A Feature Space Transformation to Intrusion Detection Systems

Roberto Saia, Salvatore Carta, Diego Reforgiato Recupero, Gianni Fenu

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

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

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

Abstract

The anomaly-based Intrusion Detection Systems (IDSs) represent one of the most efficient methods against the network intrusion attempts. However, their effectiveness is jeopardized by some open problems, such as the difficulty of correctly classifying attacks with characteristics very similar to a normal network activity, or the difficulty of contrasting novel forms of attacks (zero-days). The proposed *Twofold Feature Space Transformation* (TFST) approach faces these problems by adding meta-information in order to improve the event characterization, and by performing the discretization of this extended feature space in order to join together patterns related to the same events. The validation process, performed on a real-world dataset, indicates that *TFST* outperforms the canonical state-of-the-art algorithms, improving their intrusion detection capability in the context of different data scenarios.

Research Scenario

On the basis of our previous works, where we have experimented the positive effects resulting from the transformation of the original data feature space, we propose a revised and improved approach named *Twofold Feature Space Transformation* (*TFST*).

Open Problems

The main source of problems, which makes the correct classification of network events a very difficult task, is the similarity between normal and intrusion events.

Intuition

Improving the event characterization by adding meta-information in order to better differentiate the normal network activities from the intrusion ones, then discretizing the obtained feature space in order to reduce the event patterns.

Approach

Extension $\Rightarrow$ The original feature space $F = \{f_1, f_2, \ldots, f_N\}$ is extended by adding four meta-information $\Xi = \{m_1, m_2, \ldots, m_4\}$: *Minimum* ($m_1$), *Maximum* ($m_2$), *Average* ($m_3$), and *Standard Deviation* (m_4).

$$\Xi = \begin{cases} m_1 = min(f_1, f_2, \ldots, f_N) \\ m_2 = max(f_1, f_2, \ldots, f_N) \\ m_3 = \frac{1}{N}\sum_{n=1}^{N}(f_n) \\ m_4 = \sqrt{\frac{1}{N-1}\sum_{n=1}^{N}(f_n - \bar{f})^2} \end{cases}$$

Discretization $\Rightarrow$ According to an optimal discretization range experimentally defined, the extended feature space is then discretized into a range of values $\{0, 1, \ldots, \delta\} \in \mathbb{Z}$: denoting as $f \xrightarrow{\delta} d$ the discretization function, we transform each feature $f \in F$ from its original value to one of the discrete values in the range $\{d_1, d_2, \ldots, d_\delta\}$.

$$\begin{gathered} \{f_1, f_2, \ldots, f_N, f_{N+1}, f_{N+2}, f_{N+3}, f_{N+4}\} \\ \downarrow \delta \\ \{d_1, d_2, \ldots, d_N, d_{N+1}, d_{N+2}, d_{N+3}, d_{N+4}\} \end{gathered}$$

Classification $\Rightarrow$ The new feature space obtained through the previous two steps is finally exploited in the context of a classifier of the new network events, which is based on one of the canonical state-of-the-art algorithm used in this context.

Validation

Dataset • Competitors • Metrics • Strategy

- **Dataset:** *NSL-KDD*.
- **Competitors:** *Gradient Boosting (GB)*, *Adaptive Boosting (AB)*, *Random Forests (RF)*, *Multilayer Perceptron (MP)*, and *Decision Tree (DT)*.
- **Metrics:** *Specificity*, *Matthews Correlation Coefficient (MCC)*, and *Area Under the ROC Curve (AUC)*.
- **Strategy:** We evaluate the performance of the competitor classification algorithms, with and without (*baseline*) the *TFST*.

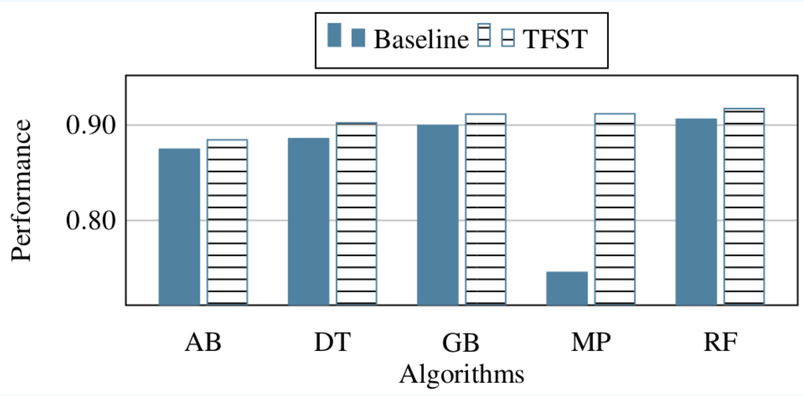
Classes of Events

- The involved classes of events in the datasets are: *Privilege Escalation Attack (PEA)*, *Denial of Service Attack (DSA)*, *Remote Scanning Attack (RSA)*, *Remote Access Attack (RAA)*, and *Normal Network Activity (NNA)*, divided as follows:

Dataset	PEA	DSA	RSA	RAA	NNA
Training	52	45,927	11,656	994	67,343
Test	67	7,460	2,421	2,885	9,710
Total	119	53,387	14,077	3,879	77,053
%	0.08	35.95	9.48	2.61	51.88

Experimental Results

- The *Performance* in the context of all events is expressed in terms of average value between *Specificity*, *MCC*, and *AUC*.



Conclusions

- in terms of average performance between the *Specificity*, *MCC* and *AUC* metrics, the proposed *TFST* approach outperforms its competitors in *19* cases out of *25*;
- also by analyzing the mean value in terms of each single metric, the *TFST* approach outperforms its competitors;
- it outperforms its competitors in datasets characterized by different number of events, type of events, and level of class balance, proving to be capable to operate in different real-world scenarios;
- summarizing, experimental results show that the performance of the canonical state-of-the-art algorithms can be improved through the *TFST* approach, regardless both the used algorithm and the data scenario, also by considering that such an improvement can be exploited in the context of multi-algorithms solutions, e.g., the ensemble-based ones.

Acknowledgements

This research is partially funded by Italian Ministry of Education, University and Research - Program Smart Cities and Communities and Social Innovation project ILEARNTV (D.D. n.1937 del 05.06.2014, CUP F74G14000200008 F19G14000910008).