**Table 1 – Fundamentals of the A-NIDS techniques**

| Technique: *basics* | ▪ Pros<br>▪ Cons | Subtypes |
|---|---|---|
| A) Statistical-based: *stochastic behaviour* | ▪ Prior knowledge about normal activity not required. Accurate notification of malicious activities. | A.1) Univariate models *(independent Gaussian random variables)* |
| | ▪ Susceptible to be trained by attackers. Difficult setting for parameters and metrics. Unrealistic quasi-stationary process assumption. | A.2) Multivariate models *(correlations among several metrics)*<br>A.3) Time series *(interval timers, counters and some other time-related metrics)* |
| B) Knowledge-based: *availability of prior knowledge/data* | ▪ Robustness. Flexibility and scalability.<br>▪ Difficult and time-consuming availability for high-quality knowledge/data. | B.1) Finite state machines *(states and transitions)*<br>B.2) Description languages *(N-grams, UML, ...)*<br>B.3) Expert systems *(rules-based classification)* |
| C) Machine learning-based: *categorization of patterns* | ▪ Flexibility and adaptability. Capture of interdependencies.<br>▪ High dependency on the assumption about the behaviour accepted for the system. High resource consuming. | C.1) Bayesian networks *(probabilistic relationships among variables)*<br>C.2) Markov models *(stochastic Markov theory)*<br>C.3) Neural networks *(human brain foundations)*<br>C.4) Fuzzy logic *(approximation and uncertainty)*<br>C.5) Genetic algorithms *(evolutionary biology inspired)*<br>C.6) Clustering and outlier detection *(data grouping)* |