A Probabilistic-driven Ensemble Approach
to Perform Event Classification in Intrusion Detection System

Roberto Saia, Salvatore Carta, Diego Reforgiato Recupero

Department of Mathematics and Computer Science, University of Cagliari, Italy

Artificial Intelligence and Big Data Laboratory (*http://aibd.unica.it/*)

{roberto.saia, salvatore, diego.reforgiato}@unica.it

Abstract

Nowadays, network services are indispensable for each category of users and they need constant efforts aimed to prevent fraudulent exploitation of the involved resources. In such a scenario the Intrusion Detection Systems cover a central role, because they have been designed to detect intrusion attempts, classifying each new network event as *normal* or *intrusion*. This work introduces a Probabilistic-Driven Ensemble (PDE) approach, where several state-of-the-art classification algorithms have been combined trough a probabilistic criterion in order to improve their ensemble effectiveness. Experiments made by using real-world data demonstrate that our approach outperforms the state-of-the-art solutions, showing a better ability to detect intrusion events.

Motivation and Intuition

The intrusion detection represents a hard task, due to the high dynamism and heterogeneity of the involved scenario, both in terms of network infrastructure and potential attacks. Considering that the behavior of many attacks is sometimes similar to that of a normal activity, it is very difficult to define efficient evaluation models.

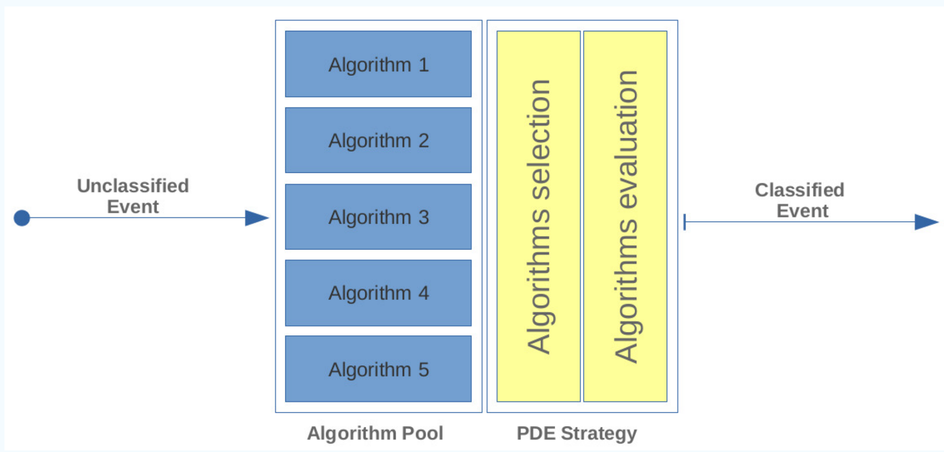
Open Issues

One of the major issues related to the state-of-the-art solutions is the difficulty to define, exhaustively, a signature for each possible intrusion event, generating a huge number of false alarms, and preventing the recognition of unknown intrusion patterns.

Intuition

Improving the intrusion detection effectiveness by adopting an ensemble approach based on several state-of-the-art classification algorithms, which are driven by a probabilistic model aimed to maximize the detection of the intrusion events.

Our approach



Model Definition

▶ We define the following model, where σ denotes the *probability* (confidence level) of a *prediction* made by an algorithm $a \in A$, during the classification of a new event $\hat{e} \in \hat{E}$, and $c(\hat{e})$ denotes our approach classification:

$$\overline{\sigma} = \frac{1}{|A|} \cdot \sum_{z=1}^{|A|} \sigma(a_z(p))$$

$$w_1 = \sum_{z=1}^{|A|} 1 \;\; if \;\; \sigma(a_z(p)) > \overline{\sigma} \;\; \wedge \;\; a_z(p) = normal$$

$$w_2 = \sum_{z=1}^{|A|} 1 \;\; if \;\; \sigma(a_z(p)) < \overline{\sigma} \;\; \vee \;\; a_z(p) = intrusion$$

$$c(\hat{e}) = \begin{cases} normal, & \text{if } w_1 > w_2 \\ intrusion, & \text{otherwise} \end{cases}$$

Evaluation

Setup and Strategy

▶ **Adopted dataset:** *NSL-KDD*.

▶ **Algorithms:** *Multilayer Perceptron*, *Decision Tree*, *Adaptive Boosting*, *Gradient Boosting*, and *Random Forests*.

▶ **Evaluation metrics:** *Specificity*, *F-score*, and *AUC*.

▶ **Experimental strategy:** We evaluate the ability to distinguish the *intrusion* events from the *normal* ones.

Classes of Events

▶ **Privilege Escalation Attack** (PEA)

▶ **Denial of Service Attack** (DSA)

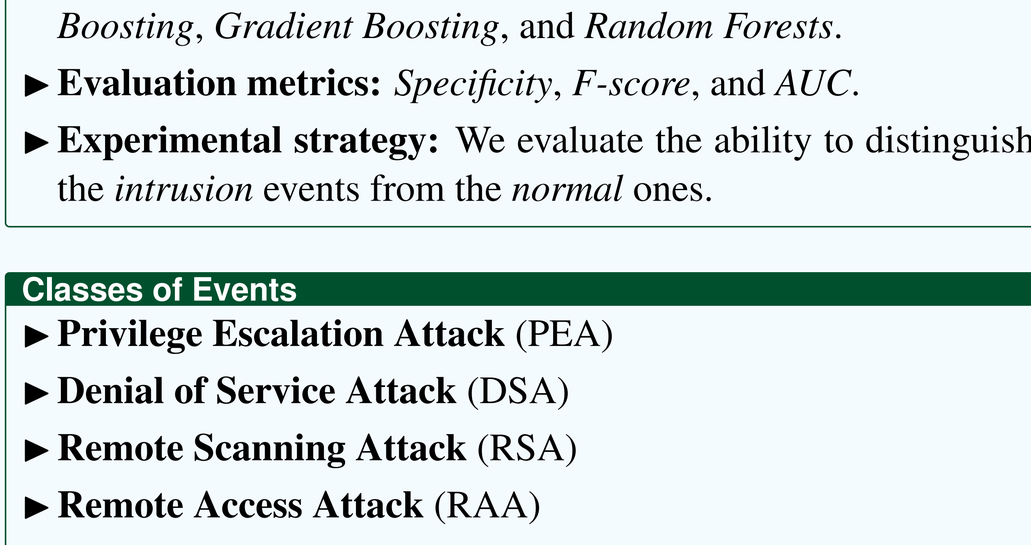
▶ **Remote Scanning Attack** (RSA)

▶ **Remote Access Attack** (RAA)

▶ **Normal Network Activity** (NNA)

Experimental Results

▶ We compared our PDE approach to all single and ensemble competitor approaches*:



(*) PEA data are reported with a different scale, which is the half of the other ones.

Conclusions

▶ The proposed *PDE* approach outperforms its competitors in terms of average performance (*TNR*, *F-score*, and *AUC*), except in the case of the *DSA* events, where it reaches the same performance of the best competitor.

▶ The increase in the number of correctly detected intrusion events (*Specificity*) does not lead to significant reduction of the classifier performance, since although we have a moderate worsening in terms of average *F-score* ($-\ 0.010$), we get an improvement in terms of average *AUC* ($+\ 0.025$).

▶ Considering that the used dataset contains a large number of events ($\sim 148K$), our approach allows a system to detect a significant number of attacks, otherwise not detected.

▶ The increase of the *True Negative Rate* (0.056) is not correlated with the increase of the *False Negative Rate* (0.007), then a very low percentage of the new detected intrusions are false alarms, also by considering that in such a scenario a false negative classification is preferable to a false positive one.

Acknowledgements

This research is partially funded by *Regione Sardegna*, *Next generation Open Mobile Apps Development* (NOMAD) project, *Pacchetti Integrati di Agevolazione* (PIA) - *Industria Artigianato e Servizi* (2013).