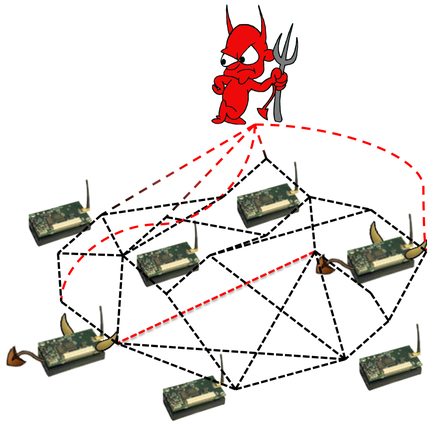
Detecting Malicious Activity in Wireless Sensor Networks using Topic Modeling with Latent Dirichlet Allocation

Model Creation Process

1. Choose N ~ Poisson(ξ)
2. Choose θ ~ Dirichlet(α)
3. For each *N* words, W_n
   A. Choose a topic Z_n~ Multinomial(θ)
   B. Choose a word W_n from $p(w_n|z_n,\beta)$



Model Data

- *Word*: Fundamental Unit

$$w_x = \begin{cases} 1, & w_x = v \\ 0, & w_x = u \end{cases}, v \neq u$$

- *Document*: Set of Words

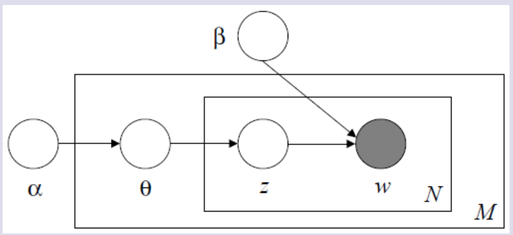
$$\boldsymbol{w} = (w_1, w_2, \ldots, w_n)$$

- *Database*: Set of Documents

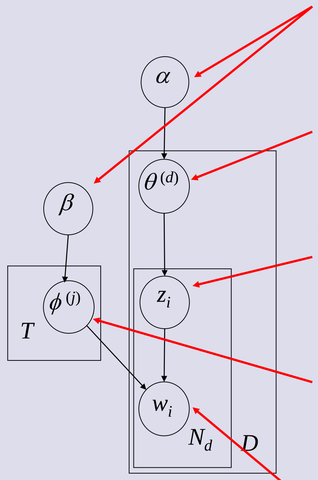
$$D = \{d_1, d_2, \ldots, d_m\}$$

Model Components

Dirichlet Prior (Topic Parameters): α, β
Selected based on database
Dirichlet Variable: θ
Fixed dimension
Topic: z
Filled node: w
Observed variable
Connections arrow
Indicates dependence based on direction



Application



Dirichlet priors

Distribution over topics for each packet

$\theta^{(d)} \sim \text{Dirichlet}(\alpha)$

Topic assignment for each node stream

$z_i \sim \text{Discrete}(\theta^{(d)})$

Distribution over node streams for each topic

$\phi^{(j)} \sim \text{Dirichlet}(\beta)$

Network traffic generated from assigned topic

$w_i \sim \text{Discrete}(\phi^{(z_i)})$

Detection of Malicious activity in WSN
Use LDA to create baseline for each node
Compare real-time behavior to baseline
Characterize abnormal variances
LDA Variables for Malicious activity Detection
Words → *Packets*
Documents → *Node Stream*
Database → *Network Traffic*

Ranking Topics

$$\underset{\text{words}}{\overset{\text{documents}}{P(w)}} = \underset{\text{words}}{\overset{\text{topics}}{P(w|z)}} \times \underset{\text{topics}}{\overset{\text{documents}}{P(z)}}$$

Topic Similarity:

$$document - similarity_{d,f} = \sum_{k=1}^{K} \left(\sqrt{\widehat{\theta_{k,v}}} - \sqrt{\widehat{\theta_{f,v}}} \right)^2$$

Term Score:

$$term - score_{k,v} = \widehat{\beta_{k,v}} \log \left(\frac{\widehat{\beta_{k,v}}}{\left(\prod_{j=1}^{K} \widehat{\beta_{j,v}}\right)^{\frac{1}{K}}} \right)$$

Metrics

Packet	Database
packetLength	NetFlow
srcAddress	MeanPacketLength
dstAddress	MeanDatagramLength
datagramLength	VarPacketLength
signalStrength	VarDatagramLengthy

Data Structure

Layer 2: Link	Layer 3 : Network	Layer 4 : Transport	Layers 5-7 : "Data"
MAC	IP	TCP UDP	HTTP FTP DHCP DNS …