A novel hybrid intrusion detection method integrating anomaly detection with misuse detection

GISUNG KIM, SEUNGMIN LEE, SEHUN KIM

INSTITUTE FOR IT CONVERGENCE, KAIST, GUSEONG-DONG, YUSEONG-GU, DAEJEON 305-701, SOUTH KOREA

FUTURE RESEARCH CREATIVE LABORATORY, ETRI 218 GAJEONG-RO, YUSEONG-GU, DAEJEON 305-700, SOUTH KOREA

Situation

- Two categories of Intrusion Detection algorithms
  - Misuse Detection
    - Detect attacks based on known attack signatures
    - Effective for known attacks with low errors
    - Can not detect new attacks
  - Anomaly Detection
    - Analyze and profile normal traffic patterns
    - Can detect new attacks
    - Higher false positive rate

Task

- Hybrid Intrusion Detection method
  - Combine Misuse and Anomaly Detection
- Previous Approach:
  - Independently train misuse and anomaly detection models
  - Aggregate results of detection models
    - Consider as attack if at least one of the two models classify as attack
      - High False Positive rate
    - Consider as attack only if both models classify as attack
      - Lower Recall rate

Approach

- Hierarchically integrate misuse detection with anomaly detection
- Anomaly model indirectly uses known attack information to build normal behavior profiles
- Use misuse detection model to decompose normal training data
  - Separate into disjoint subsets
  - Build anomaly detection model for each subset

Approach

- C4.5 Decision Tree (DT) used to create misuse detection model
  - Trained on normal traffic and known attack data
  - Produces disjoint subsets
- One Class Support Vector Machine (1-class SVM) used to create anomaly detection models
  - Trained for each disjoint subset from DT
  - Reduced data set sizes means 50% reduction in training time

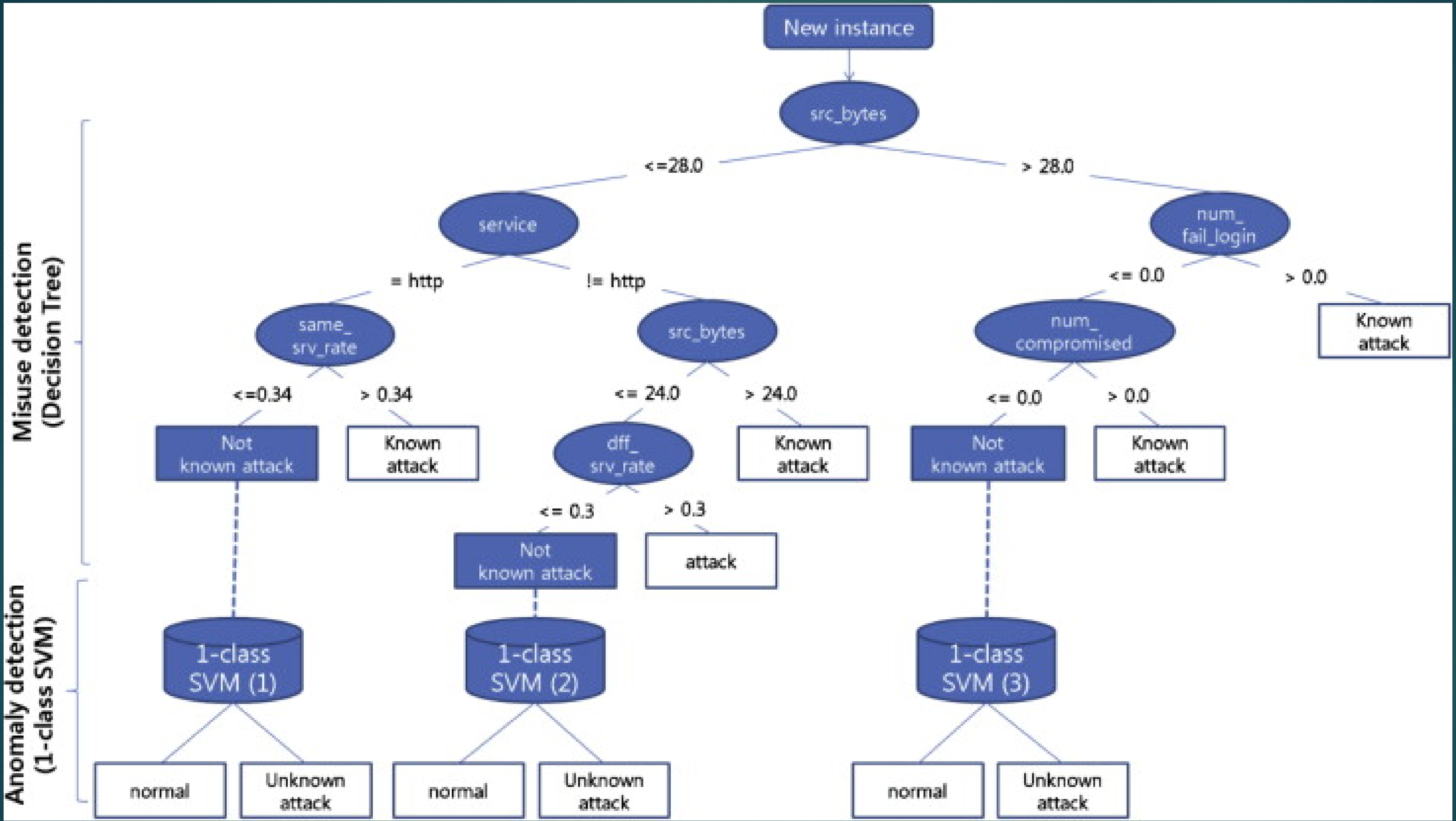


Diagram of decision making process of proposed method

Decision Tree and C4.5

- Locate attribute that best divides data into corresponding classes
- Recursively partitions data into subsets
- Creates tree-like structure
  - Node: attribute to best divide current subset
  - Edges: possible values/ranges of selected attribute
  - Leaves: terminating node – no further distinguishing attributes
- Decomposes data space into homogenous regions
- Prunes data to generalize tree

Decision Tree and C4.5

- C4.5 builds tree using information entropy
- Highest gain of each attribute

Decision Tree and C4.5

Gain of set S after split over attribute A

$$\mathrm{Gain}(S, A) = \mathrm{Entropy}(S) - \sum_{i=1}^{n} f_S(A_i) \times \mathrm{Entropy}(S_{A_i})$$

n – number of different values of attribute A in S

$f_S(j)$ – proportion of the value j in the set S

A_i – *i*th possible value of A

S_{A_i} – subset of S containing all items with value $A = A_i$

Decision Tree and C4.5

- Information Entropy of set S

$$\text{Entropy}(S) = -\sum_{j=1}^{m} f_S(j) \times \log_2 f_S(j)$$

$f_S(j)$ – proportion of the value j in the set S

m – number of different values of the attribute in S

One-class Support Vector Machine

- Feature map non-linearly transforms data to Feature Space
- Locates hyper-plane to detect outliers in Feature space

$$\min_{w,\xi,\rho} \quad \frac{1}{2}\|w\|^2 + \frac{1}{\nu l}\sum_{i=1}^{l}\xi_i - \rho$$

$$\text{subject to} \quad (w \cdot \Phi(x_i)) \geqslant \rho - \xi_i, \quad \xi_i \geqslant 0, \quad i = 1, \ldots, l$$

w	vector orthogonal to hyper plane
$\xi = [\xi_1, \ldots, \xi_l]$	vector of slack variables (penalizes rejected instances)
ρ	margin (distance from origin to hyper plane)
ν	fraction training instances that can be rejected

One-class Support Vector Machine

- Utilize kernel theory
  - Inner product in feature space can be computed using kernel function

$$k(x, y) = \Phi(x) \cdot \Phi(y)$$

  - Consider Gaussian kernel:

$$k(x, y) = e^{-\gamma \|x-y\|^2}$$

parameter γ affects decision boundary

- small γ = smooth boundary
- large γ = sensitive to training data

One-class Support Vector Machine

- Utilize kernel theory
  - Decision function for test instance z becomes:

$$f(z) = sgn \sum_{i=1}^{l} (\alpha_i k x_i (z - \rho))$$

    - Positive $f(z)$ indicates similar to training data set
    - Negative $f(z)$ indicates outlier

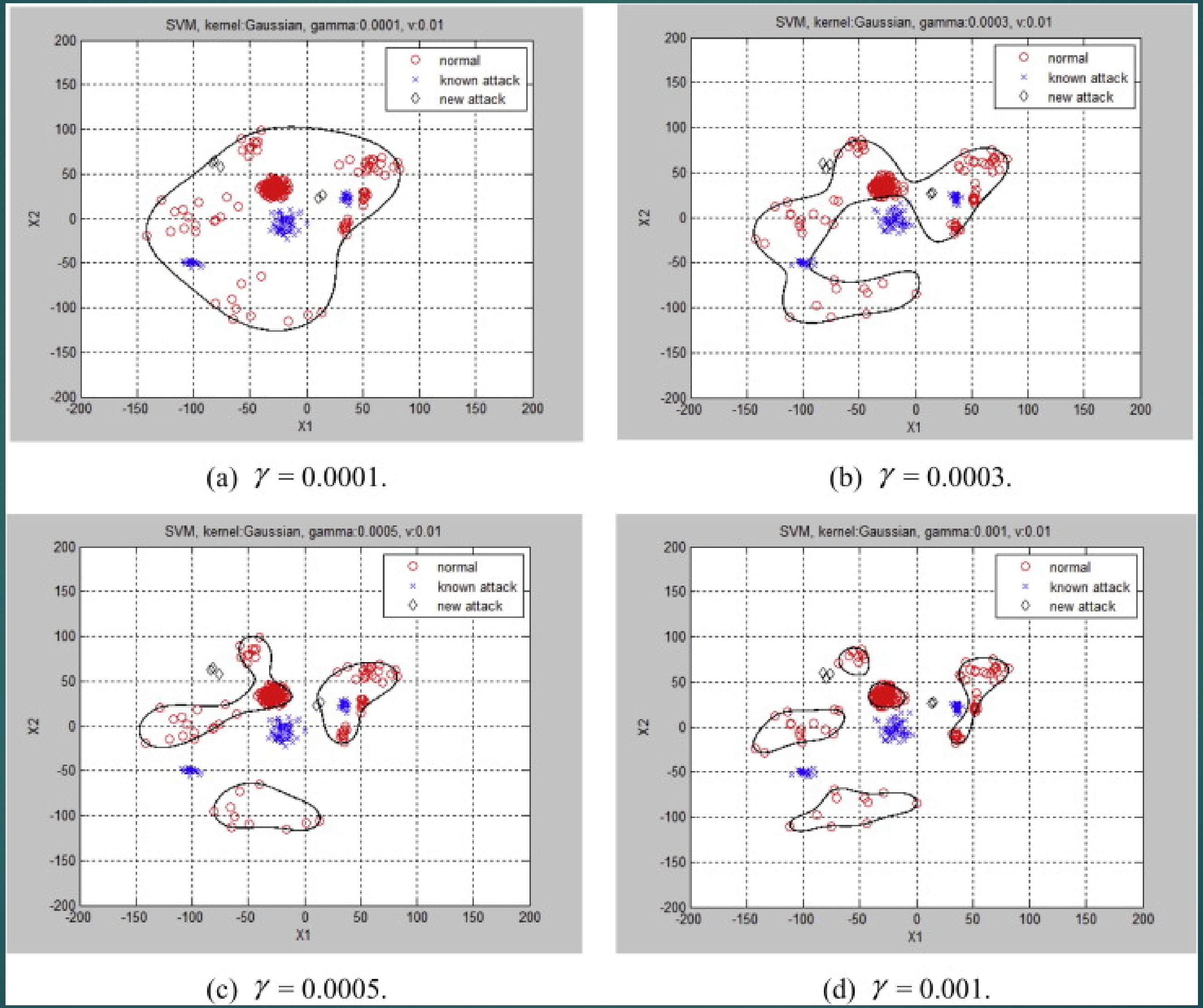
One-class Support Vector Machine

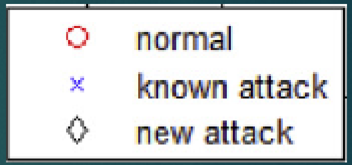
Important Parameters:

- ν - fraction training instances that can be rejected
  - High ν focuses on most frequent patterns
  - Low ν includes noisy data

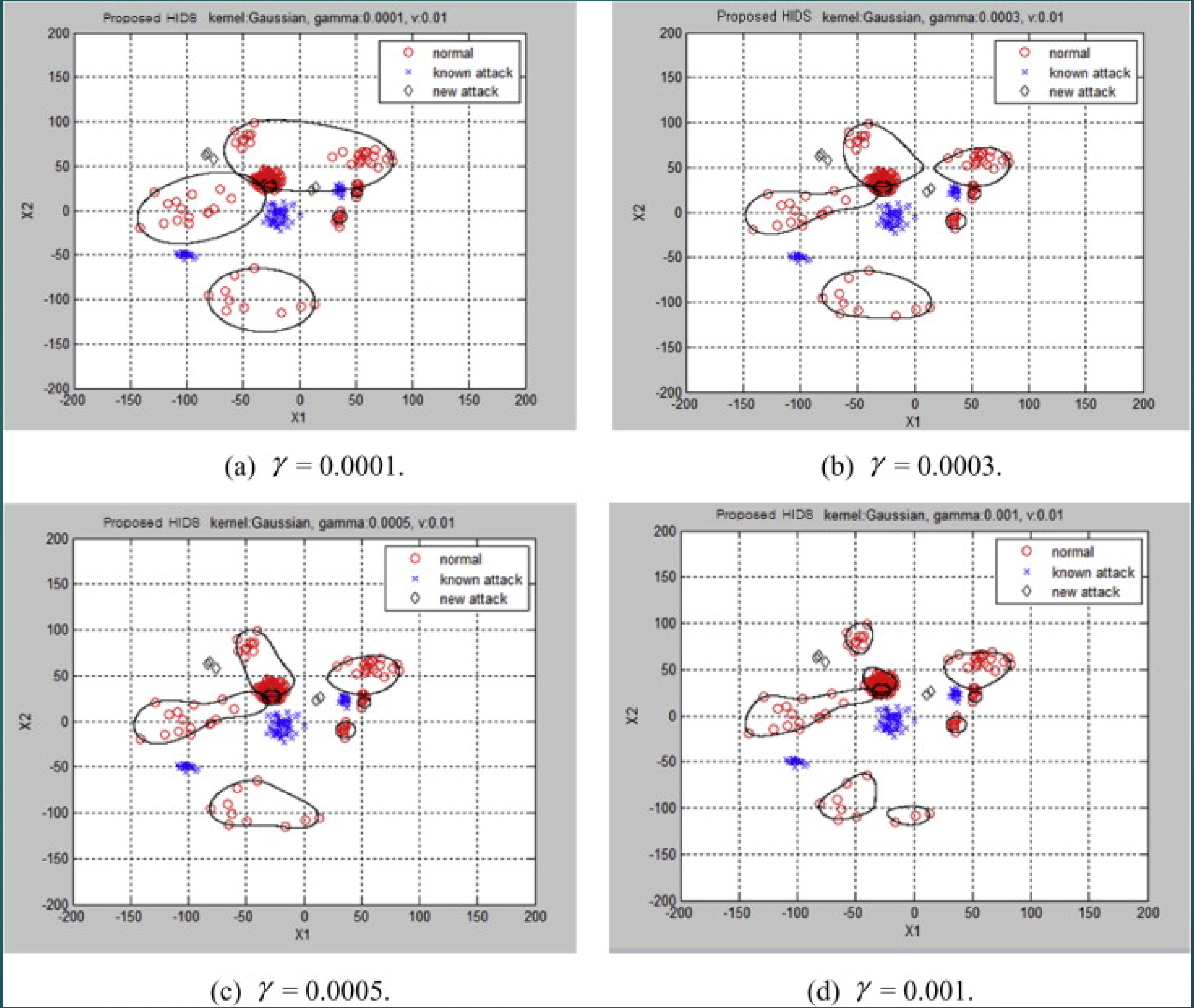
- γ - affects decision boundary
  - Low γ (0.0001) profiles normal data broadly
  - Higher γ (0.001) profiles normal data narrowly

Decision boundaries of the conventional 1-class SVM model

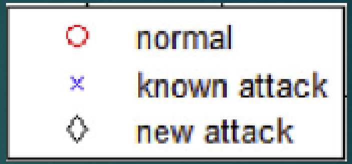




Decision boundaries of the proposed method



(a) $\gamma = 0.0001$. (b) $\gamma = 0.0003$. (c) $\gamma = 0.0005$. (d) $\gamma = 0.001$.



Experiments

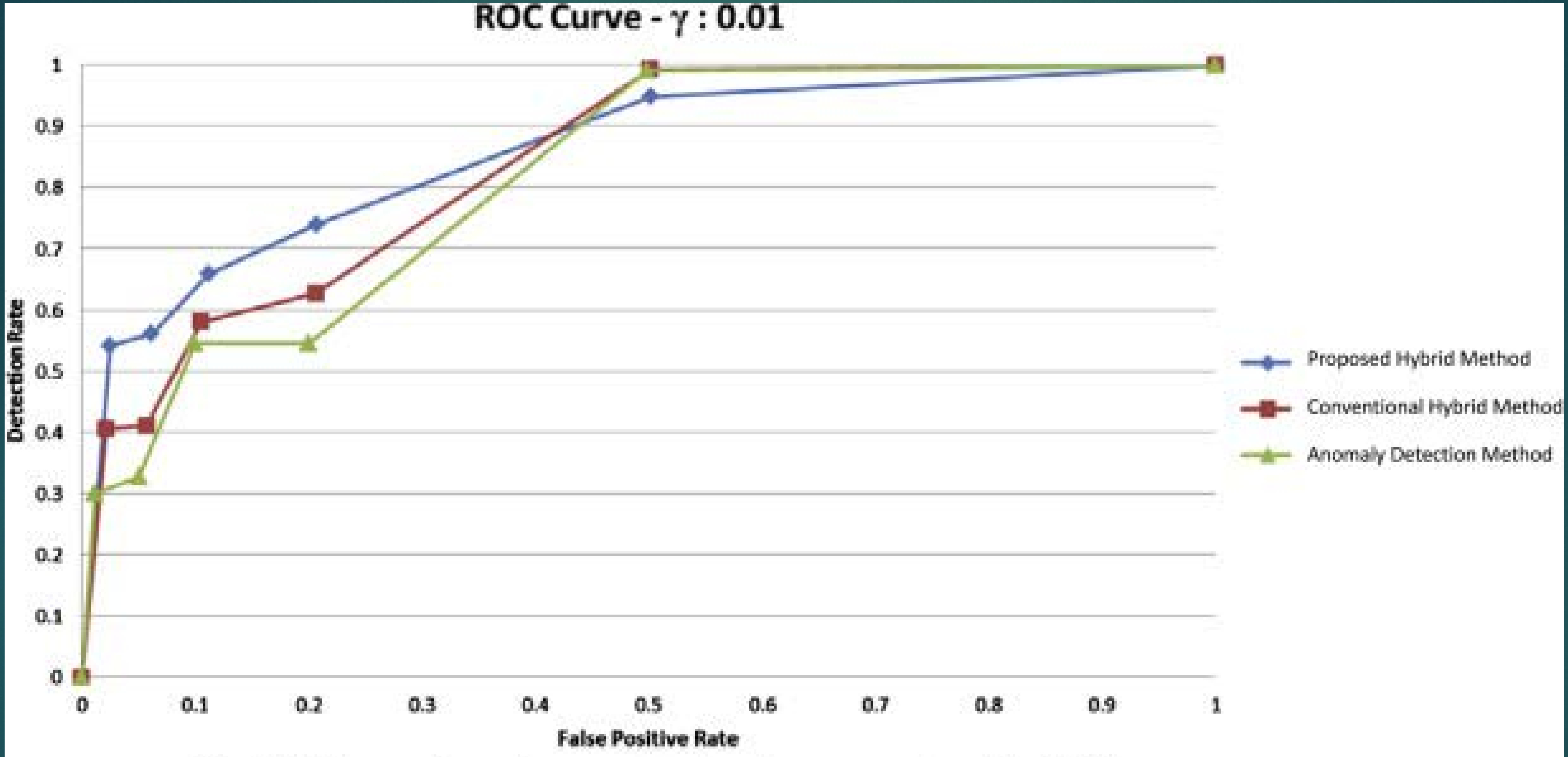
- Effectiveness evaluated with NSL-KDD data set
  - Modified version of KDD’99
  - Redundant instances removed
- Performance evaluated with Weka 3.6 and LibSVM (from MATLAB)

Experiments

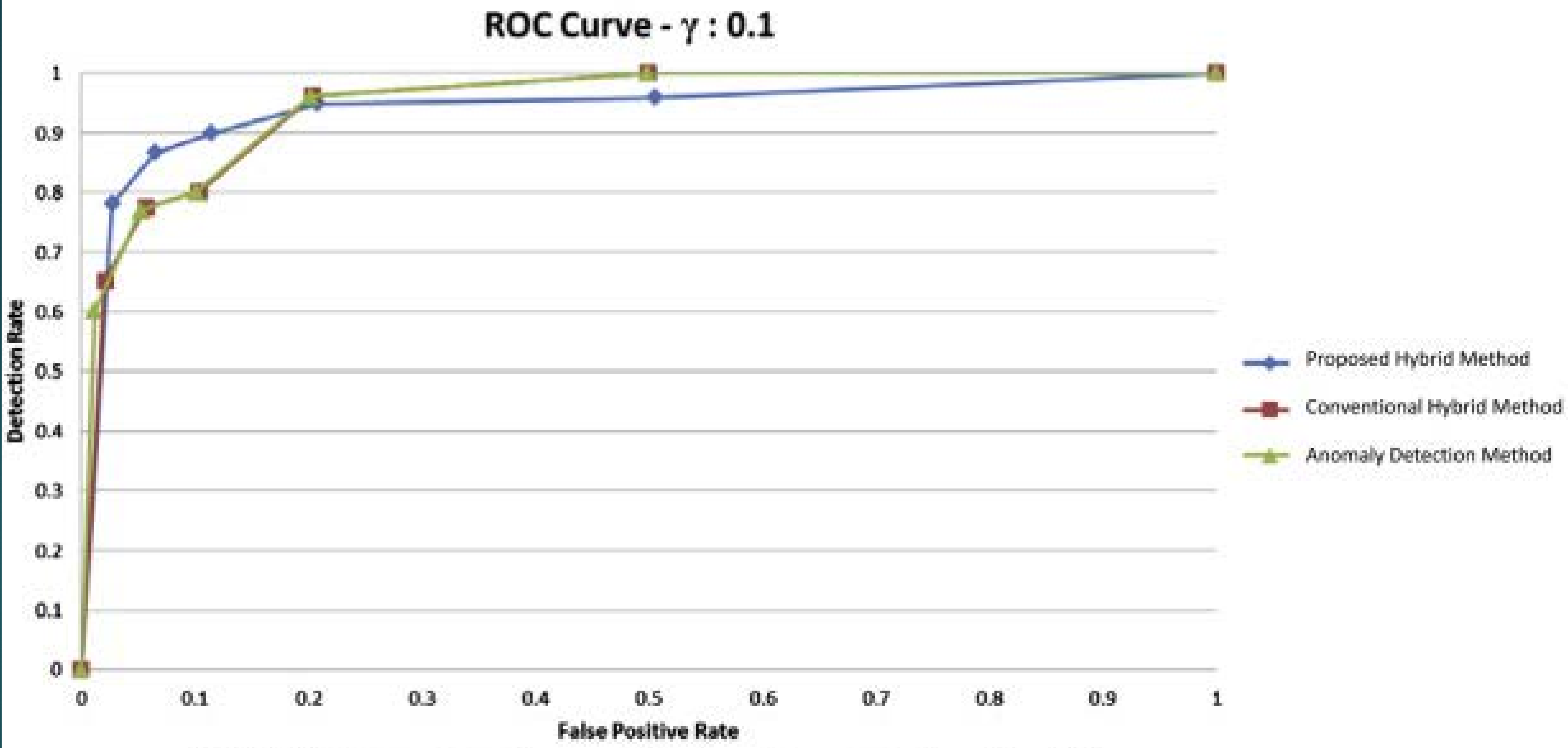
- NSL-KDD data set includes KDDTrain+.TXT and KDDTest+.TXT
- KDDTest+.TXT contains both “known” and “unknown” attacks
  - Problem: “Known” attack characteristics don’t always match same label in KDDTrain+.TXT
  - Solution: Split KDDText+ into “Known” and “Unknown” connections
  - Mix “Known” data set into KDDTrain+
  - Evenly split mixed data set into training and test sets
  - Add “Unknown” connections back into test set

Detection Performance

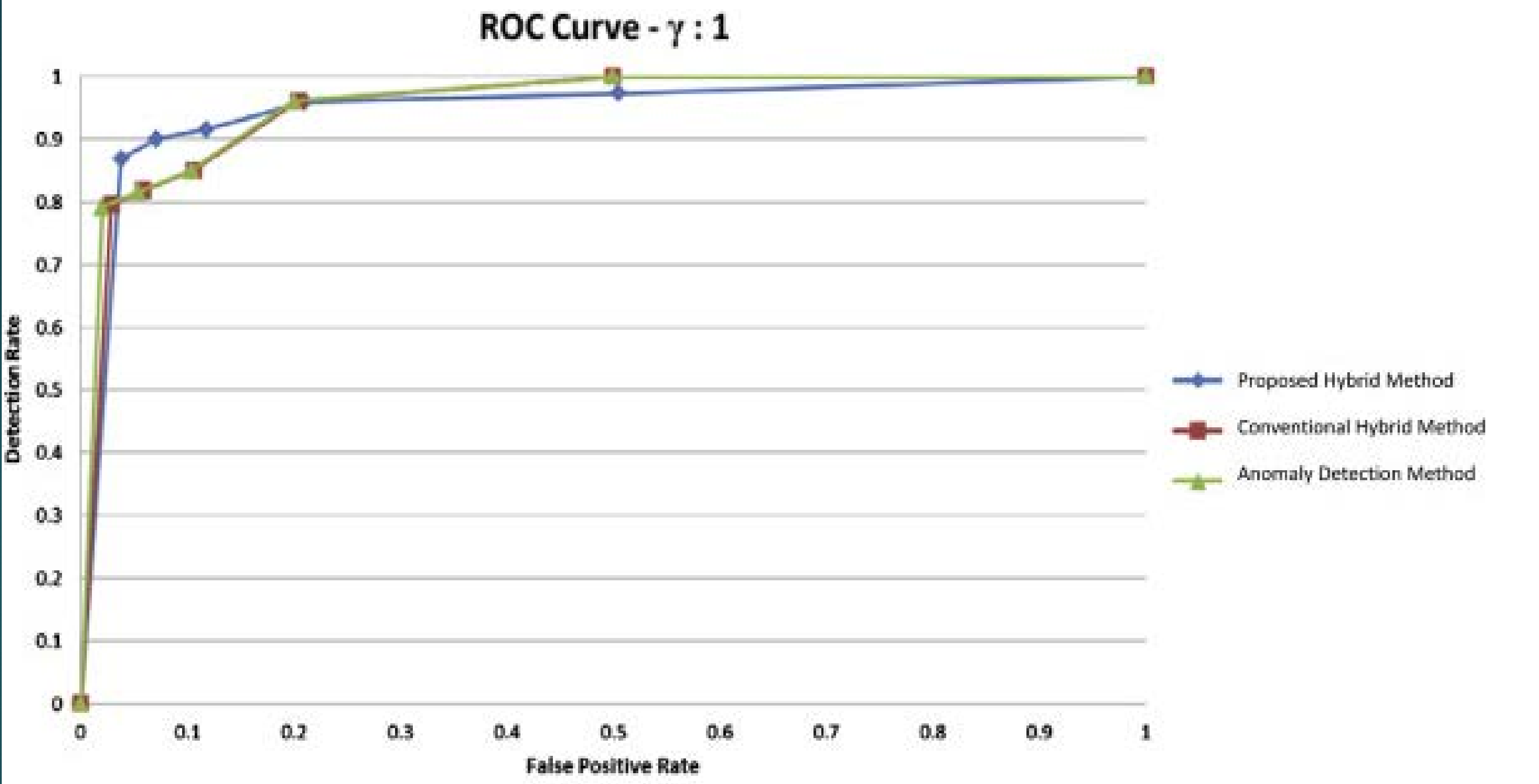
- Compare new hybrid method with:
  - Decision Tree misuse detection method
  - 1-class SVM anomaly detection method
  - Conventional Hybrid approach



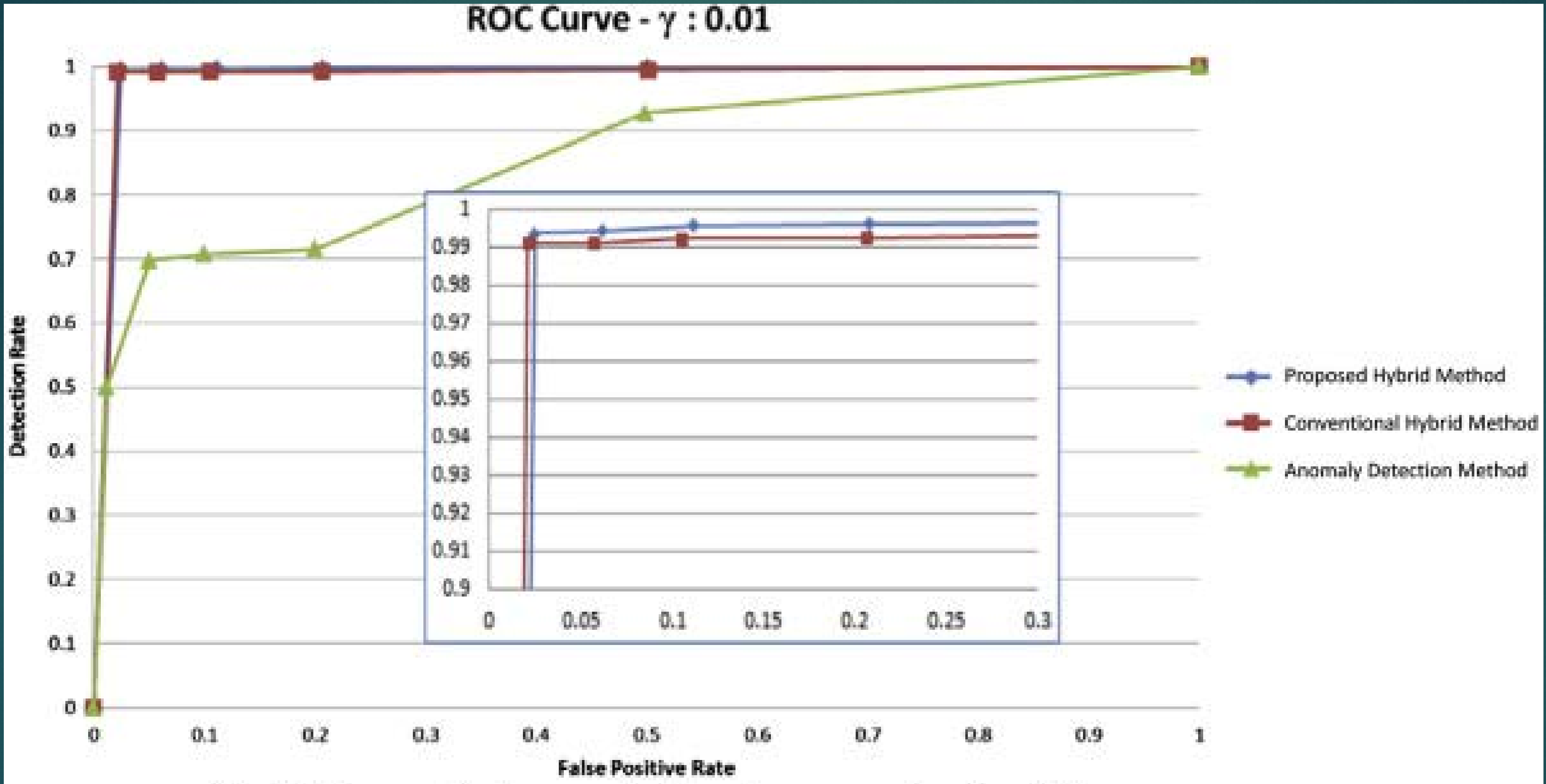
(a) ROC curve for unknown attacks when parameter $\gamma = 0.01$.



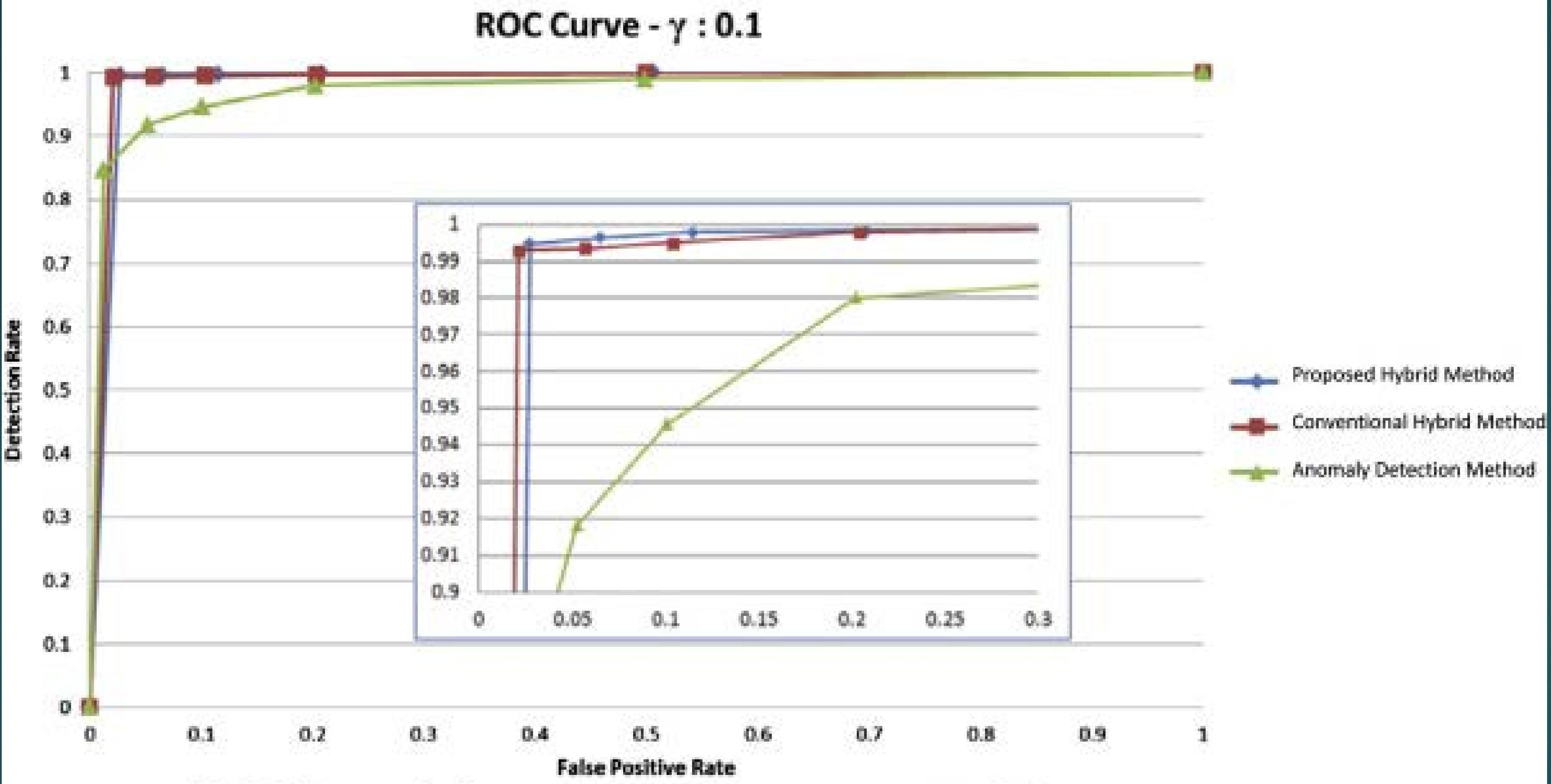
(b) ROC curve for unknown attacks when parameter $\gamma = 0.1$.



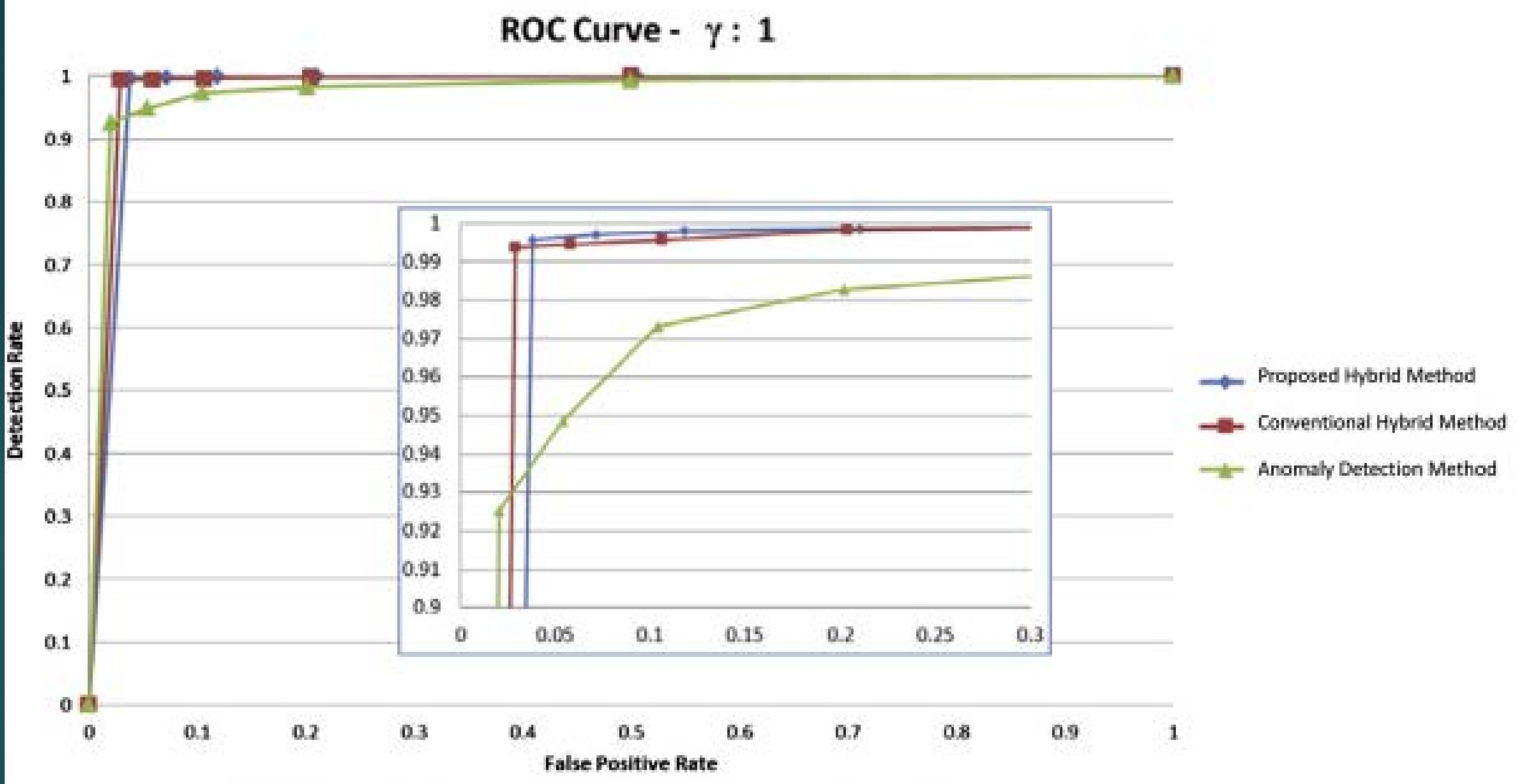
(c) ROC curve for unknown attacks when parameter $\gamma = 1$.



(a) ROC curve for known attacks when parameter $\gamma = 0.01$.



(b) ROC curve for known attacks when parameter $\gamma = 0.1$.



(c) ROC curve for known attacks when parameter $\gamma = 1$.

Any Questions?

A novel hybrid intrusion detection method integrating anomaly detection with misuse detection

Gisung Kim, Sehun Kim

Institute for IT Convergence, KAIST, Guseong-dong, Yuseong-gu, Daejeon 305-701, South Korea

Seungmin Lee

Future Research Creative Laboratory, ETRI 218 Gajeong-ro, Yuseong-gu, Daejeon 305-700, South Korea