A COMPARATIVE STUDY OF ANOMALY DETECTION SCHEMES IN NETWORK INTRUSION DETECTION

Aleksandar Lazarevic, Levent Ertoz,
Aysel Ozgur, Vipin Kumar, Jaideep Srivastava

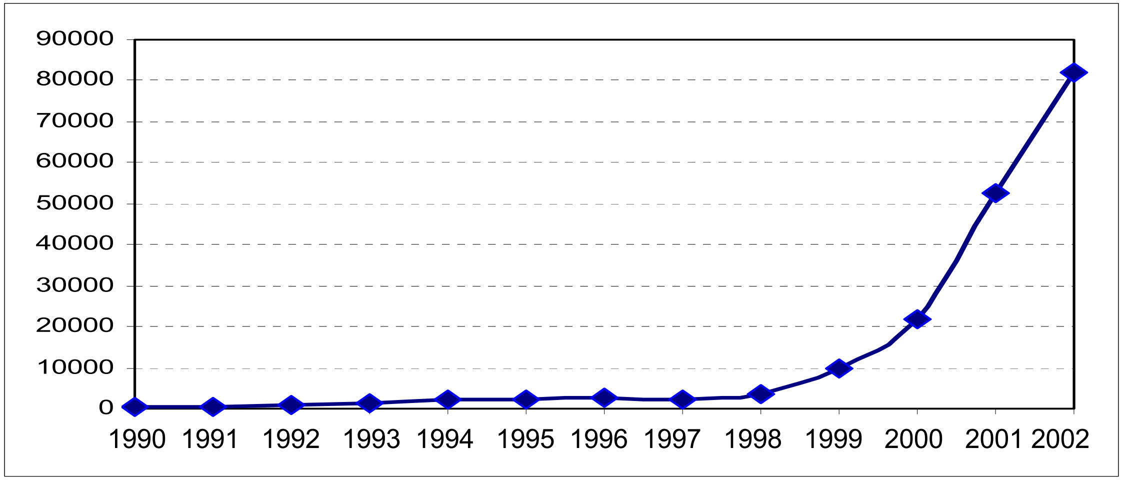
Department of Computer Science
University of Minnesota

Research supported by AHPCRC/ARL

Introduction

- Due to the proliferation of high-speed Internet access, more and more organizations are becoming increasingly vulnerable to potential cyber threats such as network intrusions

Incidents Reported to Computer Emergency Response Team/Coordination Center (CERT/CC)

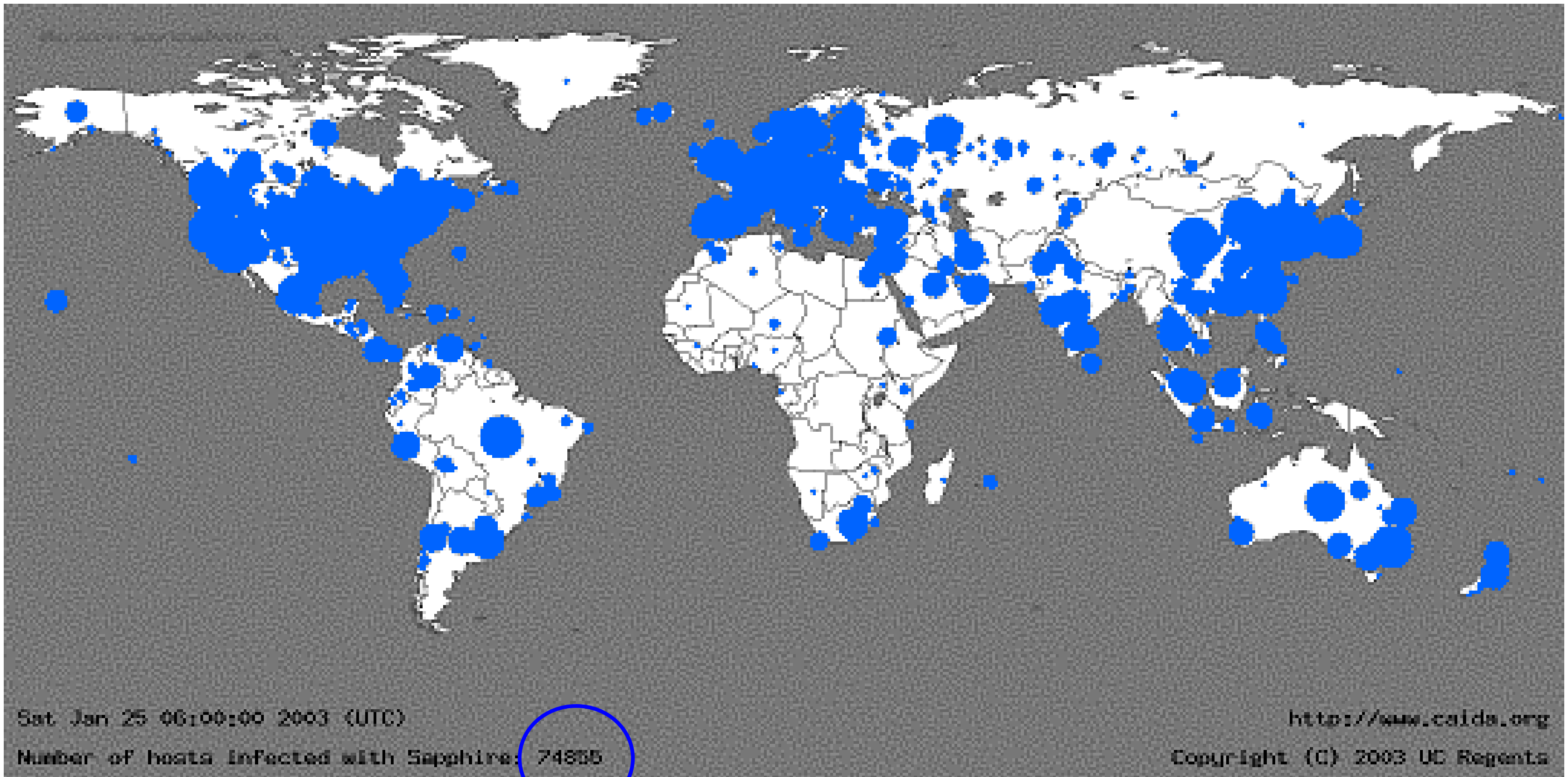


- Sophistication of cyber attacks as well as their severity has also increased recently (e.g., Code-Red I & II, Nimda, and more recently the SQL slammer worm on Jan. 25)

AHPCRC

The Spread of the Sapphire/Slammer Worm

- The geographic spread of Sapphire/Slammer Worm 30 minutes after release on January 25th, 2003



Source: www.caida.org

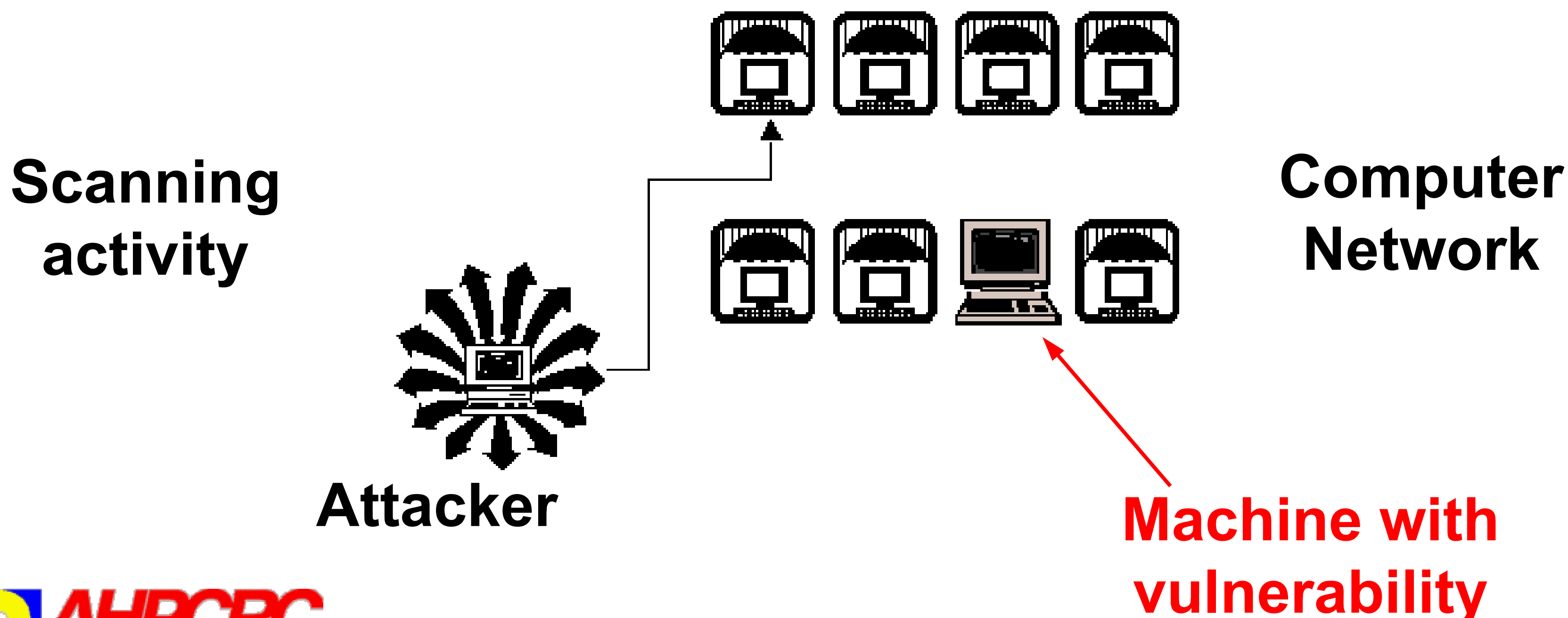
Why we need intrusion detection systems?

- **Security mechanisms always have inevitable vulnerabilities**
- **Current firewalls are not sufficient to ensure security in computer networks**
- **Increasingly important to make our information systems, resistant to and tolerant of various computer attacks**

AHPCRC

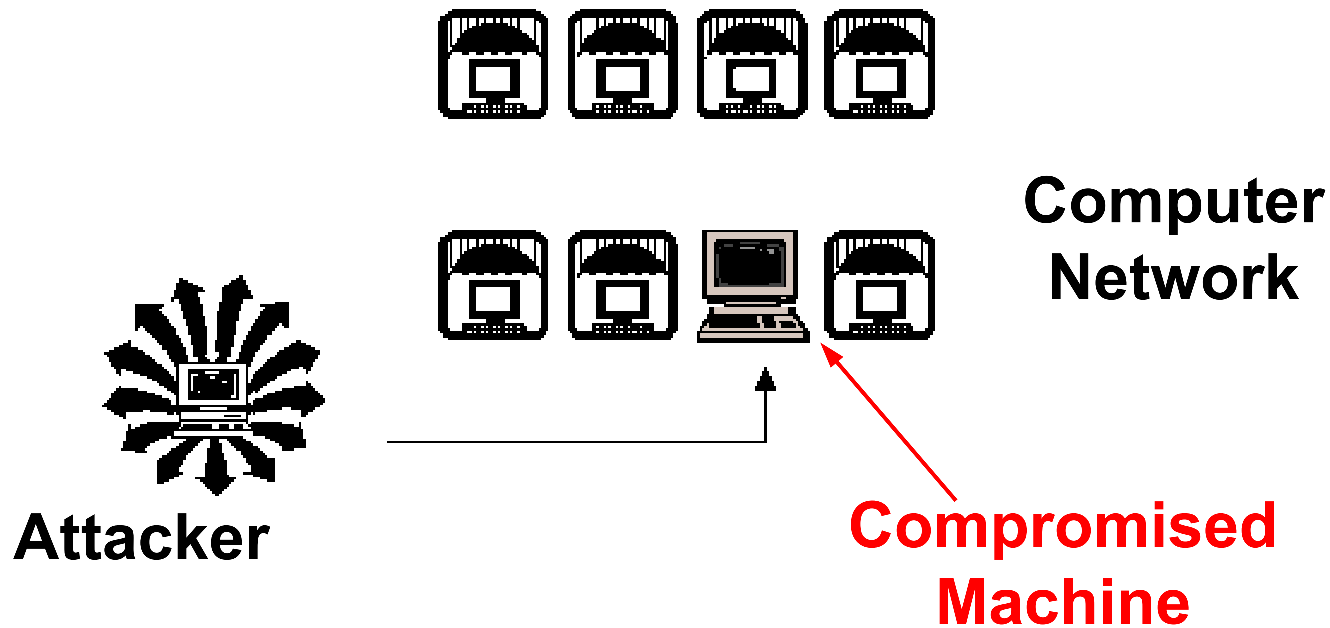
What are Intrusions?

- Intrusions are actions that attempt to bypass security mechanisms of computer systems. They are caused by:
  - Attackers accessing the system from Internet
  - Insider attackers - authorized users attempting to gain and misuse non-authorized privileges
- Typical intrusion scenario



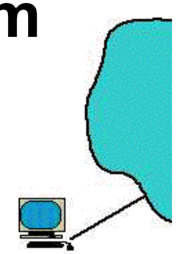
What are Intrusions?

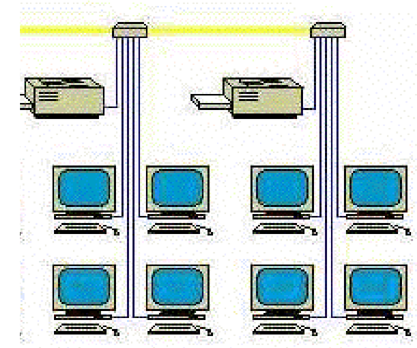
- Intrusions are actions that attempt to bypass security mechanisms of computer systems. They are caused by:
  - Attackers accessing the system from Internet
  - Insider attackers - authorized users attempting to gain and misuse non-authorized privileges
- Typical intrusion scenario



Intrusion Detection Systems (IDS)

- **Intrusion Detection System**
  - **combination of software and hardware that attempts to perform intrusion detection**
  - **raises the alarm when possible intrusion happens**





- **Traditional intrusion detection system IDS tools (e.g. SNORT) are based on signatures of known attacks**
  - **Example of SNORT rule (MS-SQL “Slammer” worm)**

    any -> udp port 1434 (content:"|81 F1 03 01 04 9B 81 F1 01|"; content:"sock"; content:"send")

www.snort.org

- **Limitations**
  - **Signature database has to be manually revised for each new type of discovered intrusion**
  - **They cannot detect emerging cyber threats**
  - **Substantial latency in deployment of newly created signatures**
- **Data mining based IDSs can alleviate this limitation**

AHPCRC

Data Mining for Intrusion Detection

- ***Misuse detection***
  - **Building predictive models from labeled labeled data sets (instances are labeled as “normal” or “intrusive”)**
  - **Can only detect known attacks and their variations**
  - **High accuracy in detecting many kinds of known attacks**
- ***Anomaly detection***
  - **Able to detect novel attacks as deviations from “normal” behavior**
  - **Potential high false alarm rate - previously unseen (yet legitimate) system behaviors may also be recognized as anomalies**

AHPCRC

Evaluation of Intrusion Detection Systems

Standard metrics for evaluations of intrusions (attacks)

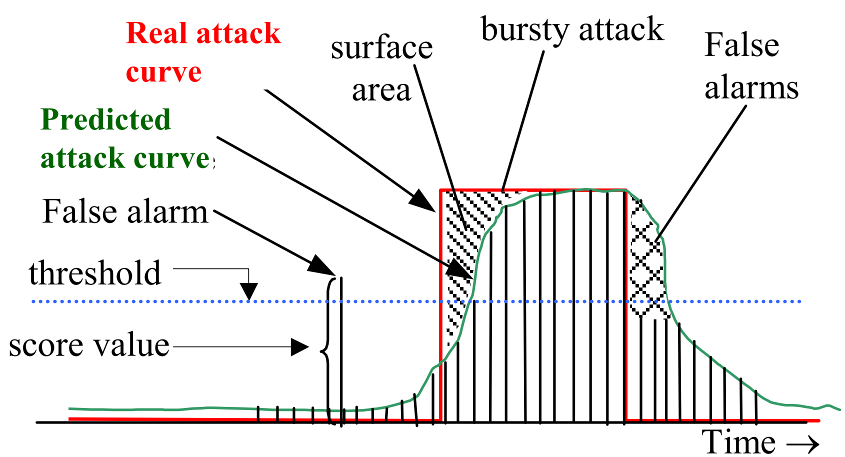
Standard metrics		Predicted connection label	
		Normal	Intrusions (Attacks)
Actual connection label	Normal	True Negative (TN)	False Alarm (FP)
	Intrusions (Attacks)	False Negative (FN)	Correctly detected intrusions - Detection rate (TP)

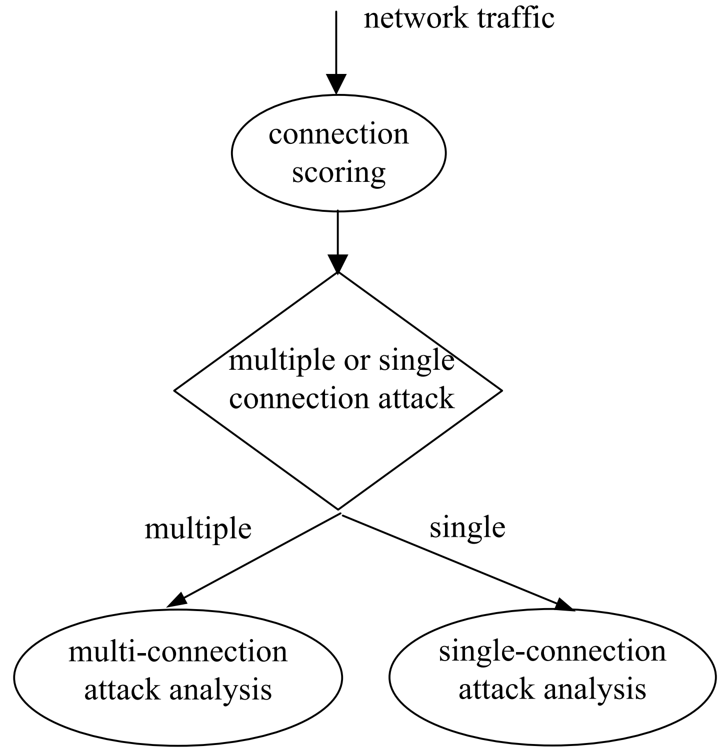
- **Standard measures for evaluating IDSs:**
  - ***Detection rate*** **- ratio between the number of correctly detected attacks and the total number of attacks**
  - ***False alarm (false positive)*** **rate - ratio between the number of normal connections that are incorrectly misclassified as attacks (False Alarms in Table) and the total number of normal connections**
  - **Trade-off between detection rate and false alarm rate**

AHPCRC

Characteristics of network intrusions

- **Two types of network intrusions:**
  - **Single connection attacks**
  - **Multi-connection attacks**

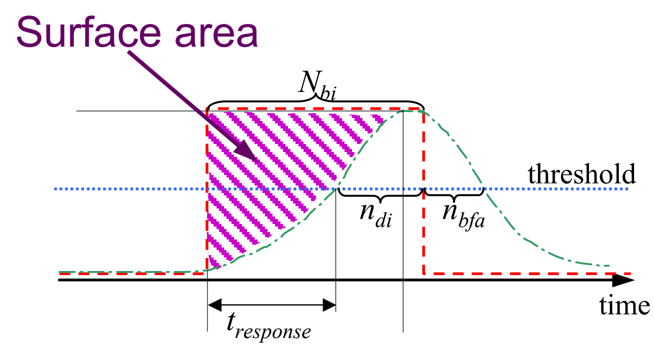




AHPCRC

Alternative evaluation measures for IDS

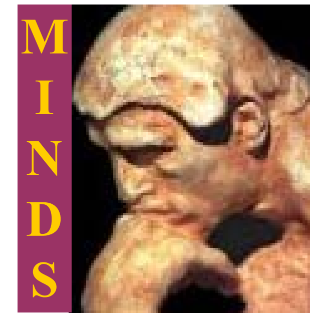
- **Surface area between the real attack curve and the predicted attack curve**
- **The smaller the surface area between the real and the predicted attack curve, the better the intrusion detection algorithm**

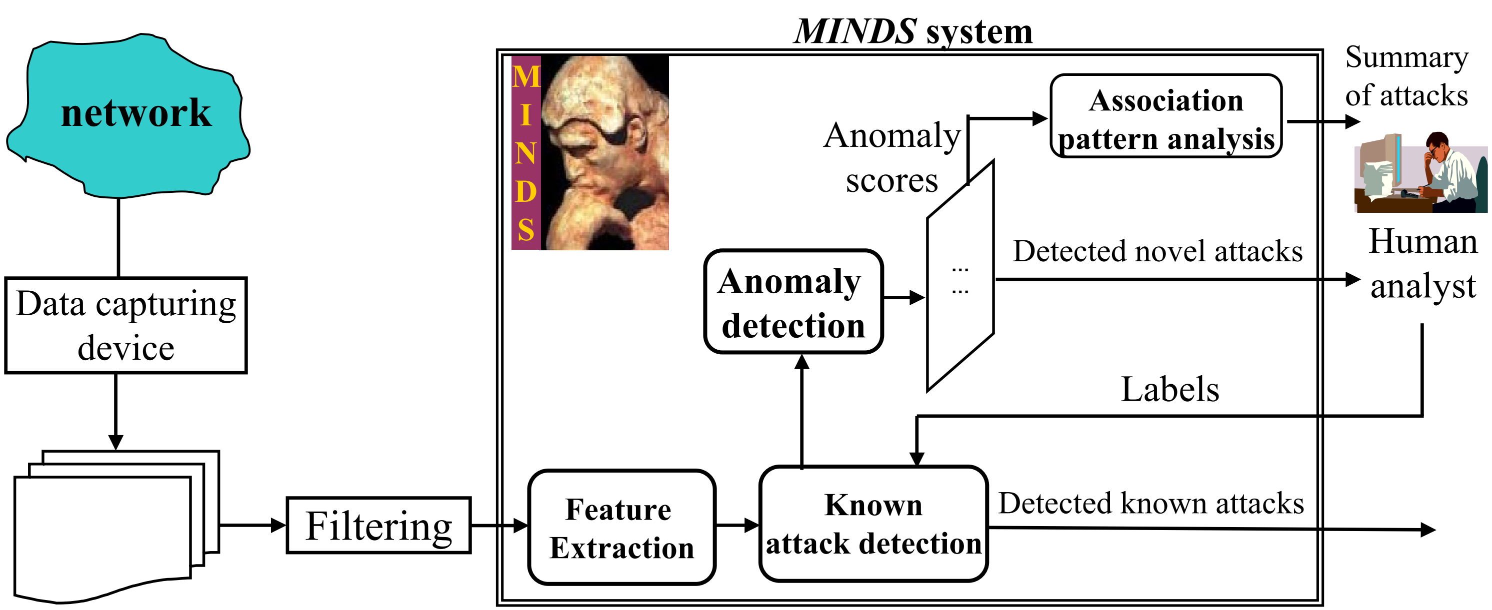


Metric	Definition
bdr	*burst detection rate* = n_{di}/N_{bi}
n_{di}	number of intrusive connections that have score value higher than threshold
n_{bfa}	number of normal connections that follow attack and that are misclassified as intrusive
$t_{response}$	*response time* – time to reach the prespecified threshold

The MINDS Project

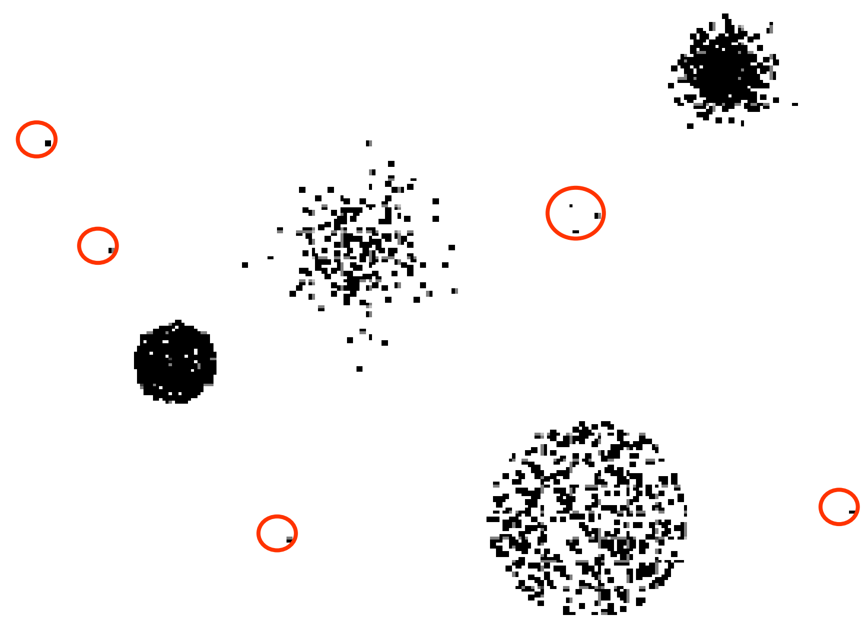
- **MINDS - Minnesota Intrusion Detection System, uses a suite of data mining techniques to analyze network traffic data**





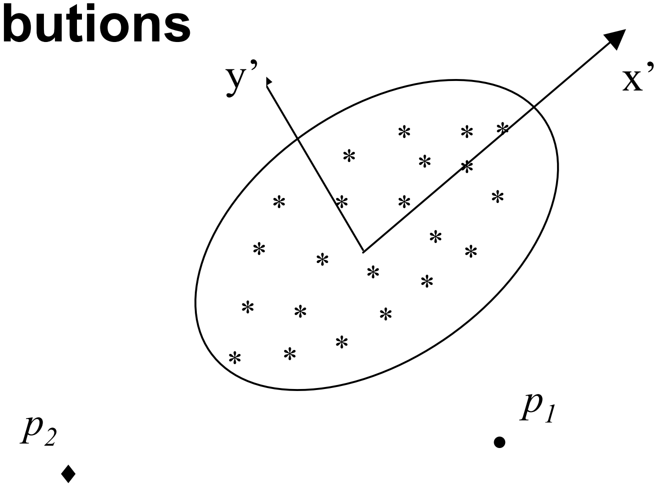
Anomaly/Outlier Detection Schemes

- **Approach**
  - Detecting novel attacks/intrusions by identifying them as deviations from “normal” behavior
- **Goals:**
  - Construct useful set of features for data mining algorithms
  - Identify novel intrusions using outlier detection schemes
    - Distance based techniques
      - Nearest Neighbor approach
      - Mahalanobis distance based
    - Density based schemes
    - Unsupervised support vector machines (SVMs)



Distance based Outlier Detection Schemes

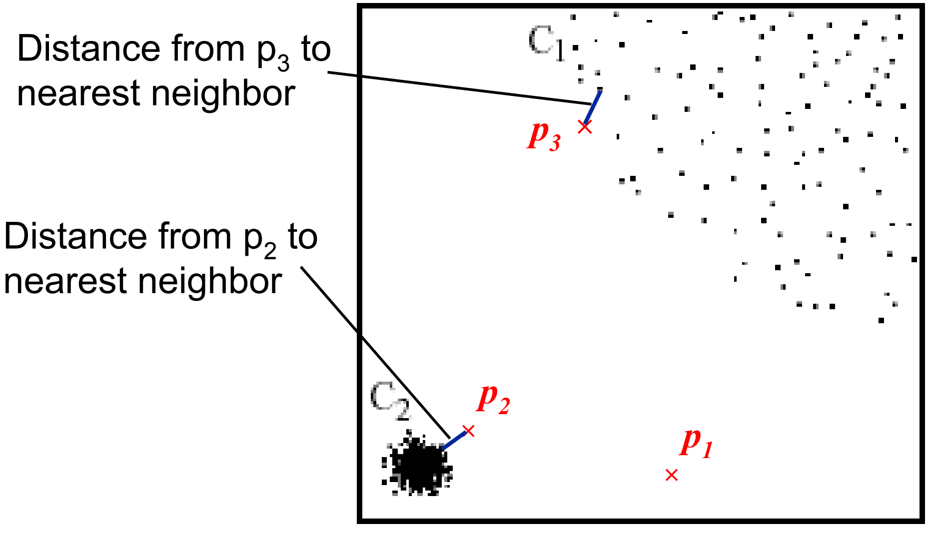
- ***Nearest Neighbor (NN) approach***
  - For each point compute the distance to the *k-th* nearest neighbor d_k
  - Outliers are points that have larger distance d_k and therefore are located in the more sparse neighborhoods
  - Not suitable for datasets that have modes with varying density
- ***Mahalanobis-distance based approach***
  - Mahalanobis distance is more appropriate for computing distances with skewed distributions



AHPCRC

Density based Outlier Detection Schemes

- ***Local Outlier Factor (LOF) approach***
  - **For each point compute the density of local neighborhood**
  - **Compute *LOF* of example *p* as the average of the ratios of the density of example *p* and the density of its nearest neighbors**
  - **Outliers are points with the largest *LOF* value**

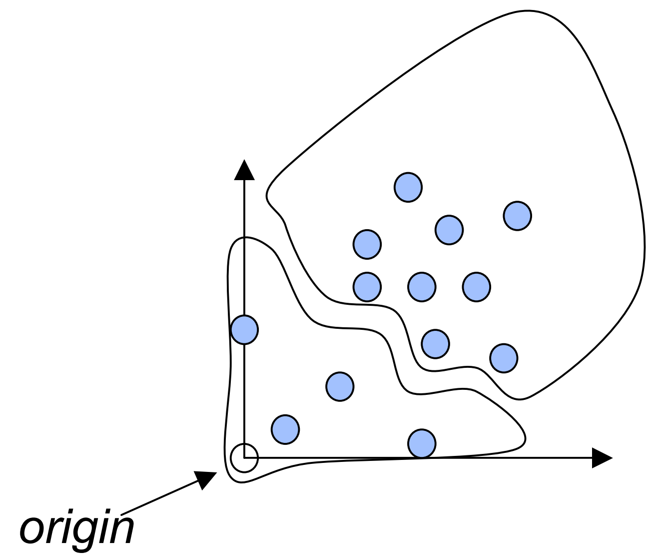


In the *NN* approach, p_2 is not considered as outlier, while the *LOF* approach find both p_1 and p_2 as outliers

NN approach may consider p_3 as outlier, but LOF approach does not

Unsupervised Support Vector Machines for Outlier Detection

- **Unsupervised SVMs attempt to separate the entire set of training data from the origin, i.e. to find a small region where most of the data lies and label data points in this region as one class**
- **Parameters**
  - **Expected number of outliers**
  - **Variance of rbf kernel**
    - **As the variance of the rbf kernel gets smaller, the separating surface gets more complex**



push the hyper plane away from origin as much as possible

AHPCRC

DARPA 1998 Data Set

- DARPA 1998 data set (prepared and managed by MIT Lincoln Lab) includes a wide variety of intrusions simulated in a military network environment
- 9 weeks of raw TCP dump data
  - 7 weeks for training (5 million connection records)
  - 2 weeks for training (2 million connection records)
- Connections are labeled as normal or attacks (4 main categories of attacks - 38 attack types)
  - DOS - Denial Of Service
  - Probe - e.g. port scanning
  - U2R - unauthorized access to gain root privileges,
  - R2L - unauthorized remote login to machine,
- Two types of attacks
  - Bursty attacks - involve multiple network connections
  - Non-bursty attacks - involve single network connections

Feature Extraction Module

- Four groups of features
  - Basic features of individual TCP connections
    - source & destination IP/port, protocol, number of bytes, duration, number of packets (used in SNORT only in stream builder module)
  - Content based features
    - Features extracted from “raw tcpdump” data (e.g. the number of SYN packets flowing from source to destination)
  - Time based features
    - For the same source (destination) IP address, number of unique destination (source) IP addresses inside the network *in last T seconds*
    - Number of connections from source (destination) IP to the same destination (source) port *in last T seconds*
  - Connection based features
    - For the same source (destination) IP address, number of unique destination (source) IP addresses inside the network *in last N connections*
    - Number of connections from source (destination) IP to the same destination (source) port *in last N connections*

MINDS Outlier Detection on DARPA'98 Data

- Detection rate using standard evaluation measures for fixed false alarm rate 2%

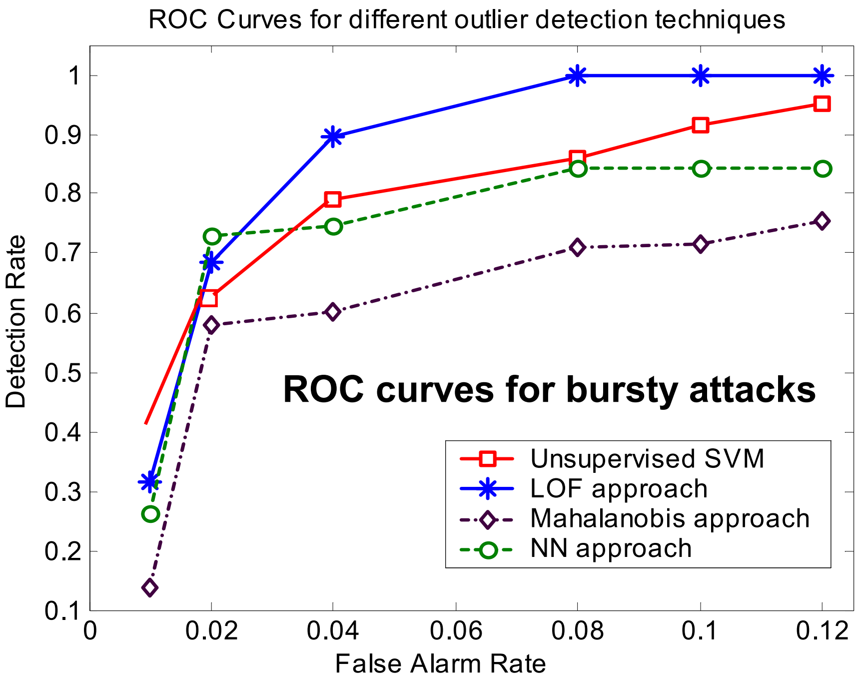
Attack type	LOF	NN	Mahalanobis	SVM
DoS	3/3	2/3	1/3	2/3
probe (scan)	7/11	9/11	7/11	7/11
U2R	2/3	2/3	2/3	2/3
R2L	1/2	1/2	1/2	1/2
Total Detection Rate	13/19 (68.4%)	14/19 (73.7%)	11/19 (57.9%)	12/19 (63.2%)

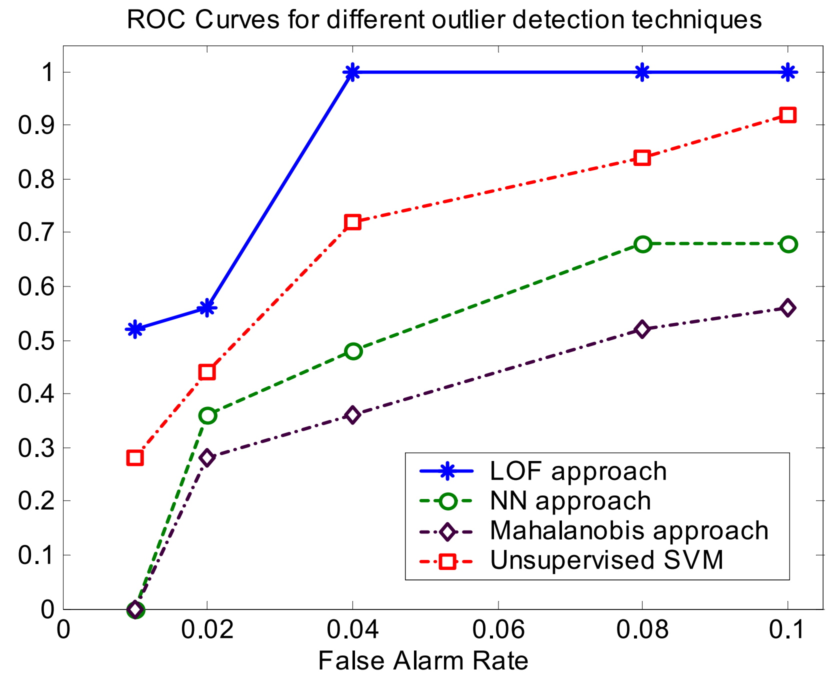
- Detection rate using alternative measures (FA - 2%)

Attack type	LOF	NN	Mahalanobis	SVM
DoS	3/3	2/3	1/3	3/3
probe (scan)	8/11	10/11	6/11	9/11
U2R	2/3	2/3	2/3	2/3
R2L	1/2	1/2	1/2	1/2
Total Detection rate	14/19 (73.7%)	15/19 (78.9%)	10/19 (52.6%)	15/19 (78.9%)

AHPCRC

MINDS Outlier Detection on DARPA'98 Data





ROC curves for single-connection attacks

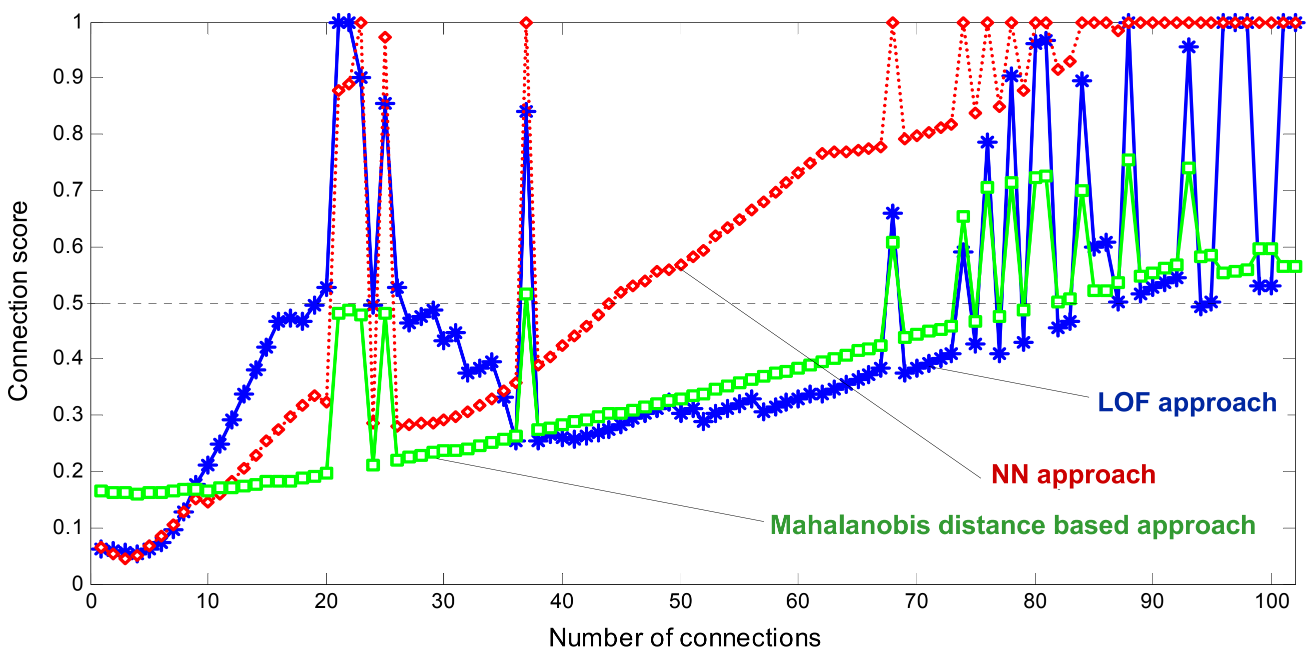
- ***LOF approach*** **is consistently better than other approaches**
- ***Unsupervised SVMs*** **are good but only for high false alarm (FA) rate**
- ***NN approach*** **is comparable to LOF for low FA rates, but detection rate decrease for high FA**
- ***Mahalanobis-distance approach*** **– poor due to multimodal normal behavior**

- ***LOF approach*** **is superior to other outlier detection schemes**
- **Majority of single connection attacks are probably located close to the dense regions of the normal data**

AHPCRC

Outlier Detection Recent Results (on DARPA'98 data)

- **Analyzing multi-connection attacks using the score values assigned to network connections**
- **Detection rate is measured through number of connections that have score higher than 0.5**



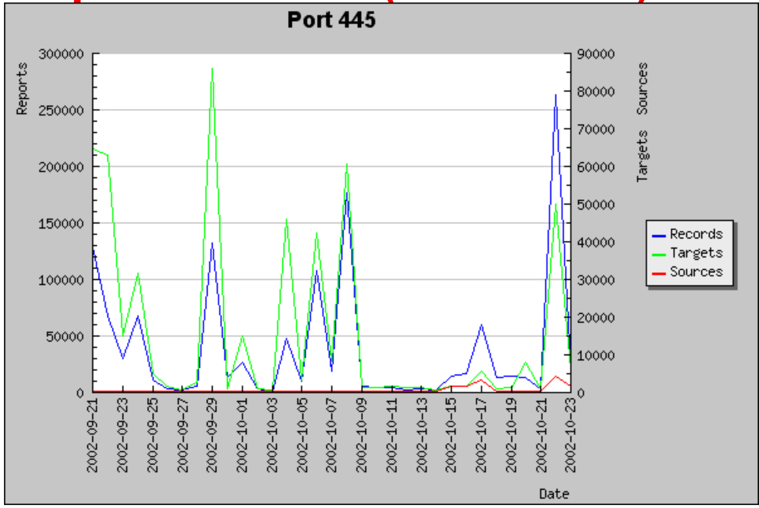
Low peaks due to occasional "reset" value for the feature called "connection status"

Anomaly Detection on Real Network Data

- During the past nine months various intrusive/suspicious activities were detected at the AHPCRC and at the U of Minnesota using *MINDS*
- Many of these could not be detected using state-of-the-art tools like SNORT
- Anomalies/attacks picked by *MINDS*
  - Scanning activities
  - Non-standard behavior
    - Policy violations
    - Worms

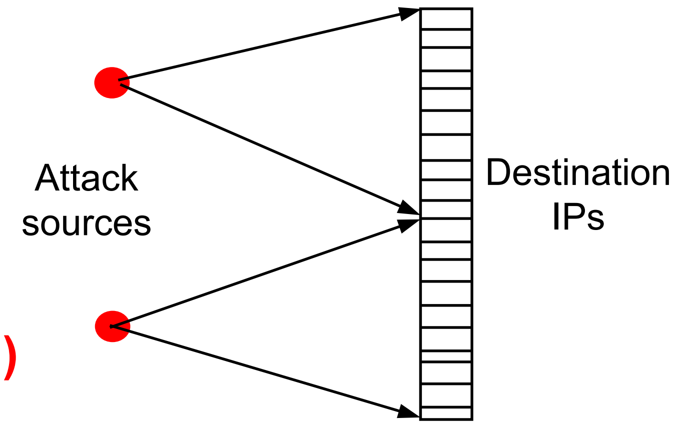
Detection of Scans on Real Network Data

- **August 13, 2002**
  - **Detected scanning for Microsoft DS service on port 445/TCP (Ranked #1)**
    - **Reported by CERT as recent DoS attack that needs further analysis (CERT August 9, 2002)**
    - **Undetected by SNORT since the scanning was non-sequential (very slow)**
    - **A rule added to SNORT later in September**



Number of scanning activities on Microsoft DS service on port 445/TCP reported in the World (Source www.incidents.org)

- **August 13, 2002**
  - **Detected scan for Oracle server (Ranked #2)-Reported by CERT, June 13, 2002**
    - **First detection of this attack type by our University**
    - **Undetected by SNORT because the scanning was hidden within another Web scanning**
- **October 10, 2002**
  - **Detected a distributed windows networking scan from multiple source locations (Ranked #1)**



Distributed scanning activity

Detection of Policy Violations on Real Network Data

- **August 8, 2002**
  - Identified machine that was running Microsoft PPTP VPN server on non-standard ports, which is a policy violation (Ranked #1)
    - Undetected by SNORT since the collected GRE traffic was part of the normal traffic
- **August 10 2002, October 30, 2002**
  - Identified compromised machines that were running FTP servers on non-standard ports, which is a policy violation (Ranked #1)
    - Anomaly detection identified this due to huge file transfer on a non-standard port
    - Undetectable by SNORT due to the fact there are no signatures for these activities
    - Example of anomalous behavior following a successful Trojan horse attack

AHPCRC

Detection of Policy Violations on Real Network Data

- **February 6, 2003**
  - **Detected a computer on the network apparently communicating with a computer in California over a VPN.**
    - ***Worst case*: This is a covert channel by which someone might be gaining access to the University network in an unauthorized way.**
    - ***Best case*: This is someone at the University creating unauthorized tunnels between the University and some other network, which is not allowed.**
- **February 7, 2003**
  - **Detected a computer in the CS department talking on IPv6**
    - **This is extremely rare traffic and represents a possible covert tunnel to the outside world**
    - **It turns out that the person doing this is on system staff and is in fact using this as a covert tunnel to his home computers**

Detection of Worms on Real Network Data

- **January 26, 2003 (48 hours after the "slammer" worm)**

score	srcIP	sPort	dstIP	dPort	protocc	flags	packets	bytes	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
37674.69	63.150.X.253	1161	128.101.X.29	1434	17	16	[0,2)	[0,1829)	0	0	0	0	0	0	0	0	0.81	0	0.59	0	0	0	0	0
26676.62	63.150.X.253	1161	160.94.X.134	1434	17	16	[0,2)	[0,1829)	0	0	0	0	0	0	0	0	0.81	0	0.59	0	0	0	0	0
24323.55	63.150.X.253	1161	128.101.X.185	1434	17	16	[0,2)	[0,1829)	0	0	0	0	0	0	0	0	0.81	0	0.58	0	0	0	0	0
21169.49	63.150.X.253	1161	160.94.X.71	1434	17	16	[0,2)	[0,1829)	0	0	0	0	0	0	0	0	0.81	0	0.58	0	0	0	0	0
19525.31	63.150.X.253	1161	160.94.X.19	1434	17	16	[0,2)	[0,1829)	0	0	0	0	0	0	0	0	0.81	0	0.58	0	0	0	0	0
19235.39	63.150.X.253	1161	160.94.X.80	1434	17	16	[0,2)	[0,1829)	0	0	0	0	0	0	0	0	0.81	0	0.58	0	0	0	0	0
17679.1	63.150.X.253	1161	160.94.X.220	1434	17	16	[0,2)	[0,1829)	0	0	0	0	0	0	0	0	0.81	0	0.58	0	0	0	0	0
8183.58	63.150.X.253	1161	128.101.X.108	1434	17	16	[0,2)	[0,1829)	0	0	0	0	0	0	0	0	0.82	0	0.58	0	0	0	0	0
7142.98	63.150.X.253	1161	128.101.X.223	1434	17	16	[0,2)	[0,1829)	0	0	0	0	0	0	0	0	0.82	0	0.57	0	0	0	0	0
5139.01	63.150.X.253	1161	128.101.X.142	1434	17	16	[0,2)	[0,1829)	0	0	0	0	0	0	0	0	0.82	0	0.57	0	0	0	0	0
4048.49	142.150.Y.101	0	128.101.X.127	2048	1	16	[2,4)	[0,1829)	0	0	0	0	0	0	0	0	0.83	0	0.56	0	0	0	0	0
4008.35	200.250.Z.20	27016	128.101.X.116	4629	17	16	[2,4)	[0,1829)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
3657.23	202.175.Z.237	27016	128.101.X.116	4148	17	16	[2,4)	[0,1829)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
3450.9	63.150.X.253	1161	128.101.X.62	1434	17	16	[0,2)	[0,1829)	0	0	0	0	0	0	0	0	0.82	0	0.57	0	0	0	0	0
3327.98	63.150.X.253	1161	160.94.X.223	1434	17	16	[0,2)	[0,1829)	0	0	0	0	0	0	0	0	0.82	0	0.57	0	0	0	0	0
2796.13	63.150.X.253	1161	128.101.X.241	1434	17	16	[0,2)	[0,1829)	0	0	0	0	0	0	0	0	0.82	0	0.57	0	0	0	0	0
2693.88	142.150.Y.101	0	128.101.X.168	2048	1	16	[2,4)	[0,1829)	0	0	0	0	0	0	0	0	0.83	0	0.56	0	0	0	0	0
2683.05	63.150.X.253	1161	160.94.X.43	1434	17	16	[0,2)	[0,1829)	0	0	0	0	0	0	0	0	0.82	0	0.57	0	0	0	0	0
2444.16	142.150.Y.236	0	128.101.X.240	2048	1	16	[2,4)	[0,1829)	0	0	0	0	0	0	0	0	0.83	0	0.56	0	0	0	0	0
2385.42	142.150.Y.101	0	128.101.X.45	2048	1	16	[0,2)	[0,1829)	0	0	0	0	0	0	0	0	0.83	0	0.56	0	0	0	0	0
2114.41	63.150.X.253	1161	160.94.X.183	1434	17	16	[0,2)	[0,1829)	0	0	0	0	0	0	0	0	0.82	0	0.57	0	0	0	0	0
2057.15	142.150.Y.101	0	128.101.X.161	2048	1	16	[0,2)	[0,1829)	0	0	0	0	0	0	0	0	0.83	0	0.56	0	0	0	0	0
1919.54	142.150.Y.101	0	128.101.X.99	2048	1	16	[2,4)	[0,1829)	0	0	0	0	0	0	0	0	0.83	0	0.56	0	0	0	0	0
1634.38	142.150.Y.101	0	128.101.X.219	2048	1	16	[2,4)	[0,1829)	0	0	0	0	0	0	0	0	0.83	0	0.56	0	0	0	0	0
1596.26	63.150.X.253	1161	128.101.X.160	1434	17	16	[0,2)	[0,1829)	0	0	0	0	0	0	0	0	0.82	0	0.57	0	0	0	0	0
1513.96	142.150.Y.107	0	128.101.X.2	2048	1	16	[0,2)	[0,1829)	0	0	0	0	0	0	0	0	0.83	0	0.56	0	0	0	0	0
1389.09	63.150.X.253	1161	128.101.X.30	1434	17	16	[0,2)	[0,1829)	0	0	0	0	0	0	0	0	0.82	0	0.57	0	0	0	0	0
1315.88	63.150.X.253	1161	128.101.X.40	1434	17	16	[0,2)	[0,1829)	0	0	0	0	0	0	0	0	0.82	0	0.57	0	0	0	0	0
1279.75	142.150.Y.103	0	128.101.X.202	2048	1	16	[0,2)	[0,1829)	0	0	0	0	0	0	0	0	0.83	0	0.56	0	0	0	0	0
1237.97	63.150.X.253	1161	160.94.X.32	1434	17	16	[0,2)	[0,1829)	0	0	0	0	0	0	0	0	0.83	0	0.56	0	0	0	0	0
1180.82	63.150.X.253	1161	128.101.X.61	1434	17	16	[0,2)	[0,1829)	0	0	0	0	0	0	0	0	0.83	0	0.56	0	0	0	0	0
1107.78	63.150.X.253	1161	160.94.X.154	1434	17	16	[0,2)	[0,1829)	0	0	0	0	0	0	0	0	0.83	0	0.56	0	0	0	0	0

AHPCRC

Conclusion

- LOF is more robust than Nearest Neighbor and SVM in detecting both single connection and bursty attacks
- Mahalanobis distance based approach has poor performance (potentially due to multi-modality of data)
- Computational complexity is O($n*k + k^2$) for LOF and O($n*k$) for NN approach, where n is test set size and k is training set size.
  - Optimizations are possible for low dimensional problems
- LOF performs well on real life network data

AHPCRC

Questions?

Thanks !