THINK.
CHANGE.
DO

UNIVERSITY OF TECHNOLOGY SYDNEY

IEEE Transactions on Computers, by Tan, He et al., November 2014

Xiangjian (Sean) He
Global Big Data Technologies Centre (GBDTC)

DETECTION OF DENIAL-OF-SERVICE ATTACKS BASED ON COMPUTER VISION TECHNIQUES

Xiangjian.He@uts.edu.au

INTRODUCTION – BACKGROUND AND MOTIVATION

- Computer networks
  - A key component of the infrastructure of today's human society.
  - Targeted by cyber criminals.
  - Seriously threatened by Denial-of-Service (DoS) attacks.
- DoS attack mechanisms
  - Exploitation of system vulnerability
  - Network flooding to connected systems
- Schemes of defence
  - Defence mechanisms
    - Detection, prevention, mitigation and response.
  - Detection
    - It is playing an increasingly important role.

RELATED WORKS – DOS ATTACK DETECTION

- In terms of detection method
  - Misuse-based detection
  - Anomaly-based detection, such as detection techniques based on *machine learning* and *statistical analysis*
- In terms of audit source location
  - Host-based
  - Network-based
- Major issue of the network anomaly-based detection approaches
  - **High false positive rates** – this is partly because they either neglect the dependency and correlation between features/attributes or do not manage to fully exploit the correlation.
- **Recent studies** take full advantage of the correlation in design.

TRADITIONAL CORRELATION APPROACHES

- Most of the proposed systems are based on traditional statistical correlation analysis techniques
  - Only capable of studying the correlations between the features (variables) in a given sample set.
  - Incapable of recognising individual attack records hidden in a sample set.

CORRELATION APPROACHES

- Jin et al. 2007 proposed a statistical detection approach using covariance matrix to represent the multivariate correlation for sequential samples
  - Vulnerable to attacks that linearly change all monitored features.
  - It can only label a group of observed samples.
- Tsai and Lin 2010 applied a triangle-area-based method to discover the correlation between observed objects and the cluster centroids.
  - The dependency on prior knowledge of anomalous behaviours diluted its accuracy and reliability on correlation discovery.

DoS DETECTION AND COMPUTER VISION

- There are some commonalities shared between DoS attack detection and computer vision tasks, such as image retrieval and object shape recognition.
- Normal traffic to DoS attack detection can be equivalent to queries to image retrieval or object shape recognition.
- DoS attacks to our detection task can be interpreted as the images or the object shapes that do not match the queries.
- Therefore, computer vision techniques can provide intuitive and effective solutions to the intrusion detection problem.

FEATURES OF THE PROPOSED SYSTEM

- The hidden correlations between the features of network traffic are extracted using our previously developed Multivariate Correlation Analysis (MCA) technique.
- Individual attack records hidden in the crowd can be easily recognised by our system.
  - This is owing to one of the merits of our MCA technique which equips the analysis of correlation being conducted on individual network traffic records.
- Our proposed system adopts the principle of object shape recognition in the design of attack detectors.
  - To the best of our knowledge, it is the first time that Earth Mover's Distance (EMD) (a robust distance metric) has ever been applied to the field of network DoS attack detection.

OUR PREVIOUS APPROACHES

- A multi-tier Real-time Payload based IDS (RePIDS) (CN 2013) was proposed
  - Mahalanobis Distance Map (MDM) was used to reveal the correlation between packet payload features.
  - We attempted to remove the dependency on network traffic packet payload by diverting to connection-based features, and eliminated the restriction of the use of IDS to encrypted network traffic.
- A Multivariate Correlation Analysis (MCA) (TPDS 2014) approach embraces triangle area in estimating the correlation between features.
  - It is based on Mahalanobis distance, which does not support partial matching.
- A more sophisticated distance metric, such as the EMD, can enhance the accuracy of detection.

DIFFERENCE FROM OUR WORK IN TPDS2014*

- To improve the accuracy and to accelerate the computation
  - Principal Component Analysis (PCA) is applied to reduce the dimensionality (noise) of data.
- Before detection is conducted
  - Inbound network traffic records are converted into two-dimensional images
- To measure the similarity between observed inbound traffic records and a pre-built normal profile
  - EMD instead of Mahalanobis distance is utilised in this work.

*Tan, Jamdagni, He, et al.: A System for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis. IEEE Trans. Parallel Distrib. Syst. 2014

EARTH MOVER'S DISTANCE (EMD)

- EMD supports partial matching and outperforms bin-by-bin distances in matching perceptual dissimilarity.
- It benefits from the extension of the concept of a distance from between corresponding elements to between the entire distributions.
- Grauman and Darrell 2004 proposed a fast contour matching algorithm using an approximate EMD, which utilised embedding technique to accelerate the computational speed.
- Ling and Okada 2007 suggested an alternative fast version for EMD in which L1 distance was used as ground distance to compute the dissimilarity between histograms.

EMD – MATHEMATICAL REPRESENTATION

This can be formalized as the following linear programming problem: Let $P = \{(p_1, w_{p_1}), \ldots, (p_m, w_{p_m})\}$ be the first signature with m clusters, where p_i is the cluster representative and w_{p_i} is the weight of the cluster; $Q = \{(q_1, w_{q_1}), \ldots, (q_n, w_{q_n})\}$ the second signature with n clusters; and $\mathbf{D} = [d_{ij}]$ the ground distance matrix where d_{ij} is the ground distance between clusters p_i and q_j.

We want to find a flow $\mathbf{F} = [f_{ij}]$, with f_{ij} the flow between p_i and q_j, that minimizes the overall cost

$$\mathrm{WORK}(P, Q, \mathbf{F}) = \sum_{i=1}^{m} \sum_{j=1}^{n} f_{ij} d_{ij} \ ,$$

subject to the following constraints:

$$\begin{aligned}
f_{ij} &\geq 0 \qquad 1 \leq i \leq m,\ 1 \leq j \leq n \\
\sum_{j=1}^{n} f_{ij} &\leq w_{p_i} \qquad 1 \leq i \leq m \\
\sum_{i=1}^{m} f_{ij} &\leq w_{q_j} \qquad 1 \leq j \leq n \\
\sum_{i=1}^{m} \sum_{j=1}^{n} f_{ij} &= \min\left(\sum_{i=1}^{m} w_{p_i}, \sum_{j=1}^{n} w_{q_j}\right) \ ,
\end{aligned}$$

APPLICATIONS OF EMD

- EMD has been widely used to solve many problems in computer vision, such as
  - image retrieval,
  - Contour matching,
  - object shape recognition,
  - interest point matching and
  - visual tracking etc.
- It is still a new technique to computer and network security, and only a small amount of work based on EMD has been found.

SECURITY APPROACHES USING EMD

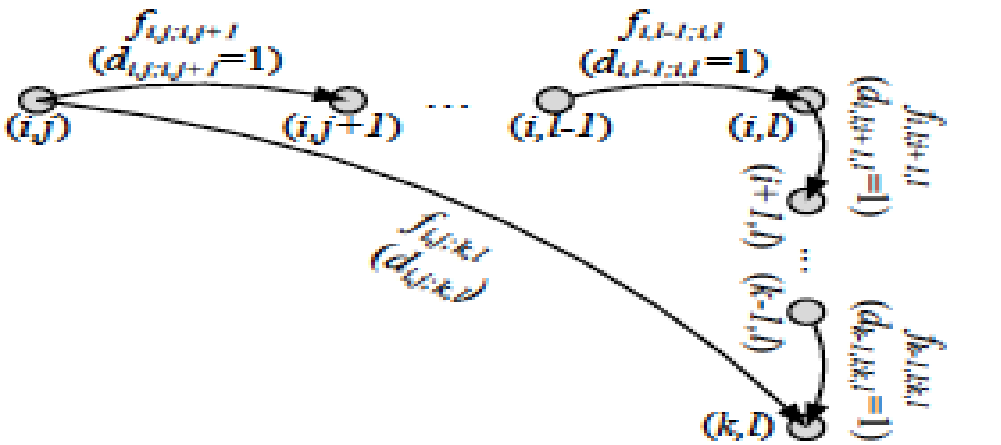
- Fu et al. 2006 converted web pages into normalised images
  - Visual similarities between a test web page and protected web pages were assessed using the EMD.
- Yen and Reiter 2010 developed a test method to differentiate patterns between Plotters (i.e., bots) and Traders (i.e., normal peers) on a P2P network.
  - EMD helped evaluate the similarity between the per-destination interstitial time distributions of hosts.
- Micarelli and Sansonetti 2007 proposed a case-based anomaly intrusion detection approach.
  - This approach monitored the output parameters and the arguments of system calls database using EMD.

LIMITATIONS OF EXISTING APPROACHES USING EMD

- None of the approaches has been designed particularly for DoS attack detection.
- The existing studies employ the original EMD.
- The heavy computational complexity of the original EMD prevents them from being applied in prompt detection tasks.
- The theoretical advantages of EMD and the shortcomings in recent applications of EMD motivate us to explore a better means to integrate EMD-L1 (a fast version of EMD) and DoS attack detection task.

EMB – L1

- L1 (i.e., Manhattan) distance redefines the computation of EMD as a "network flow problem".
- Any shortest path between two points on a network can be decomposed into a collection of edges between neighbour nodes with a ground distance of one between them.



Remark: $d_{i,j;k,l} = d_{i,j;i,j+1} + \ldots + d_{i,L-1;i,l} + d_{i,L;i+1,l} + \ldots + d_{k-1,L;k,l}$

REPRESENTATION OF 2D EMD – L1

J_1 = {(j; p; c; d): |j - c| + |p - d| = 1}

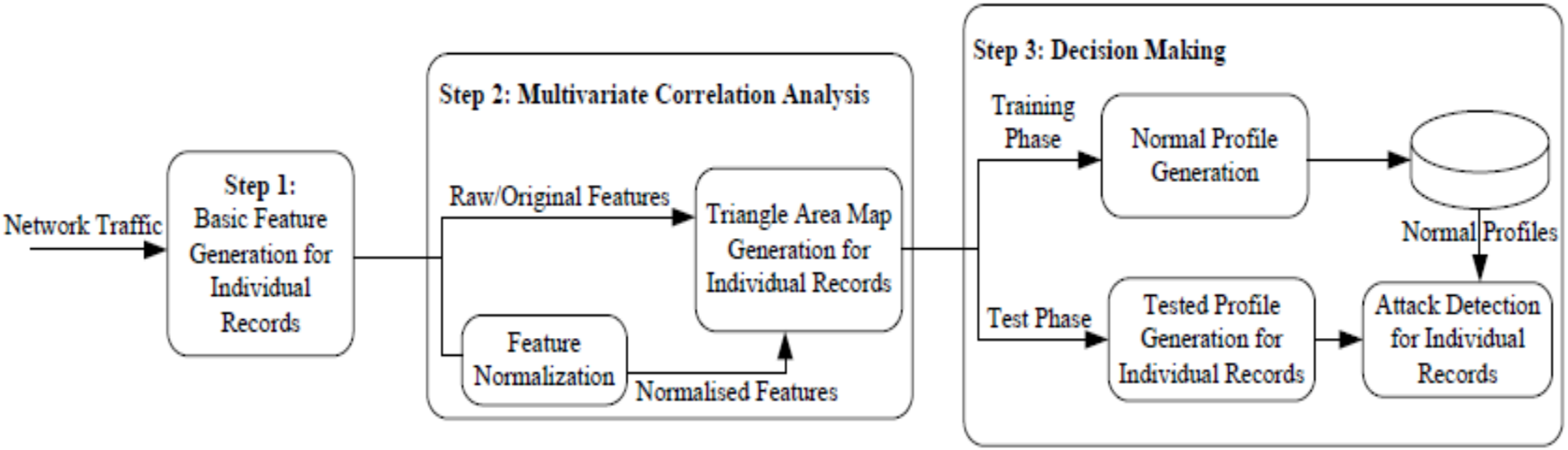
$$\text{EMD-}L_1(Y,Z) = \min_{F=\{f_{j,p;c,d}:(j,p,c,d)\in\mathcal{J}_1\}} \sum_{\mathcal{J}_1} f_{j,p;c,d}, \quad (1)$$

is subject to

$$\begin{cases} \sum_{c,d:(j,p,c,d)\in\mathcal{J}_1} (f_{j,p;c,d} - f_{c,d;j,p}) = b_{jp} \quad \forall (j,p) \in \mathcal{I} \\ f_{j,p;c,d} \geq 0 \qquad\qquad \forall (j,p,c,d) \in \mathcal{J}_1, \end{cases} \quad (2)$$

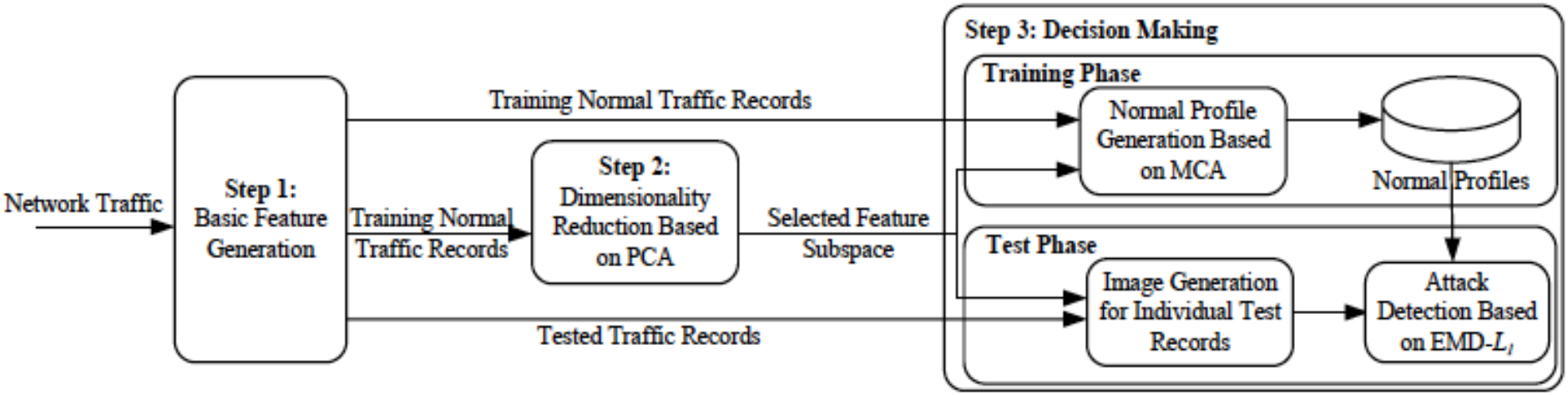
A SYSTEM FRAMEWORK FOR DOS ATTACK DETECTION – FRAMEWORK

Detection framework based on the previously proposed TAM-based MCA approach (TPDS 2014)



THE NEWLY PROPOSED FRAMEWORK

- Our proposed DoS attack detection system is comprised of three major steps
  - Basic Feature Generation
  - Dimensionality Reduction Based on PCA
  - Decision Making



OUR DETECTION MECHANISMS

- ***Traffic Monitoring at Destination***: Our proposed DoS attack detection system is deployed at the gateway of a network.
- ***Sample-by-sample Detection***: Our system investigates traffic samples individually in the process of detection.
- ***Anomaly-based Detectors***: Anomaly-based detection mechanism is adopted in our approach.
- ***Attack Recognition Based on Computer Vision***: Instances of normal traffic are interpreted as the images or the shapes that match the queries.
  - DoS attacks are interpreted as the unmatched images or the unmatched shapes.
  - EMD and its variants, make use of crossbin correlation in assessing perceptional dissimilarity between two images.

STEP 1: BASIC FEATURE GENERATION

- Basic features are generated from network traffic packets captured at the destination network.
- They are applied to construct records describing statistics for a well-defined time interval.

STEP 2: DIMENSIONALITY REDUCTION

- Our dimensionality reduction algorithm uses PCA which seeks the optimal subspace for the best representation of the data.
- The selected lower dimensional features are then used in both of the Training Phase and the Test Phase to reduce the computational overhead.

ALGORITHM FOR DIMENSIONALITY REDUCTION

- PCA is used in this work to determine the optimal feature subspace.
- The columns of the matrix W stand for the eigenvectors.

Require: Data set X $\{X$ contains n instances, and each of which has t features$\}$

Ensure: $1 \leq k \leq t$

1: $\bar{x} \leftarrow \frac{1}{n}\sum_{i=1}^{n} x_i$

2: $X_{zm} \leftarrow X - \bar{x}$ {Subtract $\bar{x}$ from each instance in X}

3: $C_X \leftarrow \frac{1}{n-1} X_{zm} X_{zm}^T$

4: Obtain Λ and W, which are subject to $\Lambda W = C_X W$

5: **for** $i = 1$ to n **do**

6: $\quad \sigma_i^2 \leftarrow \sum_{l=1}^{i} \lambda_l$

7: **end for**

8: Plot $\{\sigma_1^2, \sigma_2^2, \ldots, \sigma_n^2\}$

9: Locate the "elbow" on the scree plot and identify the index (k) of the "elbow" point

10: $W_k \leftarrow$ the selected first k eigenvectors of W

11: **return** W_k

STEP 3: DECISION MAKING – TRAINING PHASE

- Normal profiles are generated for various types of legitimate/normal traffic records (i.e., TCP, UDP and ICMP traffic).
- The normal traffic records used in this phase are identical to the set of records involved in Step 2.
- In the process of generation, normal profiles are built with the data projected onto the selected feature subspace recommended by Step 2.
- The generated normal profiles (Pro) are stored in the database and are to be used in attack detection.

A SYSTEM FRAMEWORK FOR DOS ATTACK DETECTION – MCA BASED ON TAM

The proposed TAM-based MCA approach

- Given an arbitrary dataset $X = [x_1\, x_2\, \cdots\, x_n]$, where $x_i = \begin{bmatrix} f_1^i \\ f_2^i \\ \vdots \\ f_m^i \end{bmatrix}$

- In order to obtain the triangle formed by two features (i.e., f_j^i and f_k^i), data transformation is involved.

$$y_{i,j,k} = [\varepsilon_j\ \varepsilon_k]^T x_i = \begin{bmatrix} f_j^i \\ f_k^i \end{bmatrix}, \qquad \varepsilon_j = \begin{bmatrix} e_{j,1} \\ e_{j,2} \\ \vdots \\ e_{j,m} \end{bmatrix}, \qquad \varepsilon_k = \begin{bmatrix} e_{k,1} \\ e_{k,2} \\ \vdots \\ e_{k,m} \end{bmatrix},$$

A SYSTEM FRAMEWORK FOR DOS ATTACK DETECTION – MCA BASED ON TAM

- Triangle area formed by the origin (i.e., *O*) and the projected points of the coordinate (f_j^i , f_k^i) on the *j*-axis and *k*-axis.

$$Tr_{j,k}^i = (\parallel (f_j^i, 0) - (0,0) \parallel \times \parallel (0, f_k^i) - (0,0) \parallel)/2,$$

where $1 \le i \le n$, $1 \le j \le m$, $1 \le k \le m$ and $j \ne k$.

- The Triangle Area Map (TAM) of x_i

$$TAM_{x_i} = \begin{bmatrix} 0 & Tr_{1,2}^i & \cdots & Tr_{1,m}^i \\ Tr_{2,1}^i & 0 & \cdots & Tr_{2,m}^i \\ \vdots & \vdots & \ddots & \vdots \\ Tr_{m,1}^i & Tr_{m,2}^i & \cdots & 0 \end{bmatrix}_{m \times m}$$

ALGORITHM FOR NORMAL PROFILE GENERATION

The TAM-based MCA approach is employed

Require: Data set X and subspace W_k {X contains n instances, and each of which has t features. W_k is the selected first k eigenvectors of W}

1: Initialise DIS {It is an array with n elements denoted by $Dis_i (1 \leq i \leq n)$}
2: Initialise X_{TAM} with n k-by-k matrices denoted as $TAM^i (1 \leq i \leq n)$
3: $X_{P_r} \leftarrow X \times W_k$ {X_{P_r} contains n instances, and each of which has k features}
4: **for** $i = 1$ to n **do**
5: $TAM^i \leftarrow [Tr^i_{j,p}]_{k \times k}$, where $1 \leq j, p \leq k$ {Triangle area formed involving the features j and p of X_{P_r} is computed and assigned to the (j, p)-th element in TAM^i}
6: **end for**
7: $\overline{TAM} \leftarrow \frac{1}{n} \sum_{i=1}^{n} TAM^i$
8: **for** $i = 1$ to n **do**
9: $Dis_i \leftarrow EMD\text{-}L_1(TAM^i, \overline{TAM})$ {Earth mover's distance between TAM^i and $\overline{TAM}$}
10: **end for**
11: $\overline{DIS} \leftarrow \frac{1}{n} \sum_{i=1}^{n} Dis_i$
12: $Std = \sqrt{\frac{1}{n} \sum_{i=1}^{n} (Dis_i - \overline{DIS})^2}$
13: $Pro \leftarrow (\overline{TAM}, \overline{DIS}, Std)$
14: **return** Pro

STEP 3: DECISION MAKING – TESTING PHASE

- Images of individual tested records are generated and compared against the respective normal profiles (Pro) from the Training Phase using EMD-L1 .
- Attack detection is modelled as a computer vision task, in which normal profiles are used as queries to retrieve the matched records (i.e., normal TCP, UDP and ICMP traffic records).
- Any unmatched images (records) are determined as attacks.

ALGORITHM FOR ATTACK DETECTION

- Dimensionality reduction is performed on the tested sample.
- Then, the transformation of the projected tested sample to an image is conducted.
- The image is matched against the pre-determined query.

Require: Tested sample x_{test}, subspace W_k, normal profile Pro and parameter α

1: $x_{test}^{Pr} \leftarrow x_{test} \times W_k$ {Project tested sample x_{test} onto the subspace W_k}
2: $TAM_{test} \leftarrow [Tr_{j,p}^{i}]_{k \times k}$, where $1 \leq j, p \leq k$
3: $Dis_{test} \leftarrow EMD\text{-}L_1(TAM_{test}, \overline{TAM})$
4: **if** $(\overline{DIS} - \alpha \times Std) \leq Dis_{test} \leq (\overline{DIS} + \alpha \times Std)$ **then**
5: **return** Normal
6: **else**
7: **return** Attack
8: **end if**

EXPERIMENT FEATURES

- The proposed DoS attack detection system is evaluated using the KDD Cup 99 data set and ISCX 2012 IDS Evaluation Dataset.
- The experimental results are compared against three state-of-the-art detection systems
  - network intrusion detection system based on covariance feature space,
  - triangle-area-based nearest neighbours approach and
  - DoS attack detection system using TAM-based MCA).
- The overall evaluation shows that our detection system achieves 99.95% accuracy on KDD Cup 99 data set.
- Meanwhile, our proposed detection system achieves 90.12% accuracy on the up-to-date ISCX 2012 IDS Evaluation Dataset.
- The computational complexity of our system is also discussed and compared with the three state-of-the-art detection systems.

EVALUATION ON KDD CUP 99 DATASET

- We conduct evaluations on our proposed DoS attack detection system using KDD Cup 99 data set.
- KDD Cup 99 data set has been widely used for evaluating the performance of an anomaly based IDS in detecting new intrusions.
- 10 percent labelled data subset of KDD Cup 99 data set is used, with five different types of DoS attacks:Teardrop (UDP), Smurf (ICME), Pod (ICME), Neptune (TCP) and Land attacks (TCP).
- All records of the above mentioned network traffic from the 10 percent labelled data subset are first extracted.

EVALUATION ON ISCX 2012 DATASET

- We also test our algorithm on ISCX 2012 IDS Evaluation Dataset.
- ISCX 2012 IDS Evaluation Dataset was generated from a testbed, systemically designed by the Information Security Centre of Excellence at the University of New Brunswick.
- The data set is intended to overcome the technical issues in other IDS evaluation data sets, and to provide network traces capturing updated legitimate and intrusive network behaviours and patterns.
- This data set consists of seven days' capturing with overall 2,450,324 traffic flows.
- During the evaluations, Distributed Denial of Service (DDoS) attack traffic from Tuesday's network trace is used.
- It contains 8,720 attack traffic flows. As such, the effectiveness of our detection system on modern traffic can be evaluated.

EVALUATION MATRICES

- Four metrics are used to quantitatively estimate the performance of our proposed system.
  - namely True Negative Rate (TNR)
  - Detection Rate (DR)
  - False Positive Rate (FPR)
  - Accuracy (i.e. the proportion of the overall samples which are classified correctly).

DETECTION RESULTS ON KDD 99

TABLE I
NUMBER OF RECORDS OF NORMAL AND DOS ATTACK RECORDS

Normal	Teardrop	Smurf	Pod	Neptune	Land
97,260	9,790	2,807,900	2,640	1,072,010	210

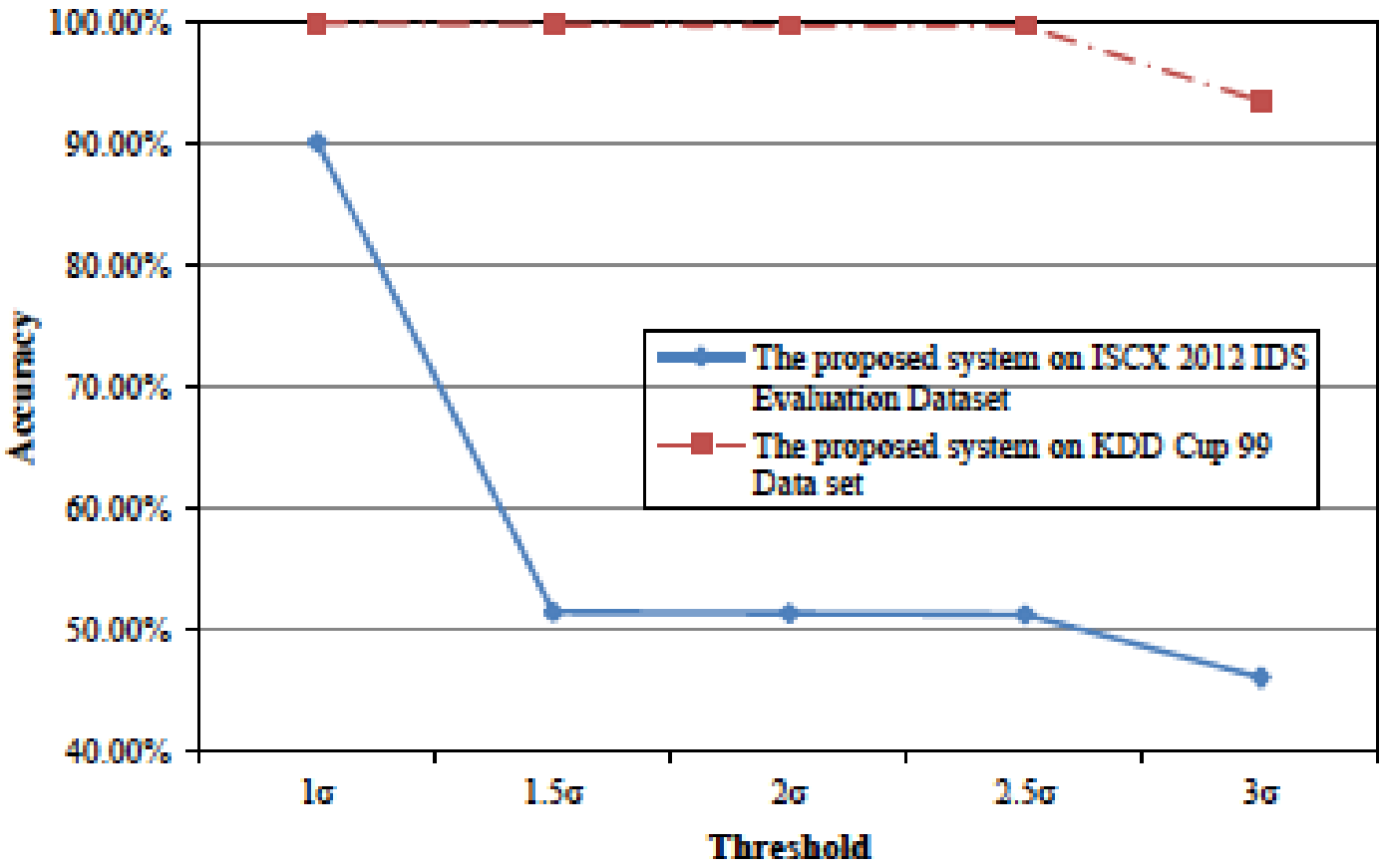
TABLE II
THE NUMBERS OF PRINCIPLE COMPONENTS USING IN THE TRAINING AND TEST FOR VARIOUS NETWORK TRAFFIC

Type of Traffic	TCP	UDP			ICMP		
No. of PCs	3 PCs	5 PCs	6 PCs	7 PCs	3 PCs	4 PCs	5 PCs

TABLE III
FALSE POSITIVE RATES, DETECTION RATES AND ACCURACIES ACHIEVING BY THE PROPOSED SYSTEM BASED ON KDD CUP 99 DATA SET

	Threshold				
	1σ	1.5σ	2σ	2.5σ	3σ
FPR	1.93%	1.19%	0.63%	0.60%	0.58%
DR	100.00%	99.83%	99.68%	99.68%	93.35%
Accuracy	99.95%	99.81%	99.67%	99.67%	93.50%

THRESHOLD VS ACCURACY



DETECTION RESULTS ON ISCX 2012

TABLE IV
FALSE POSITIVE RATES, DETECTION RATES AND ACCURACIES ACHIEVING BY THE PROPOSED SYSTEM BASED ON ISCX 2012 IDS EVALUATION DATASET

	Threshold				
	1σ	1.5σ	2σ	2.5σ	3σ
FPR	7.92%	4.75%	3.33%	2.00%	1.25%
DR	90.04%	49.82%	49.64%	49.48%	44.09%
Accuracy	90.12%	51.54%	51.41%	51.31%	46.15%

COMPARISON WITH STATE-OF-THE-ART

TABLE V
PERFORMANCE COMPARISONS WITH DIFFERENT DETECTION APPROACHES

	Network intrusion detection based on covariance feature space [11] (Threshold approach with 4D principle and *Cov_len*3_150)	Triangle area based nearest neighbours approach [12]	A system for DoS attack detection using TAM-based MCA [13] (Normalized data, Threshold = 1.5σ)	The proposed DoS attack detection system based on TAM and EMD (Threshold = 1σ)
Accuracy	97.89%	92.15%	99.95%	99.95%

TABLE VI
COMPUTATIONAL COMPLEXITIES OF DIFFERENT STATE-OF-THE-ART DETECTION APPROACHES

The proposed detection system	Network intrusion detection based on covariance feature space [11]	Triangle area based nearest neighbours approach [12]
$O(m^4)$	$O(lm^2)$	$O(l^2n^2)$

m^2 is the number of elements within a TAM, l is the number of clusters used in generating triangle areas and n is the number of training samples).

CONCLUSIONS

- This paper has proposed a DoS attack detection system using MCA technique and the EMD-L1 .
- MCA helps extract the correlations between individual pairs of two distinct features within each network traffic record
- EMD- L1 facilitates our system to be able to effectively distinguish both known and unknown DoS attacks from legitimate traffic.
- Evaluation has been conducted using the KDD Cup 99 data set and ISCX 2012 IDS.
- The results have revealed that our detection system achieves maximum 99.95% detection accuracy on KDD 99 and 90.12% detection accuracy on ISCX 2012.
- It outperforms three state-of-the-art approaches.
- The computational complexity achieves comparable performance in comparison with the two state-of-the-art approaches.
- The time cost analysis shows that the proposed detection system is able to cope with high speed network segments.

CONCLUSIONS (CONT.)

- Future Work*
  - Collaborative intrusion detection.
  - Intrusion detection for cloud computing.

*Tan, Nagar, He et al., Enhancing Big Data Security with Collaborative Intrusion Detection, IEEE Cloud Computing 2014

Questions!!!

Thank you for Listening

Email: Xiangjian.He@uts.edu.au