Discovering Flaws in IDS through Analysis of their Inputs

Raphaël Jamet and Pascal Lafourcade

Verimag, Université de Grenoble

October 14, 2013

Outline

Introduction

IDS inputs

A model to formally discover flaws in IDS

Examples

Wireless Ad-Hoc Networks (WANET)

- A multi-hop network based on wireless communications
  - Nodes may join, leave, move, ...
  - Anyone may be able to join (open network)
  - Communications may be overheard and/or jammed

Wireless Ad-Hoc Networks (WANET)

- A multi-hop network based on wireless communications
  - Nodes may join, leave, move, ...
  - Anyone may be able to join (open network)
  - Communications may be overheard and/or jammed

- All nodes are routers, and should cooperate.
  - Possibly no central trusted authority
  - Some nodes may be malicious

Wireless Ad-Hoc Networks (WANET)

- A multi-hop network based on wireless communications
  - Nodes may join, leave, move, ...
  - Anyone may be able to join (open network)
  - Communications may be overheard and/or jammed
- All nodes are routers, and should cooperate.
  - Possibly no central trusted authority
  - Some nodes may be malicious

Answers: secure hardware and protocols; Intrusion Detection Systems

What is an Intrusion Detection System (IDS) ?

An IDS is made of three parts:

- **Inputs**, which monitor specific behaviors or metrics.
- **Decision mechanisms**, to judge if the inputs show an attack or anomaly.
- **Response mechanisms**, to mitigate the attack and prevent further damage.

What is an Intrusion Detection System (IDS) ?

An IDS is made of three parts:

- **Inputs**, which monitor specific behaviors or metrics.
- **Decision mechanisms**, to judge if the inputs show an attack or anomaly.
- **Response mechanisms**, to mitigate the attack and prevent further damage.

We focus only on the inputs used in IDS for ad-hoc networks.

Outline

Introduction

IDS inputs

A model to formally discover flaws in IDS

Examples

Examples of inputs

- Traffic analysis
- Retransmission monitoring
- Received signal strength modelization
- Collaboratively mapping the network to locate wormholes
- ...

Classification : level of cooperation and source of the data

a. **Local** inputs,
b. Inputs requiring **k-neighborhood-wide cooperation**,
c. Inputs requiring **global cooperation**

1. **Offline** inputs,
2. **Topological** inputs,
3. **Radio** inputs,
4. **Routing** inputs,
5. Inputs extracted from the application **data**

Classification summary

Data source	Offline	Topology	Radio	Routing	Data
Local	[?]	[?, ?, ?, ?, ?]	[?, ?, ?] [?, ?, ?]	[?, ?, ?, ?, ?] [?, ?, ?, ?]	[?]
Neighborhood	[?]	[?, ?]	X	[?]	[?]
Global	X	[?, ?]	X	[?]	?

- A few under-represented categories (monitoring the application data)
- Some are justifiably empty (radio inputs are only relevant locally)

Observations

- Some of these inputs are well-defined, and are common to several IDS.
- Most of them are useful only against specific intruder behaviors, in specific conditions.

Observations

- Some of these inputs are well-defined, and are common to several IDS.
- Most of them are useful only against specific intruder behaviors, in specific conditions.
- An attacker will follow roughly the same steps to mount an attack on most ad-hoc networks.

Observations

- Some of these inputs are well-defined, and are common to several IDS.
- Most of them are useful only against specific intruder behaviors, in specific conditions.

- An attacker will follow roughly the same steps to mount an attack on most ad-hoc networks.

We can make a common model to check if given inputs are enough to prevent such attacker steps.

Outline

Introduction

IDS inputs

A model to formally discover flaws in IDS

Examples

Overview

1. We first build a map of attack steps (anomalies), with paths (rules).
2. The IDS's inputs correspond to a set of anomalies.
3. We identify assumptions about the network, protocol and attacker (facts).
4. We define an attacker goal (an anomaly).
5. If there exists a path from given inputs, to the attacker goal, that does not go through any anomaly monitored by an input, then the attacker may be able to bypass the IDS.

Facts

Facts are assumptions about the network, protocols and attackers.

- *HopConfidentiality*
- *OpenNetwork*
- *DirAntenna*

Anomalies

Anomalies are the results of the attacker's behavior, and are used to describe the different steps in an attack.

- *NeighborVisibleSuppression*
- *ApplicationDataAltered*
- *DirImpersonation*

Rules

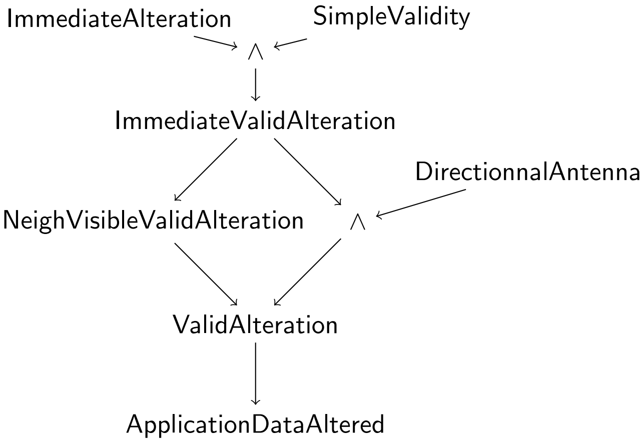
Rules describe how the attacker can leverage anomalies or inputs to produce further anomalies.

- $\mathit{NoConfidentiality} \rightarrow \mathit{Snooping}$
- $\mathit{Suppression} \rightarrow \mathit{ApplicationDataAltered}$
- $\mathit{SimpleValidity} \wedge \mathit{ImmediateAlteration} \rightarrow \mathit{ImmediateValidAlteration}$

Attacker graph

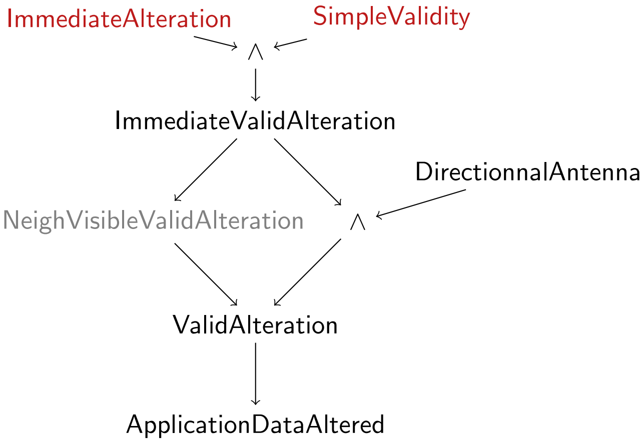
These three components describe a sort of graph, where nodes are anomalies, and directed edges are rules. To find attacks is to find paths going from x to y without passing by z.

Partial attack map



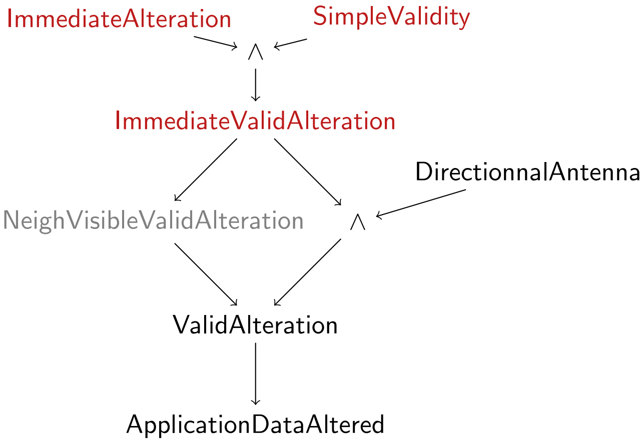
Example : simple alteration

Can promiscuous integrity checks prevent the alteration of data in messages being retransmitted ?



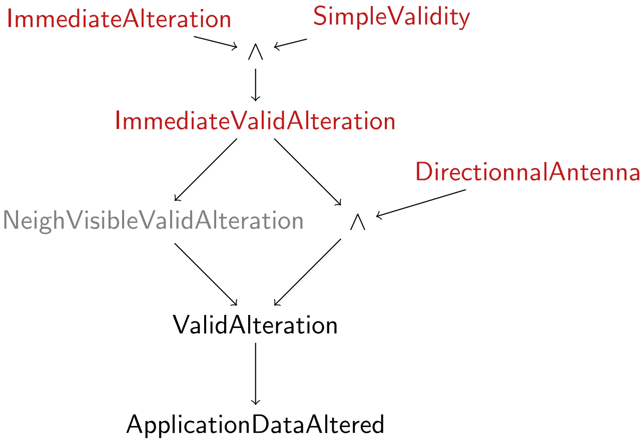
Example : simple alteration

Can promiscuous integrity checks prevent the alteration of data in messages being retransmitted ?



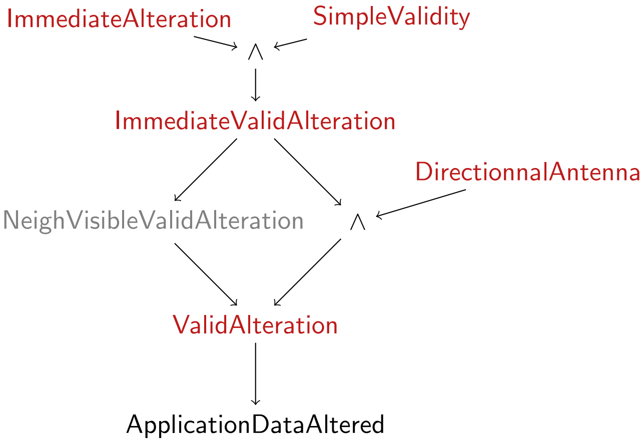
Example : simple alteration

Can promiscuous integrity checks prevent the alteration of data in messages being retransmitted ?



Example : simple alteration

Can promiscuous integrity checks prevent the alteration of data in messages being retransmitted ?



ImmediateAlteration

SimpleValidity

$\wedge$

ImmediateValidAlteration

DirectionnalAntenna

NeighVisibleValidAlteration

$\wedge$

ValidAlteration

ApplicationDataAltered

Outline

Introduction

IDS inputs

A model to formally discover flaws in IDS

Examples

Application to IDS from the litterature

We applied our model to two IDS from the litterature.

- Ilker Onat and Ali Miri, *A Real-Time Node-Based Traffic Anomaly Detection Algorithm* [**?**] — we'll present it now
- Ana Paula R. da Silva, Marcelo H. T. Martins, Bruno P. S. Rocha, Antonio A. F. Loureiro, Linnyer B. Ruiz and Hao Chi Wong, *Decentralized Intrusion Detection* [**?**] — analysis in the paper

A Real-Time Node-Based Traffic Anomaly Detection Algorithm [?]

An anomaly-based IDS based on two inputs.

- For each neighbor, received signal strength should stay stable

- Packet arrival rates should stay stable

A Real-Time Node-Based Traffic Anomaly Detection Algorithm [?]

An anomaly-based IDS based on two inputs.

- For each neighbor, received signal strength should stay stable
  - Nodes cannot move
  - Nodes cannot be impersonated without adjusting transmission power
- Packet arrival rates should stay stable
  - Attackers cannot add messages
  - Attackers cannot remove messages

A Real-Time Node-Based Traffic Anomaly Detection Algorithm [?]

An anomaly-based IDS based on two inputs.

- For each neighbor, received signal strength should stay stable
  - Nodes cannot move
  - Nodes cannot be impersonated without adjusting transmission power
- Packet arrival rates should stay stable
  - Attackers cannot add messages
  - Attackers cannot remove messages

Their IDS prevents $\mathbf{A}_I = \{\ \mathit{Suppression}, \mathit{Insertion}, \mathit{OmniImpersonation}, \mathit{DirImpersonation}\ \}$.

A Real-Time Node-Based Traffic Anomaly Detection Algorithm [?]

They make several hypothesis:

- The routing protocol is based on a tree (such as GBR),
- Nodes are static,
- Nodes can uniquely identify neighbors,
- All nodes use the same hardware and software,
- All nodes use constant transmission power.

A Real-Time Node-Based Traffic Anomaly Detection Algorithm [?]

They make several hypothesis:

- The routing protocol is based on a tree (such as GBR),
- Nodes are static,
- Nodes can uniquely identify neighbors,
- All nodes use the same hardware and software,
- All nodes use constant transmission power.

We select the following facts: $\mathbf{F}_I = \{ \textit{CanImpersonate, DirAntenna} \}$.

A Real-Time Node-Based Traffic Anomaly Detection Algorithm [?]

We ran three analysis:

1. According to their hypothesis, can an intruder impersonate nodes ?
2. According to their hypothesis, can an intruder alter application data ?

3. Going further than their hypothesis, can an intruder alter application data ?

A Real-Time Node-Based Traffic Anomaly Detection Algorithm [?]

We ran three analysis:

1. According to their hypothesis, can an intruder impersonate nodes ?
2. According to their hypothesis, can an intruder alter application data ?
    - An attacker cannot have a node able to do any of this, as it cannot associate in the network.
3. Going further than their hypothesis, can an intruder alter application data ?

A Real-Time Node-Based Traffic Anomaly Detection Algorithm [?]

We ran three analysis:

1. According to their hypothesis, can an intruder impersonate nodes ?
2. According to their hypothesis, can an intruder alter application data ?
    - An attacker cannot have a node able to do any of this, as it cannot associate in the network.
3. Going further than their hypothesis, can an intruder alter application data ?
    - The paper did not mention anything about node compromise, through for instance a virus, and it did not either specify any cryptographic protection of packets. Therefore, if we suppose *CanCompromise* and *NoValidity*, there are no inputs detecting intruders that compromise an honest node, and alter the data they reforward.

Prototype

A tool based on this model is available at
`http://www-verimag.imag.fr/~rjamet/IDS/`.

```
[rjamet@dinah Proto]$ ./proto.pl +CanImpersonate +DirAntenna +TxPowAdjust
-Suppression -Insertion -OmniImpersonation -DirImpersonation %Impersonation
  [?]  Proto :  usage ./proto.pl [%TargetAnomaly] +Fact1 +Fact2 -Anomaly1
-Anomaly2
  [...]
  ...  Reaching TxPowImpersonation using rule PowI from (TxPowAdjust and
CanImpersonate)
  ...  Reaching DirTxPowImpersonation using rule DirPowI from (TxPowAdjust and
DirAntenna and CanImpersonate)
  ...  Reaching Impersonation using rule TtoI from (TxPowImpersonation)
  [+] Finished :  reached Impersonation, there is an undetected attack using our
model.
```

A first step towards automated IDS analysis

We think that the model is solid, but the trust lies in the attack map:

A first step towards automated IDS analysis

We think that the model is solid, but the trust lies in the attack map:

- We assumed reasonable protocol properties, which may not be specific enough
- Attacks not modeled in the map will not be detected
- Disponibility attacks are tricky to model
- Not enough details on the radio and MAC side of things

A first step towards automated IDS analysis

We think that the model is solid, but the trust lies in the attack map:

- We assumed reasonable protocol properties, which may not be specific enough
- Attacks not modeled in the map will not be detected
- Disponibility attacks are tricky to model
- Not enough details on the radio and MAC side of things

However, the map is easily modifiable