Detekce anomálií v počítačové síti

Jan Kohout

Motivace

- Využití v bezpečnosti: Ne vše v síti je legitimní provoz
- Předpokládáme, že alespoň (výrazná) většina provozu je legitimní
- Nežádoucí provoz se nečím od legitimního liší $\rightarrow$ projeví se jako anomálie
- Použití technik strojového učení

Proč takhle?

"Klasické" metody často spoléhají na databázi známých útoku

- Problém s odhalením neznámých útoků, časté aktualizace

Lze použít i bez inspekce obashu

- Nevadí šifrování obsahu, lze použít i ve velké síti

Problém bývá s přesností detekce - obvykle vyšší míra falešných alarmů

Detekce anomálií

- Obecně: identifikovat data, která se liší od většiny ostatních
- Postup:
  - Zvolit reprezentaci dat (jako n-dimenzionální vektory, časovou řadu,...)
    - Záleží na konkrétní aplikaci
  - Každému vzorku přiřadit hodnotu anomálie
  - Reportovat data s hodnotou anomálie větší než zvolený *práh*

Jak určit hodnotu anomálie? Jak zvolit *práh*?

Algoritmy

Pár příkladů:

- Metody založené na vzdálenosti od nejbližších sousedů
  - *Local Outlier Factor (LOF)*
- *One-class SVM*
- Využití odhadu pravděpodobnostní distribuce známých dat
  - Určení anomálie pomocí věrohodnosti vzorku (*log-likelihood*)
- Metody využívající PCA (*Principal Component Analysis*)
- Detekce významné odchylky od predikce časové řady

Náhodné projekce

Používá odhad pravděpodobnosti, n-rozměrnou distribuci nahrazuje k jednorozměrnými distribucemi

- Zvolíme k náhodných vektorů $w_1, ..., w_k \in R^n$
- Pro $x \in R^n$ určíme hodnotu anomálie:

$$Anom(x) = -\frac{1}{k} \sum_{i=1}^{k} \log(p_i(w_i^T \cdot x))$$

p_i je odhad pravděpodobnosti výskytu hodnoty $w_i^T \cdot x$, pomocí histogramu dosud pozorovaných hodnot (lze aktualizovat on-line)

[T. Pevný: Anomaly Detection by Bagging]

Principal Component Analysis

Transformace souřadnic, nové souřadnice určeny vlastními vektory kovarianční matice dat Σ
Matice dat $X \in R^{m \times n}$ (se stř. hodnotou 0):

$$\Sigma = \frac{1}{m-1} X^T X$$

- Významnost komponenty určena rozptylem dat v jejím směru, komponenty jsou seřazeny podle významnosti
- Předpoklad: Pro reprezentaci normálních dat stačí prvních $k < n$ komponent (*normal data sub-space*)

Principal Component Analysis

- Komp. $1, ..., k$ - podprostor normálních dat
- Komp. $k+1, ..., n$ - podprostor anomálních dat

Projekci vzorku $x \in R^n$ lze rozložit na projekci na prostor normálních dat (x') a na prostor anomálních dat (x'')
Hodnotu anomálie můžeme určit např.:

$$Anom(x) = ||x''||^2$$

[Lakhina et al.: Diagnosing Network-Wide Traffic Anomalies]

Principal Component Analysis - příklad

Stav sítě sledujeme v časových krocích, pro každou IP adresu $i \in \mathrm{I}$ v čase t držíme $H^{\tau}_{dPr}(i), H^{\tau}_{sPr}(i), H^{\tau}_{dIP}(i), \tau \in \{t-5, ..., t-1\}$ - entropie zdrojových portů, cílových portů a cílových IP adres $\rightarrow$ 15-dim. vektor pro každou adresu $i \in \mathrm{I}$
Matice dat $X \in R^{|\mathrm{I}| \times 15}$ v čase t:

$$X = (H^{t-5}_{dPr}(i), H^{t-5}_{sPr}(i), H^{t-5}_{dIP}(i), ..., H^{t-1}_{dPr}(i), H^{t-1}_{sPr}(i), H^{t-1}_{dIP}(i)), i \in \mathrm{I}$$

Dokáže např. odhalit vertikální/horizontální skenování sítě

[Grill, Pevný: Detecting anomalous network hosts by means of PCA]

Jak stanovit práh?

Různě:

- Někdy je možné určit analyticky podle požadavků na přesnost/spolehlivost detekce
- Přimíchat do dat simulované útoky a práh odhadnout podle jejich hodnot anomá lie
- Vždy reportovat x% dat s nejvyšší hodnotou anomálie