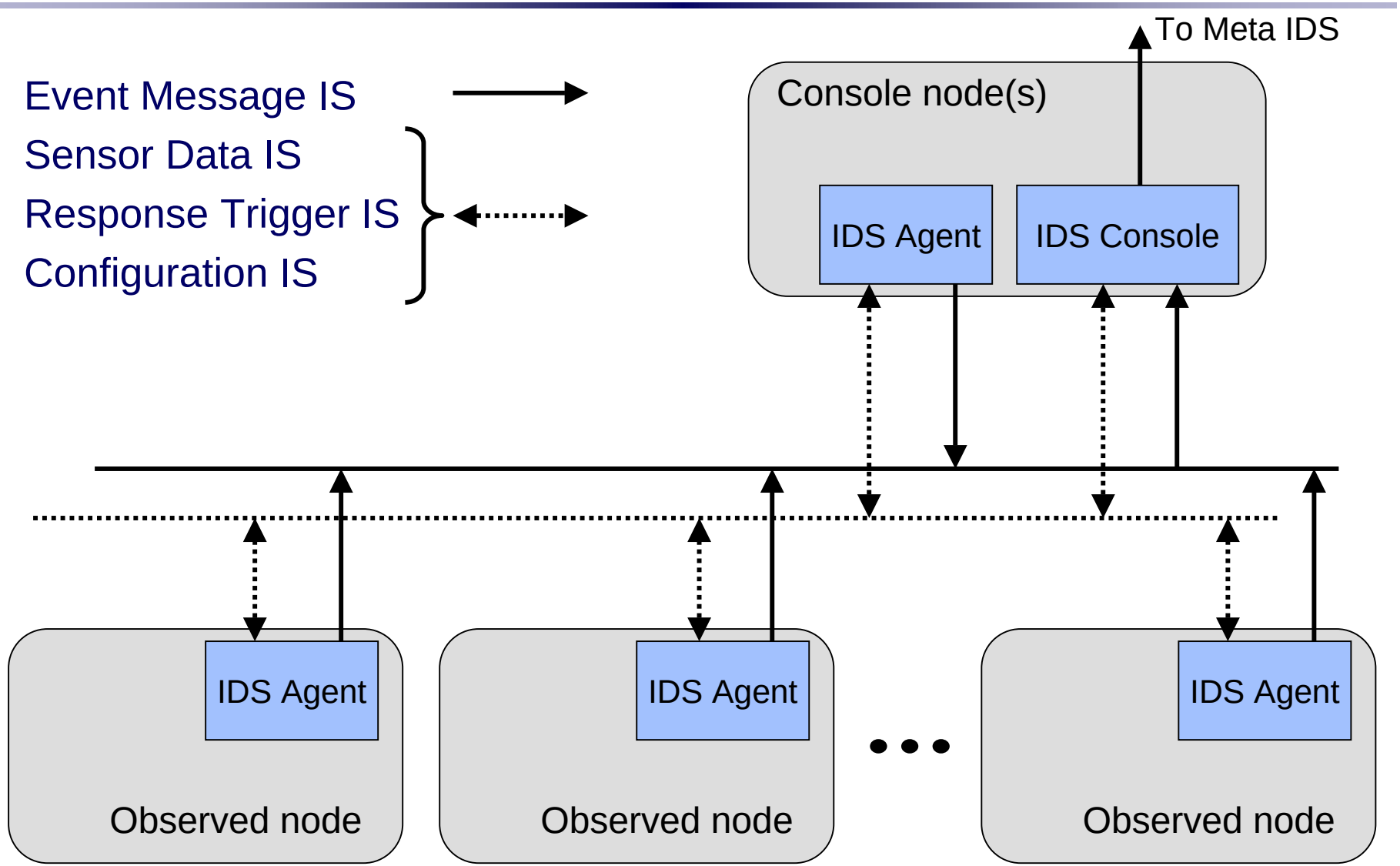
- Introduction
- Deployment Scenario: Tactical MANETs
- Network Management Domain: SNMP
- Modelling IDS Infrastructures w/ SNMP
- Performance Simulation
- Implementation Status
- Conclusions & Further Work

Terminology: Distributed IDS Components

- Agent
  - Sensors
  - Detectors
  - Responders
  - Message processing modules
- Console
  - Message consolidation
  - Databases
  - Correlation engines
  - Other analysis modules

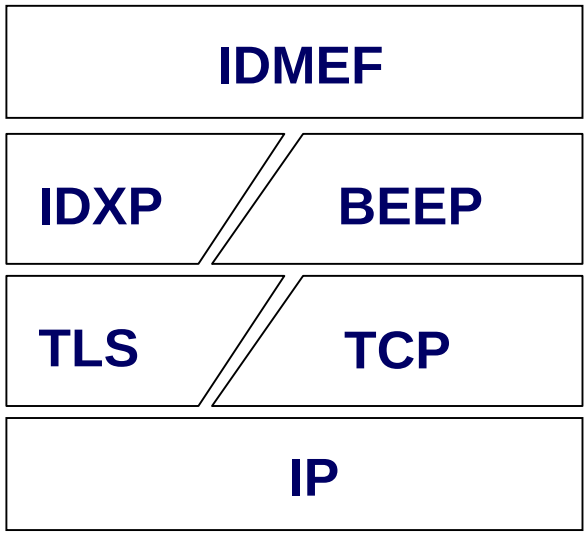
Types of IDS Infrastructures

- Event Message IS
- Sensor Data IS
- Response Trigger IS
- Configuration IS



Existing Data Models & Communication Protocols

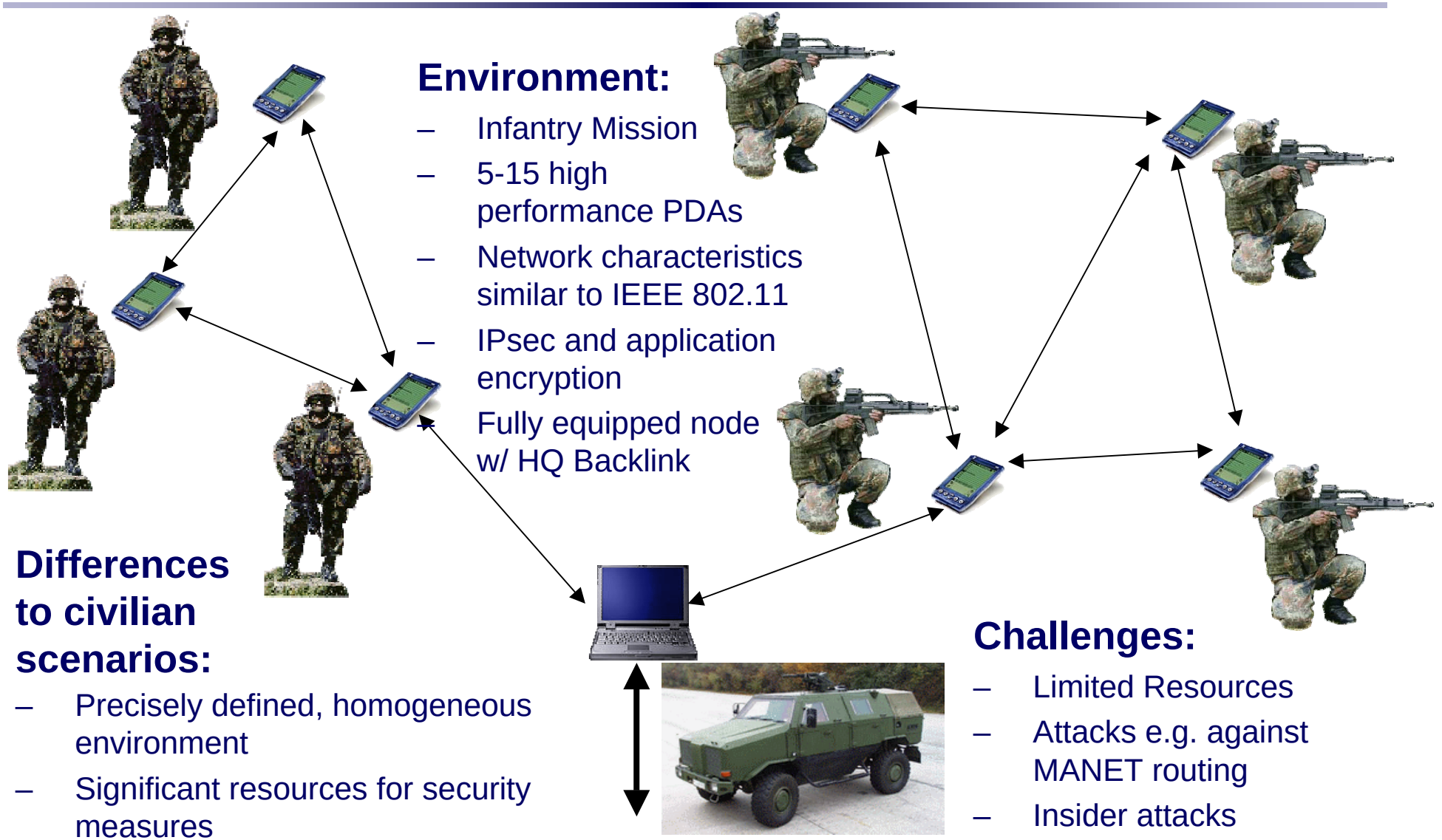
- IETF IDWG Recommendations



- **Drawbacks:** Overhead
  - TCP/SSL/BEEP Handshakes
  - Channel Management
  - XML Encoding

```
<IDMEF-Message version="1.0">
  <Alert ident="abc123456789">
    <Analyzer analyzerid="hq-dmz-analyzer01">
      <Node category="dns">
        <location>Headquarters DMZ Network</location>
        <name>analyzer01.example.com</name>
      </Node>
    </Analyzer>                                   who reports
    <CreateTime ntpstamp="0xbc723b45.0xef449129">
      2000-03-09T10:01:25.93464-05:00
    </CreateTime>                                 when
    <Source ident="a1b2c3d4">
      <Node ident="a1b2c3d4-001" category="dns">
        <name>badguy.example.net</name>
        <Address ident="a1b2c3d4-002" category="ipv4-net-mask">
          <address>192.0.2.50</address>
          <netmask>255.255.255.255</netmask>
        </Address>
      </Node>
    </Source>                                     who
    <Target ident="d1c2b3a4">
      <Node ident="d1c2b3a4-001" category="dns">
        <Address category="ipv4-addr-hex">
          <address>0xde796f70</address>
        </Address>
      </Node>
    </Target>                                     where
    <Classification origin="bugtraqid">
      <name>124</name>
      <url>http://www.securityfocus.com</url>
    </Classification>                             what happened
  </Alert>
</IDMEF-Message>
```

Deployment Scenario: Tactical MANETs



Environment:

- Infantry Mission
- 5-15 high performance PDAs
- Network characteristics similar to IEEE 802.11
- IPsec and application encryption
- Fully equipped node w/ HQ Backlink

Differences to civilian scenarios:

- Precisely defined, homogeneous environment
- Significant resources for security measures

Challenges:

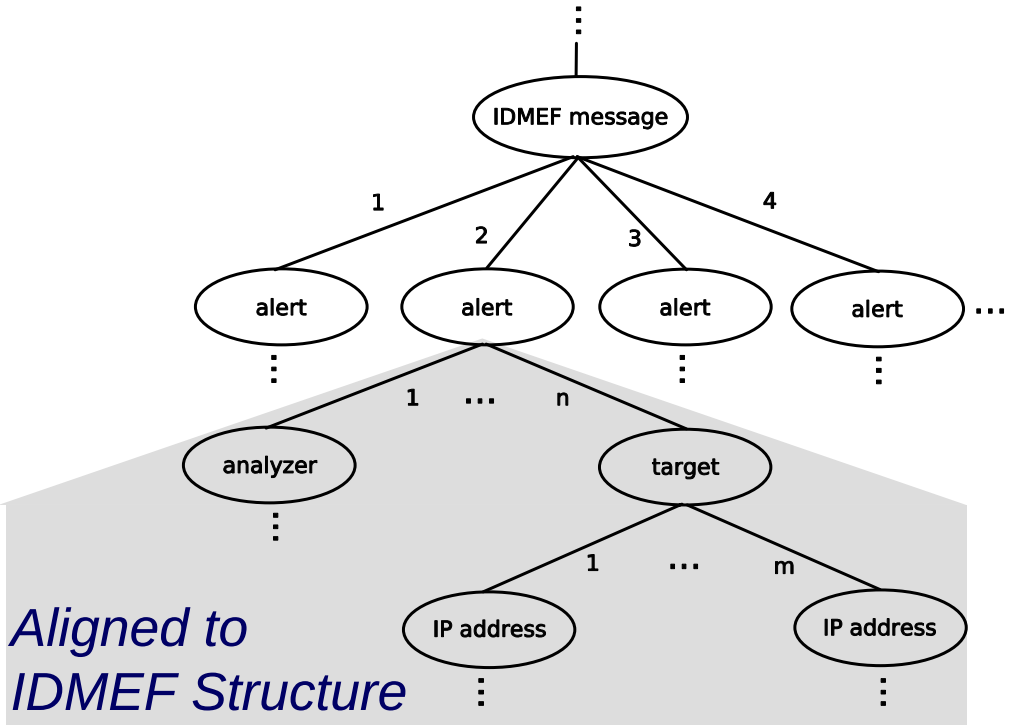
- Limited Resources
- Attacks e.g. against MANET routing
- Insider attacks

Management Domain: SNMPv3

- Monitoring & Configuration
- Agent/Manager based concept
- UDP based
- Security in SNMPv3
- Management Information Base (MIB)
- Object and Instance Identifier (OID/IID)
- get/setValue Requests (single value, list or bulk)
- Traps and Notifications

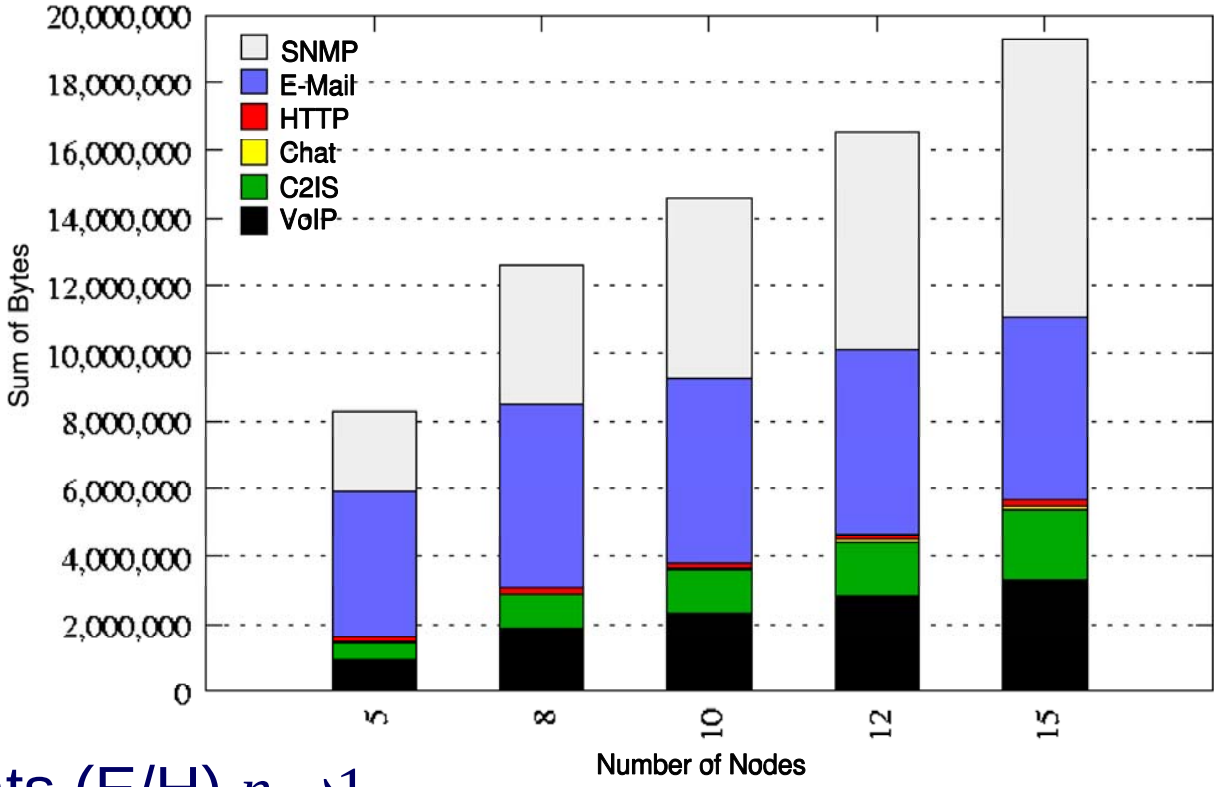
Modeling IDS Infrastructure w/ SNMP

- **Sensor IS**
  - getValue
  - getNext / Bulk
- **Response Trigger IS**
  - setValue
- **Configuration IS**
  - get/setValue
- **Message IS**
  - Insert new alerts into MIB as single subtree structure
  - Send an acknowledged notification to console, containing most important fields
  - Console may request additional message fields



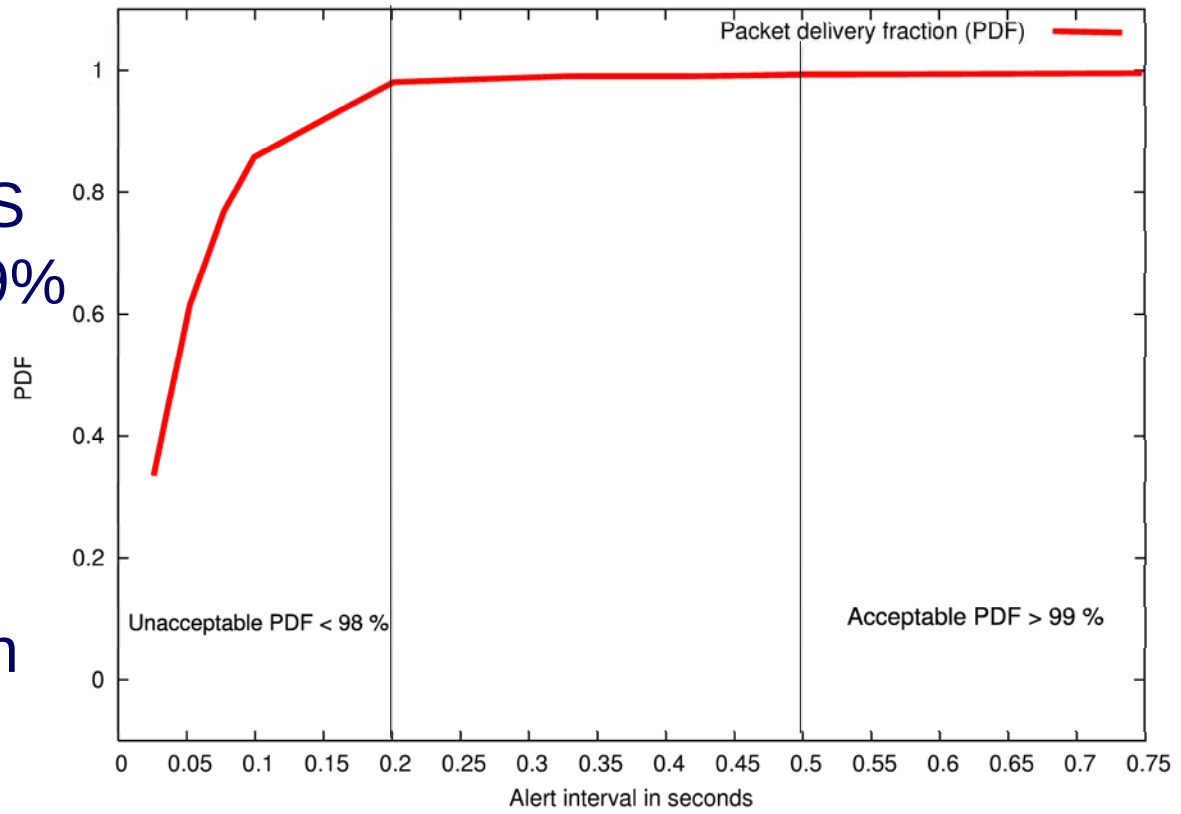
Performance Simulations (1): Overall Traffic

- Network
  - IEEE 802.11b
- Applications
  - VoIP (2.4 kbit/s)
  - C2IS (JMS)
  - UChat
  - SMTP/HTTP
- IDS Messages
  - Events/Heartbeats (E/H) $n \rightarrow 1$
  - Neighborhood Watching (NW) $n \rightarrow m$
  - Traffic Statistics (TS) $n \rightarrow 1$



Performance Simulations (2): Packet Delivery

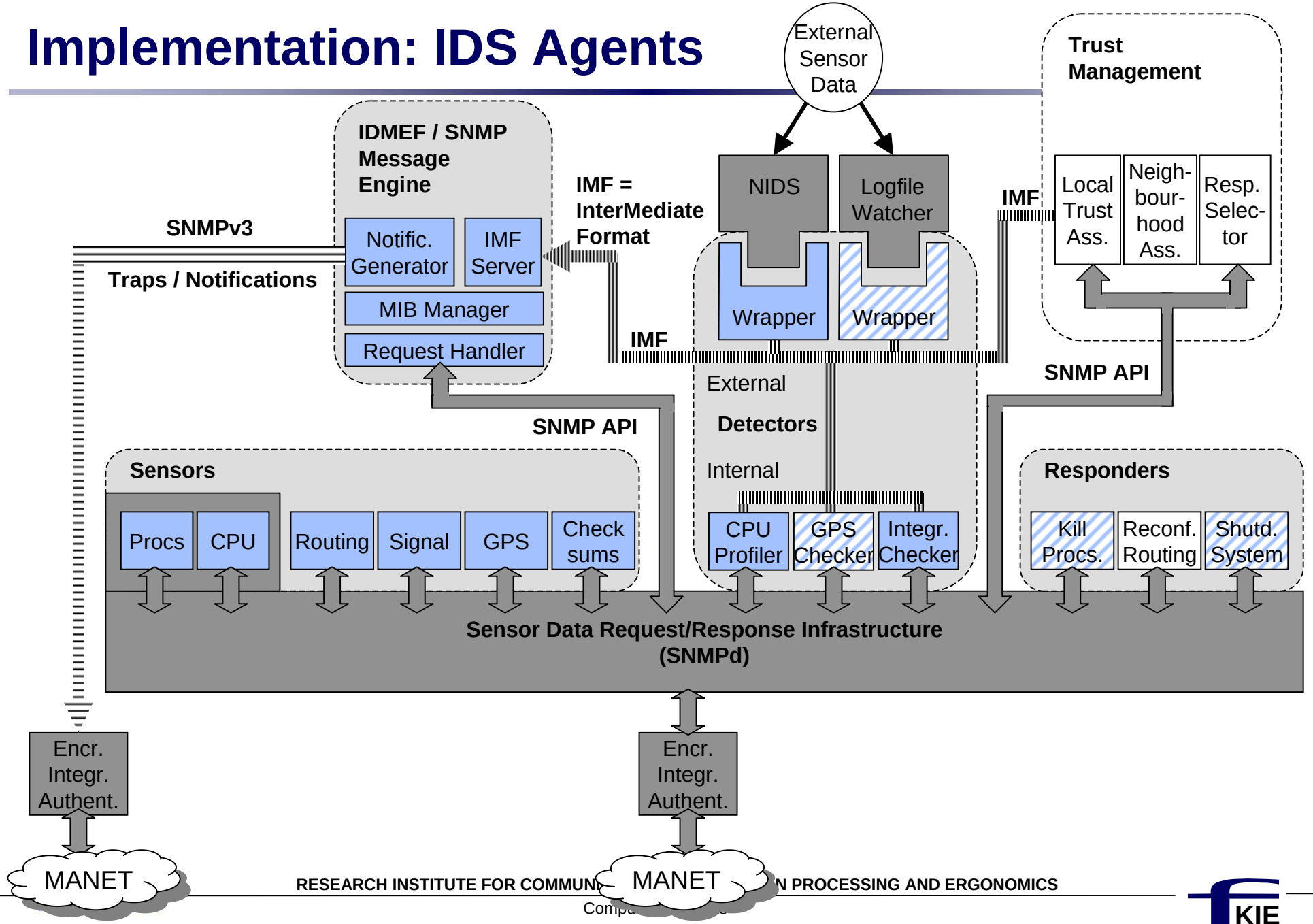
- PDF decreases due to significant amount of IDS traffic
- Maximum rates for IDS Messages for PDF>99%
  - E/H: 2 Hz
  - NW: 0.1 Hz
  - TS: 0.1 Hz
- Higher packet loss can be expected in reality:
  - Buffer overflows
  - Radio interference



Advantages of SNMP approach

- Characteristics of MANETs are considered
  - Dynamic behaviour and short link lifetimes
    - ➢Connectionless and robust communication
  - Low CPU performance and limited battery capacity
    - ➢Lightweight protocol and architecture
- Compatibility w/ existing protocols & data models
    - ➢(Meta-)IDS-interconnection
    - ➢Integration into SNMP Management Frameworks
- Free configurability for different IDS setups due to different deployment scenarios and network sizes
- Usage of existing products for message transport and security

Implementation: IDS Agents



Conclusions & Further Work

- Current IDS infrastructure protocols do not meet the requirements of tactical MANETs.
- SNMPv3 provides mechanisms for implementing all necessary types of IDS infrastructures.
- Development of architecture components
- Prototypical implementation
  - Sensor / detector / responder infrastructure
  - Dynamic storage of IDS event messages in the Management Information Base (MIB)
- Further Work:
  - Integration of more sensors / detectors / responders
  - Anomaly detection approach for traffic statistics

Questions?

Implementation (2): Event Message Handling