DDoS Event Forecasting using Twitter Data

Zhongqing Wang[1,2] and Yue Zhang[2]
[1.] *Soochow University, Suzhou, China*
[2.] *Singapore University of Technology and Design, Singapore*
wangzq.antony@gmail.com, yue_zhang@sutd.edu.sg

DDoS Attacks

- A Distributed Denial of Service (DDoS) attack employs multiple compromised systems to interrupt or suspend services of a host connected to the Internet.
  - *Almost half (45%) of the respondents indicated their attacks*
  - *The average DDoS cost can be assessed at about $500,000*
- DDoS assaults come in many shapes and sizes, so organizations must be prepared for anything in order to protect themselves.

DDoS Detection vs. Forecast

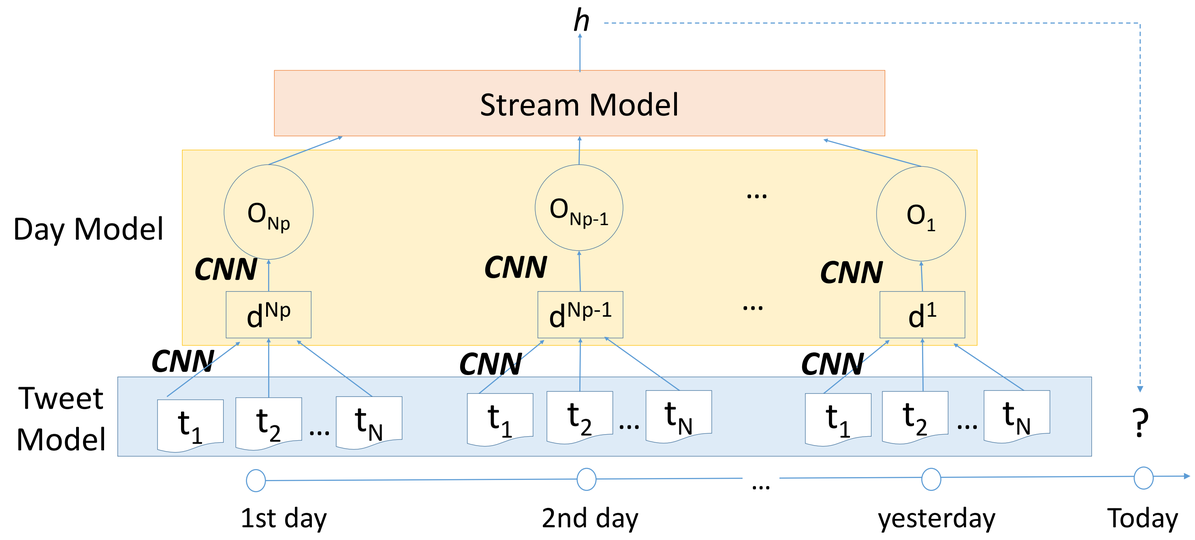
- Traditionally, the aim of a DDoS detection system is to detect malicious packet traffic from legitimate traffic.
  - However, malicious traffic occurs only *after a DDoS attack* has begun, there is limited time to prevent damage.
- This paper investigates the feasibility of **forecasting the likelihood of DDoS attacks before they happen** by monitoring social media stream.

Assumptions of Forecasting

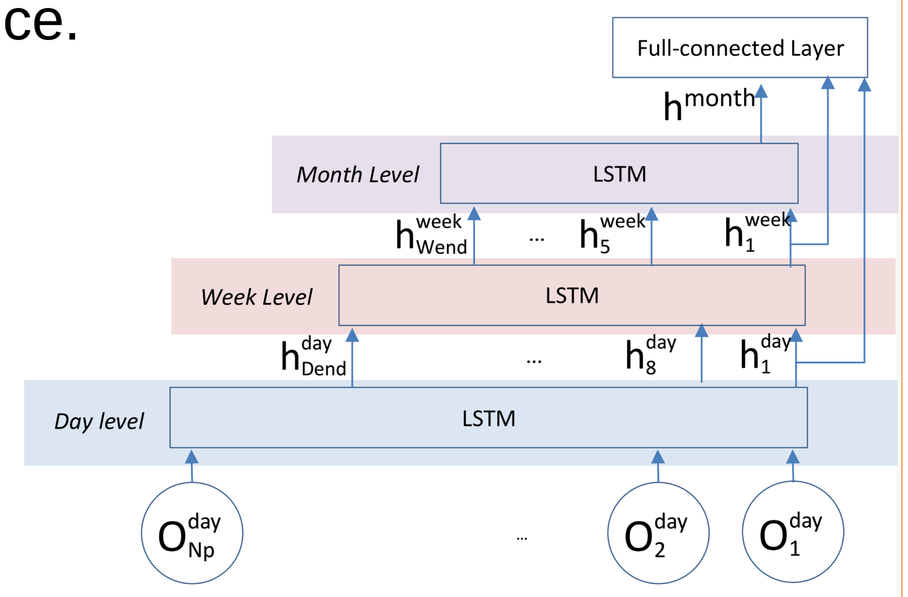
- Our motivation is that the attacked targets may be mentioned unfavorably or arouse negative sentiments in social media text.

Post	Target
The Thai government is about to end their citizens internet freedom.	Thai government
Soooooooo basically they are all leaving soon, sony is mad as hell.	SONY

Neural Stream Model



- Hierarchical Stream Model
  - We propose a fine-grained *stacked* LSTM model, arranging daily, weekly, and monthly history into a *hierarchical* structure, to capture *infinitely* long history without losing short and long term difference.



Experimental Results

- Compare the proposed Model (LSTM-HS) with various baselines.

Method	AUC
Neg-Term-count	0.233
SVM	0.164
SVM-emb	0.212
SVM-emb-senti	0.254
LSTM-emb	0.259
LSTM-senti	0.232
LSTM-emb-senti	0.293
LSTM-HS	**0.346**