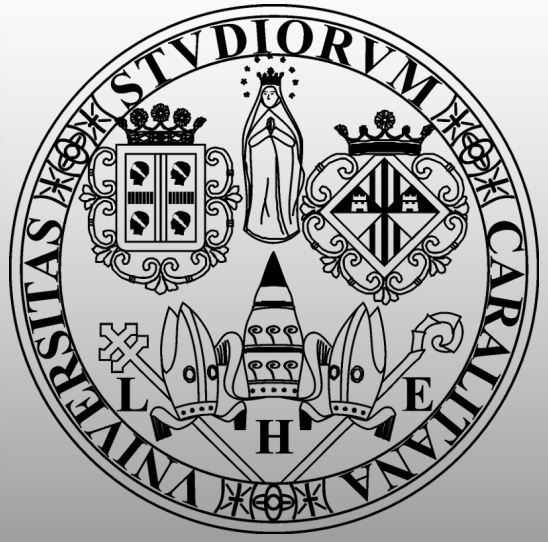


Decomposing Training Data to Improve Network Intrusion Detection Performance

Roberto Saia, Alessandro Sebastian Podda, Gianni Fenu, and Riccardo Balia

Department of Mathematics and Computer Science
University of Cagliari, Italy

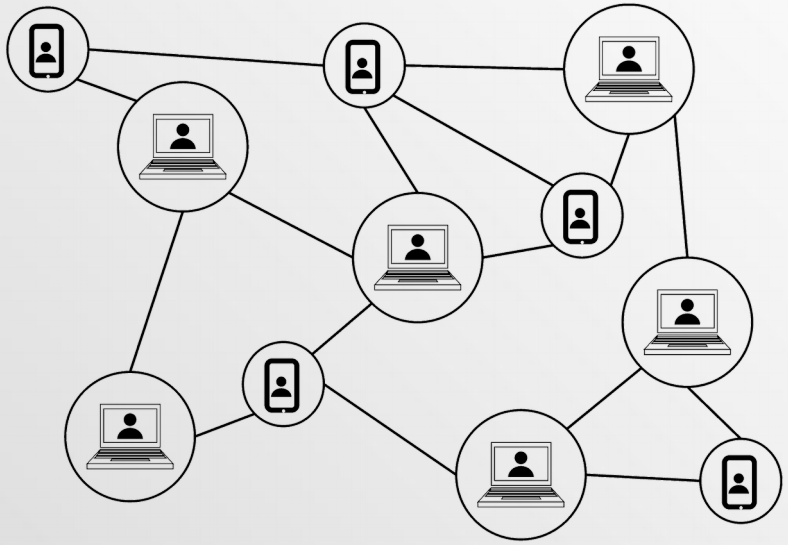
KDIR 2021, 13th International Conference on Knowledge Discovery and Information Retrieval
25÷27 October 2021 – Online Streaming

Outline

- Scenario
- Idea
- Formalization
- Conclusion

Scenario

The enormous exponential growth of **network-based services** has made the problem of their security a crucial aspect of the everyday life, public and private, since the high degree of **heterogeneity** that characterizes network events makes the detection of attacks an **hard task**



Scenario

The **Intrusion Detection Systems** (IDSs) have been designed to face such a problem, as their goal is to classify all the network events as **normal** or **intrusion**

But regardless of the adopted classification technique, their effectiveness is reduced by:

- A high level of **heterogeneity** and **dynamism** of the network events
- The fact that an attack **behavior** can be very similar to that of a **legitimate** network activity

Idea

- The idea behind the **proposed strategy** relies on the observation that the data used to train an evaluation model refers to **different periods**, as well as the features that characterize each event refer to **different aspects** of the involved scenario.
- We proposed to **divide** the training dataset into **several regions**, in order to characterize different scenarios in terms of **time** (*events*) and **characteristics** (*features*)
- The **event classification** will be performed on the basis of **all the models** we trained using these data regions

Formalization

- We **combine** different **evaluation models**, each of them trained on a different region of the training set **T**
- the regions are **bounded** in terms of *events* ***e*** and *features* ***f***, as in the following example, where a **2x2 region** has been highlighted

$$\mathbf{T} = \begin{array}{c} \longleftarrow \textit{behavior} \longrightarrow \\ \begin{array}{|cccc|c} e_1(f_1) & e_1(f_2) & e_1(f_{...}) & e_1(f_W) & \uparrow \\ e_2(f_1) & e_2(f_2) & e_2(f_{...}) & e_2(f_W) & \textit{time} \\ \vdots & \vdots & \ddots & \vdots & \downarrow \\ e_N(f_1) & e_N(f_2) & e_N(f_{...}) & e_N(f_W) & \end{array} \end{array}$$

Formalization

- An **intrusion detection algorithm** is applied to a **different part** of the training set
- The event classification depends on all single region **r** classification, as shown in the following equation, which refers to a training set with **4 events** and **4 features**, divided into **2x2 regions** that involve four $\mathbf{m_1}$, $\mathbf{m_2}$, $\mathbf{m_3}$, and $\mathbf{m_4}$ evaluation models

$$\left[\begin{array}{c|c} r_1 & r_2 \\ \hline r_3 & r_4 \end{array}\right] = \left[\begin{array}{cc|cc} f_{1,1} & f_{2,1} & f_{3,1} & f_{4,1} \\ f_{1,2} & f_{2,2} & f_{3,2} & f_{4,2} \\ \hline f_{1,3} & f_{2,3} & f_{3,3} & f_{4,3} \\ f_{1,4} & f_{2,4} & f_{3,4} & f_{4,4} \end{array}\right] \Rightarrow \left[\begin{array}{c|c} m_1 & m_2 \\ \hline m_3 & m_4 \end{array}\right]$$

Conclusions

- The proposed strategy is aimed to **improve** the performance of the IDSs
- It operates by **dividing** the training dataset into **several regions**, in order to better characterize the network events
- Each region is used to trains an **independent evaluation model**, and the event classification takes into account all the models, according to a majority voting criterion

Decomposing Training Data to Improve Network Intrusion Detection Performance

THANK YOU FOR YOUR ATTENTION

KDIR 2021, 13th International Conference on Knowledge Discovery and Information Retrieval
25÷27 October 2021 – Online Streaming