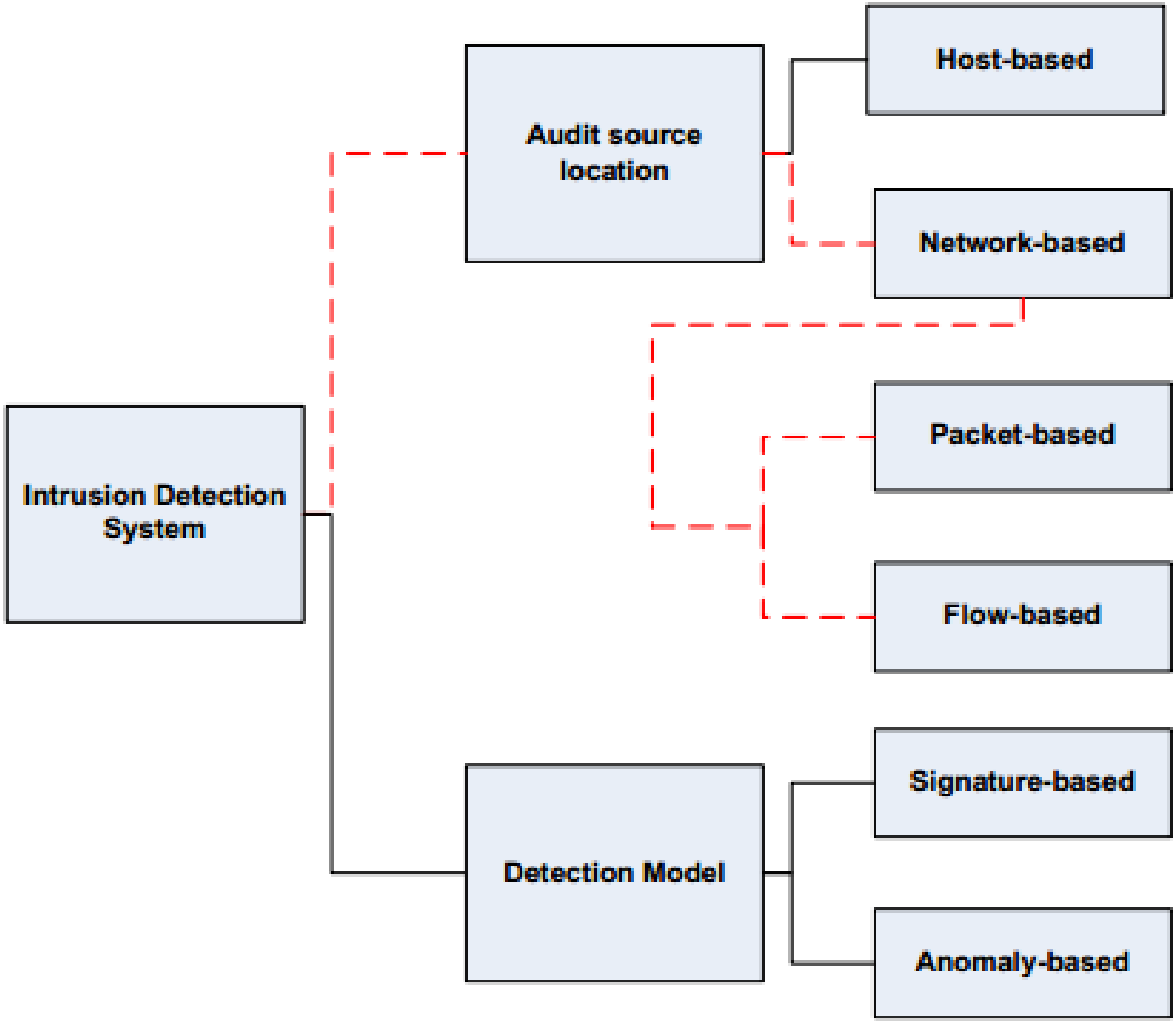
IDS Classification


Intrusion Detection System
Audit source location
Host-based
Network-based
Packet-based
Flow-based
Detection Model
Signature-based
Anomaly-based

- we can divide IDSs into two basic classes based on their position in the network or audit source location: host-based IDSs (HIDSs) and network-based (NIDSs).

Host-based IDSs (HIDs)

- Host-based systems were the first type of IDS being developed and implemented
- These systems are deployed locally on each host computer and monitor only the host on which it is installed.
- They are typically placed on business critical hosts and on servers in a DMZ that are likely to be compromised

HIDs

- The HIDS operates by monitoring changes to a number of variables on the host system.
- These controls may include: System processes, registry entries, CPU Usage, file access and integrity checking, audit policies, user accounts, events logs.
- Exceeding the threshold or suspicious integrity changes will send an alert to administrators.

- Some HIDS tools: Symantec Host IDS, ISS BlackICE PC, TCPWrappers, Enterasys Dragon Host Sensor
- Some analyst consider Integrity checkers as part of HIDS, as it’s difficult to escape from the notice of integrity checker tools (Tripwire is an example of integrity tool)

Network-Based IDS (NIDS)

- The majority of commercial intrusion detection systems are network based.
- These IDSs detect attacks by capturing and analyzing network packets.
- one network-based IDS can monitor the network traffic affecting multiple hosts that are connected to the network segment

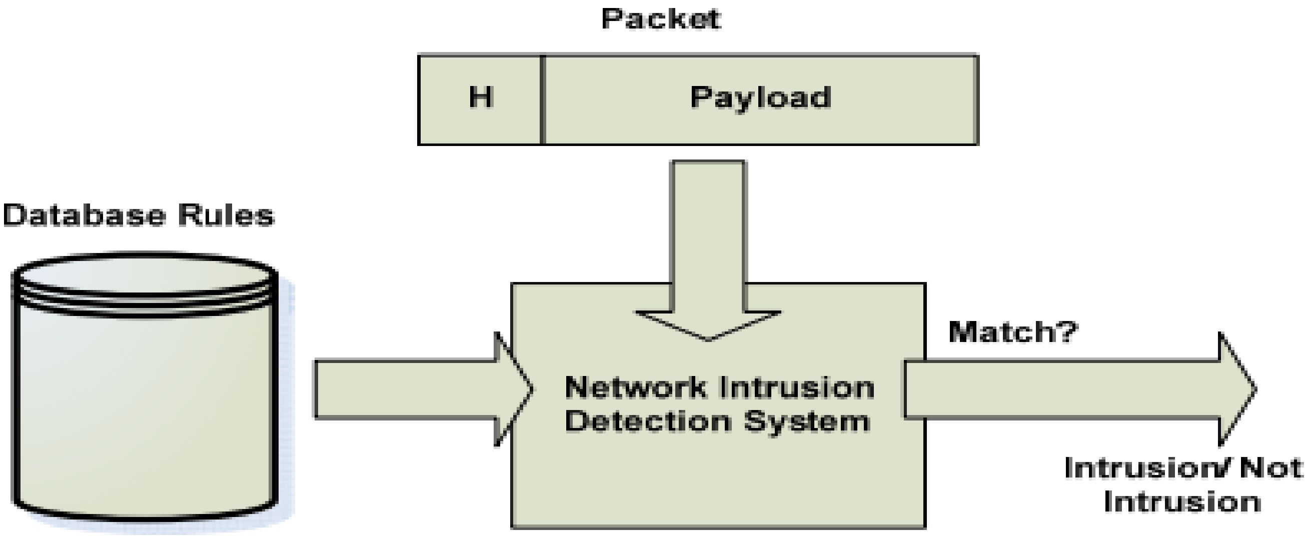
- An efficient NIDSs has two features :
  - high accuracy (low false alarms)
  - high performance (high speed of auditing)
- NIDSs should be able to handle the growth in Internet bandwidth as well as the increase in line speed and the growing number of attacks

- When packets are not analyzed on time, NIDSs start to drop packets
- These dropped packets may have aggressive data with attack signatures, which causes a high false negative (when no alert raise but intrusion attempt takes place) rates in NIDSs

packet-based NIDS

- Here, all network packets passing a certain observation point such as a router are captured without any loss of information.
- Also known as “Deep Packet Inspection” (DPI)
- A combination of header and payload scan determines whether a packet is an intrusion or not.
- Is realized by making use of software such as tcpdump

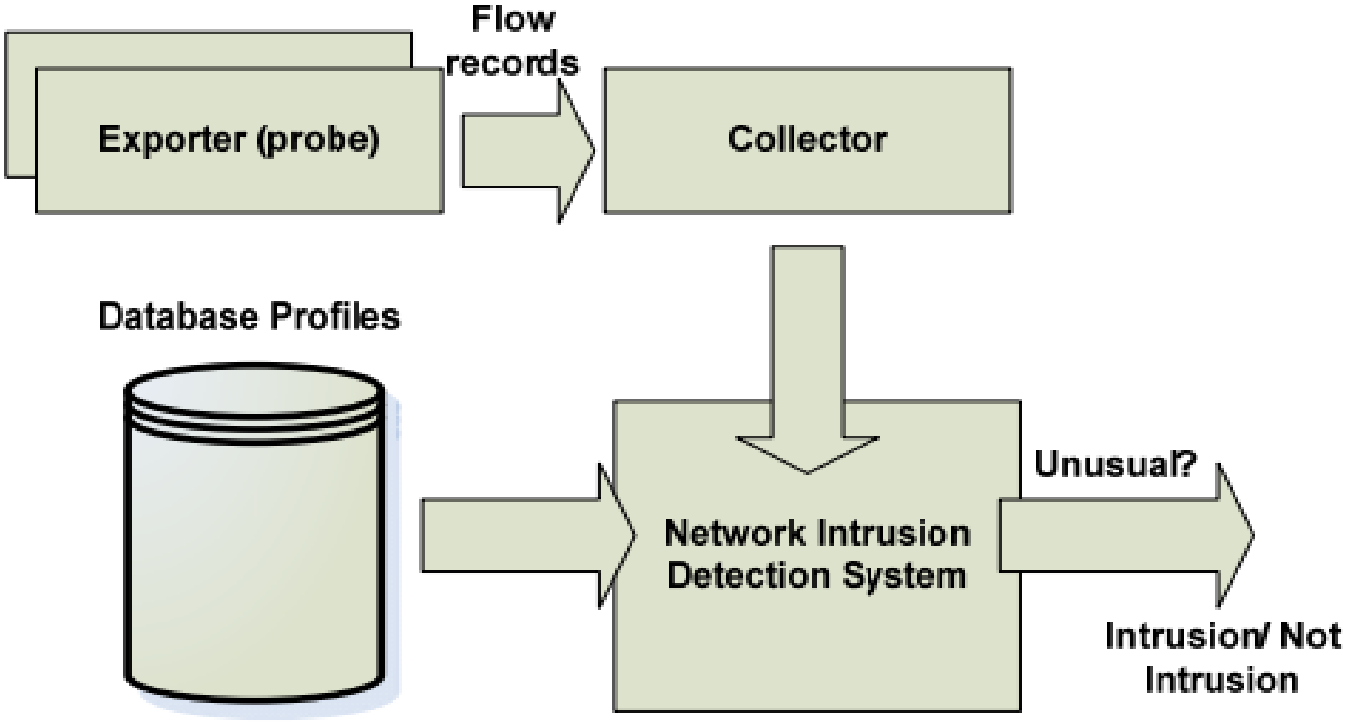
- Packets capturing and analysis can take place at different locations such as routers, switches, and network monitors form which the resulting measurement data is transported to a remote analysis



- Drop of packets will occur if the NIDSs speed is not high enough to let the analysis process be done
- Packet-based scheme are very time consuming, therefore should not utilized in high-speed links
- Signature matching is impossible for most cases of encrypted payload, degrading the detection performance of NIDSs.

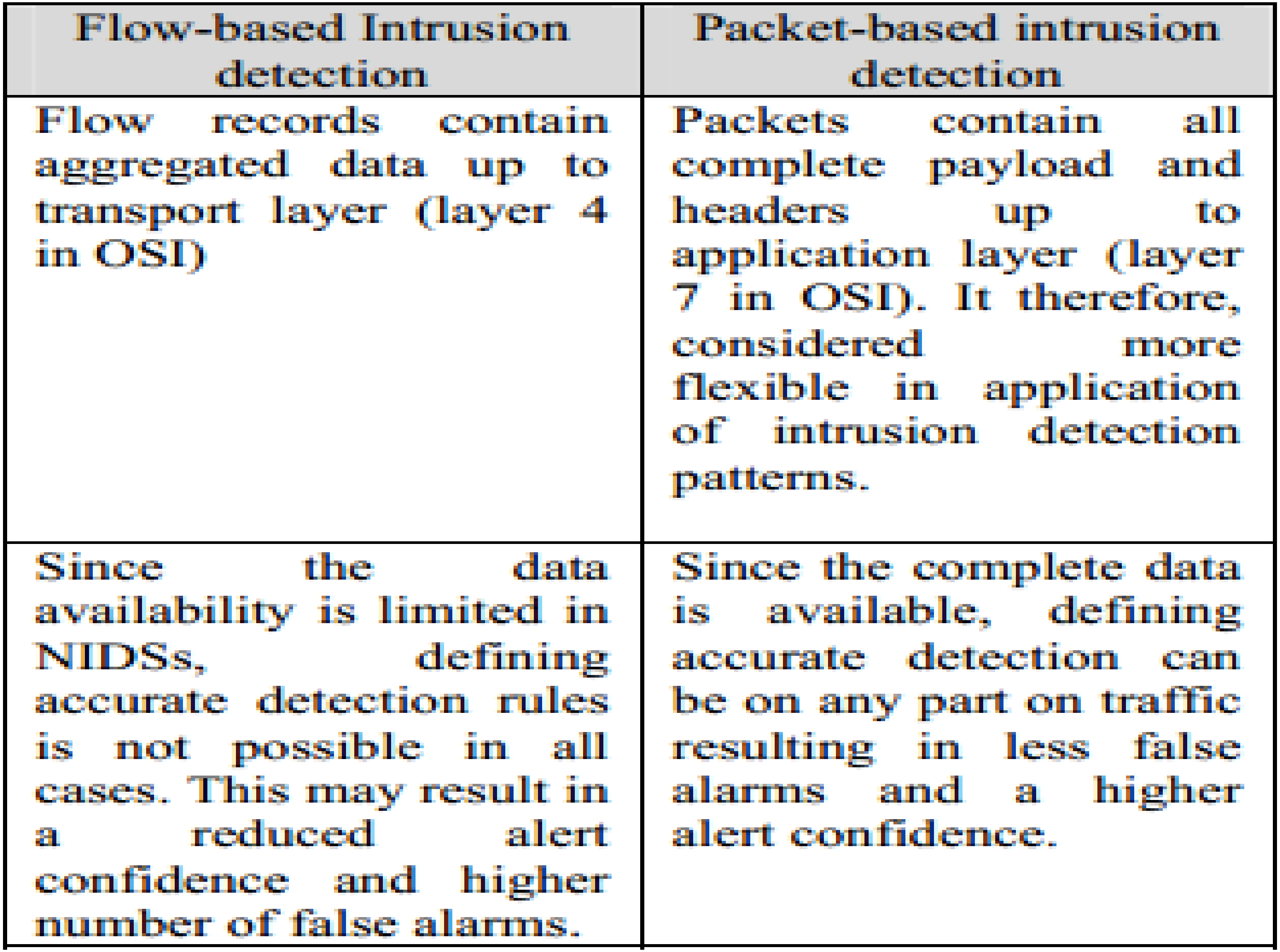
Flow based NIDS

- Network flows don’t provide any packet payload unlike packet-based approach.
- It rather relies on information and statistics of network flows, therefore flow-based NIDSs also called “network behavior


Flow records
Exporter (probe)
Collector
Database Profiles
Network Intrusion Detection System
Unusual?
Intrusion/ Not Intrusion

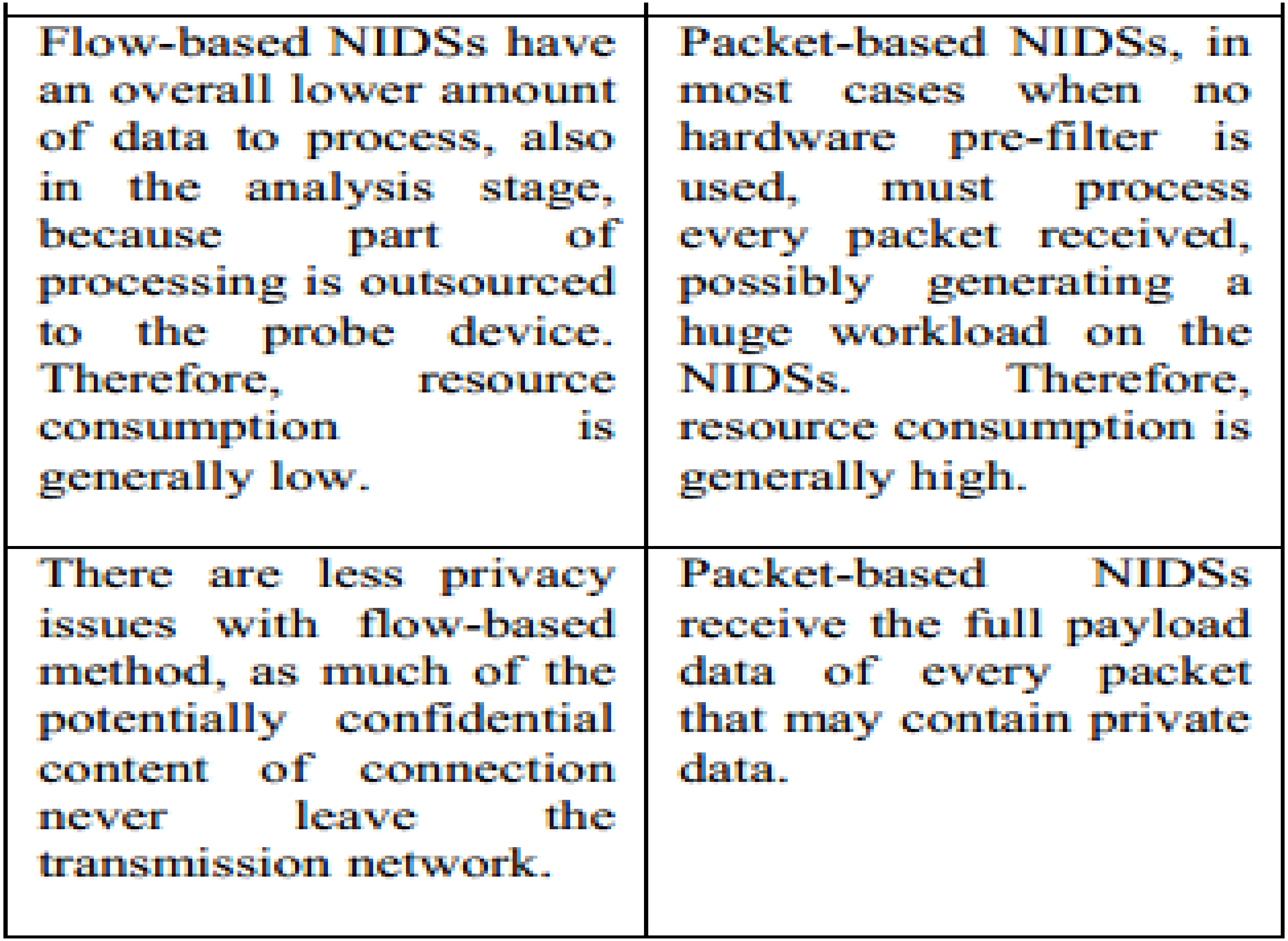
- A flow can be defined as a unidirectional data stream between two computer systems where all transmitted packets of this stream share the following characteristics:
    - IP source and destination address
    - source and destination port number
    - The number of packets and amount of bytes transferred in a flow
    - The start and end time of a flow (in millisecond)

- Any attack that only injected in payload will not be identified in flow-based method
-



Flow-based Intrusion detection	Packet-based intrusion detection
Flow records contain aggregated data up to transport layer (layer 4 in OSI)	Packets contain all complete payload and headers up to application layer (layer 7 in OSI). It therefore, considered more flexible in application of intrusion detection patterns.
Since the data availability is limited in NIDSs, defining accurate detection rules is not possible in all cases. This may result in a reduced alert confidence and higher number of false alarms.	Since the complete data is available, defining accurate detection can be on any part on traffic resulting in less false alarms and a higher alert confidence.

The generation of flow records introduces a delay between the moment the first packet of a connection is established and the time when the record reaches the NIDSs. Depending on the configuration, record may be released after the connection has been closed o timed out.	The complete data is available to NIDSs immediately without delay.
Encrypted payload does not influence the operability of flow-based NIDSs	Signature matching is impossible for most cases of encrypted payload, degrading the detection performance of NIDSs.



Flow-based NIDSs have an overall lower amount of data to process, also in the analysis stage, because part of processing is outsourced to the probe device. Therefore, resource consumption is generally low.	Packet-based NIDSs, in most cases when no hardware pre-filter is used, must process every packet received, possibly generating a huge workload on the NIDSs. Therefore, resource consumption is generally high.
There are less privacy issues with flow-based method, as much of the potentially confidential content of connection never leave the transmission network.	Packet-based NIDSs receive the full payload data of every packet that may contain private data.

IDS Classification

- IDSs also can be classified based on its detection model into two categories: signature-based and anomaly based.

Signature-based IDS

- The signature-based IDSs, also named “misused based”, employs a signature database of know attacks, and if a successful match with current input, an alert is raised. Example—Snort
- A signature defines the characteristics of an attack (protocol, service, source, pattern)

- It is based on the search for evidence of attacks based on the incremental knowledge from known attacks.
- This type of IDS can only detect attacks which it has the signature.
- Frequently updates are necessary to maintain up to date the knowledge database.

- Misuse-based detection is the most prevalent form of available IDS on the market

Anomaly based IDS

- Anomaly-based or behavior-based IDS works by building a model of normal traffic data pattern during a training phase, then it compares new inputs to the model.
- A significant deviation (change) is marked as an anomaly (abnormal or intrusion)

- It consists in searching for evidence of attacks based on knowledge accumulated.
- Abnormally high CPU load combined with other metrics can indicate an intrusion in progress.

- Anomaly based model has the advantage of detecting new types of attacks
- Frequent adjustments are necessary to upgrade the reference model in order to reflect the normal user’s behavior and reduce number of false positives.

- The majority of IDS based on Anomaly Detection are still under research projects (EMERALD)