SVM-DT-Based Adaptive and Collaborative Intrusion Detection

Abstract

- As a primary defense technique, intrusion detection becomes more and more significant since the security of the networks is one of the most critical issues in the world.
- We present an adaptive collaboration intrusion detection method to

  improve the safety of a network. A self-adaptive and collaborative intrusion detection model is built by applying the Environments classes, agents, roles, groups, and objects (E-CARGO) model.

  The objects, roles, agents, and groups are designed by using decision trees (DTs) and support vector machines (SVMs), and adaptive scheduling mechanisms are set up.

- The KDD CUP 1999 data set is used to verify the effectiveness of the method. The experimental results demonstrate the feasibility and efficiency of the proposed collaborative and adaptive intrusion detection method.
- Also, the proposed method is shown to be more predominant than the methods that use a set of single type support vector machine (SVM) in terms of detection precision rate and recall rate.

Introduction

- detection is an important means to guarantee the safety of a network to avoid illegal operations that are launched by intruders (such as attackers and hackers) via authentication identification [1].
- An intrusion detection system (IDS) is the most significant tool to ensure the security of a network by analyzing the audit data and current state. There are many measures to protect a network system, however, most of the conventional methods are inefficient.
- Since some attacks are composed of a series of users' operations, the users' behavior should be analyzed to detect an intrusion.

Existing system

- Since some attacks are composed of a series of users' operations, the users' behavior should be analyzed to detect an intrusion.
- users' actions are divided into normal and abnormal ones to separate the data. Then, classification is used to justify the detection result.
- As a primary defense technique, intrusion detection

  becomes more and more significant since the security of the networks is one of the most critical issues in the world.

Hardware requirement

Processor	-	Pentium –III
Speed	-	1.1 Ghz
RAM	-	256 MB(min)
Hard Disk	-	20 GB
Floppy Drive	-	1.44 MB
Key Board	-	Standard Windows Keyboard
Mouse	-	Two or Three Button Mouse
Monitor	-	SVGA

-

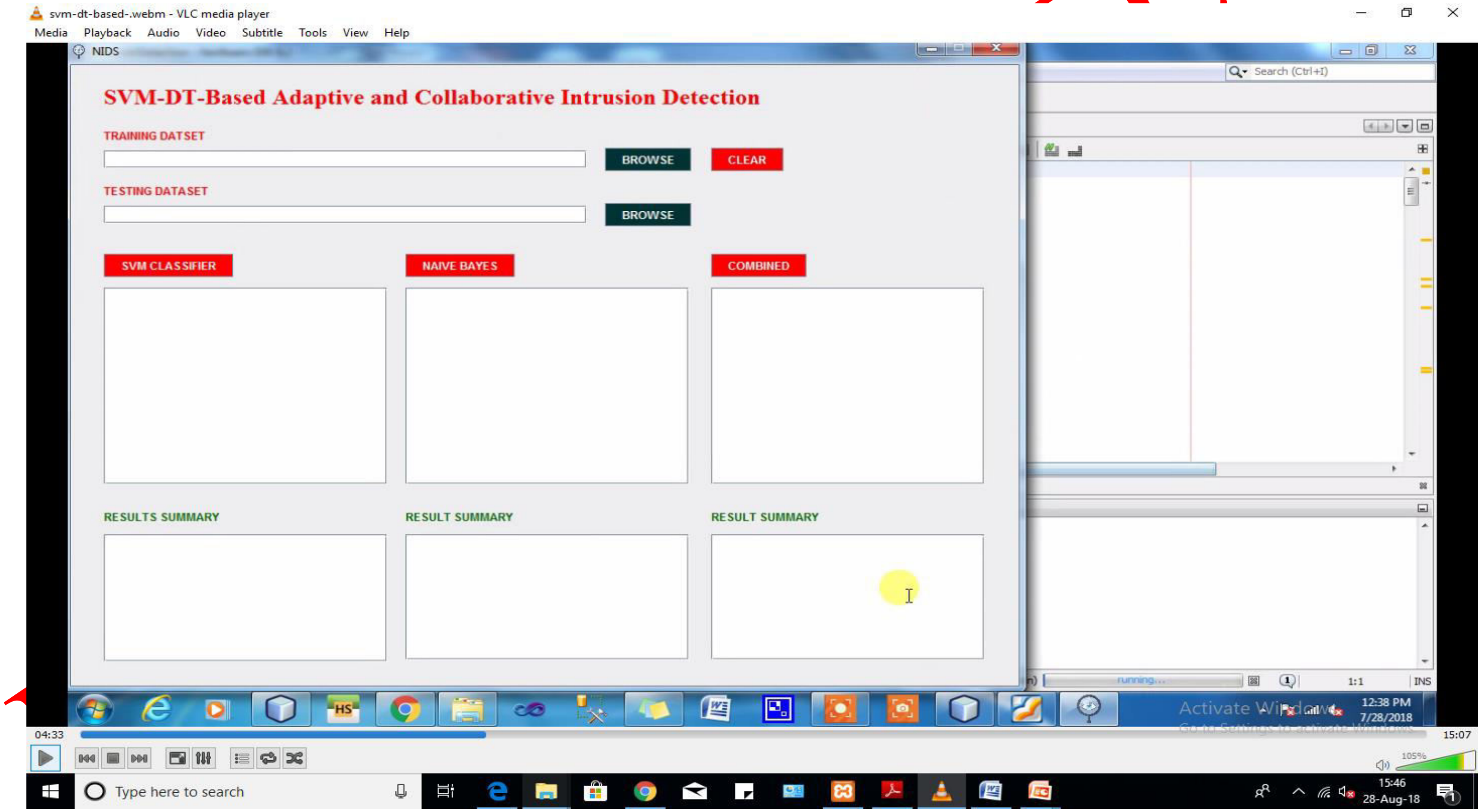
Software requirement

Operating System	Windows 7/8
Application Server	Tomcat 5.0
Front End	JAVA
IDE	NETBEANS 7.1
Back-End	HEIDISQL 3.5

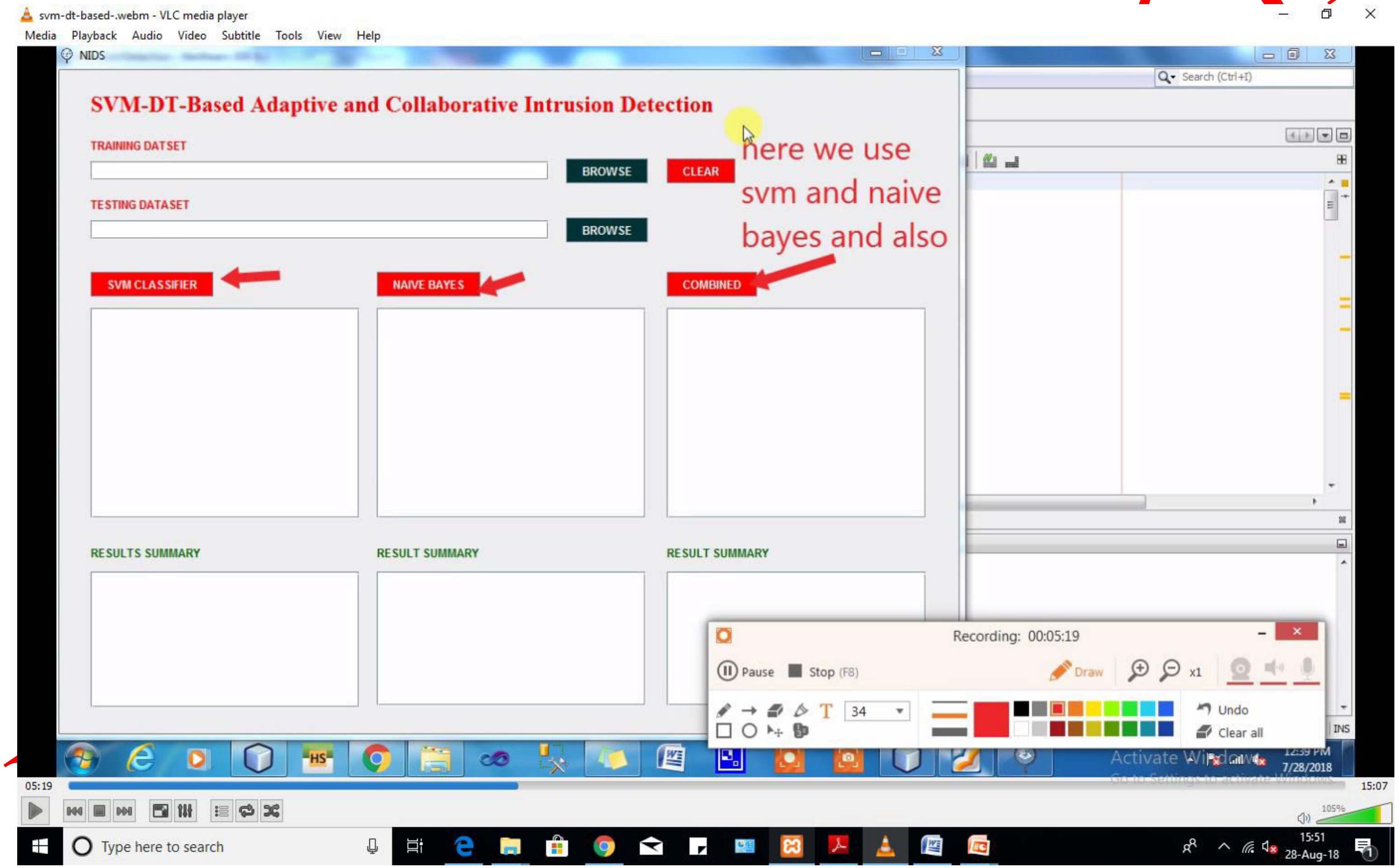
Proposed system

- The experimental results demonstrate the feasibility and efficiency of the proposed collaborative and adaptive intrusion detection method.
- Also, the proposed method is shown to be more predominant than the methods that use a set of single type support vector machine (SVM) in terms of detection precision rate and recall rate. In this paper, a collaborative and adaptive intrusion detection method based on 2-class SVMs and DTs is proposed.
- A detection model called CAIDM is created and implemented.The E-CARGO model is used as a tool for describing the intrusion detection and modeling. In this paper, roles, groups, and agents are all studied and applied, for instance, the response unit role, the suspicious event detection role, the generating suspicious event role, etc..

Screen short



SVM-DT Based adaptive and collaborative Detection

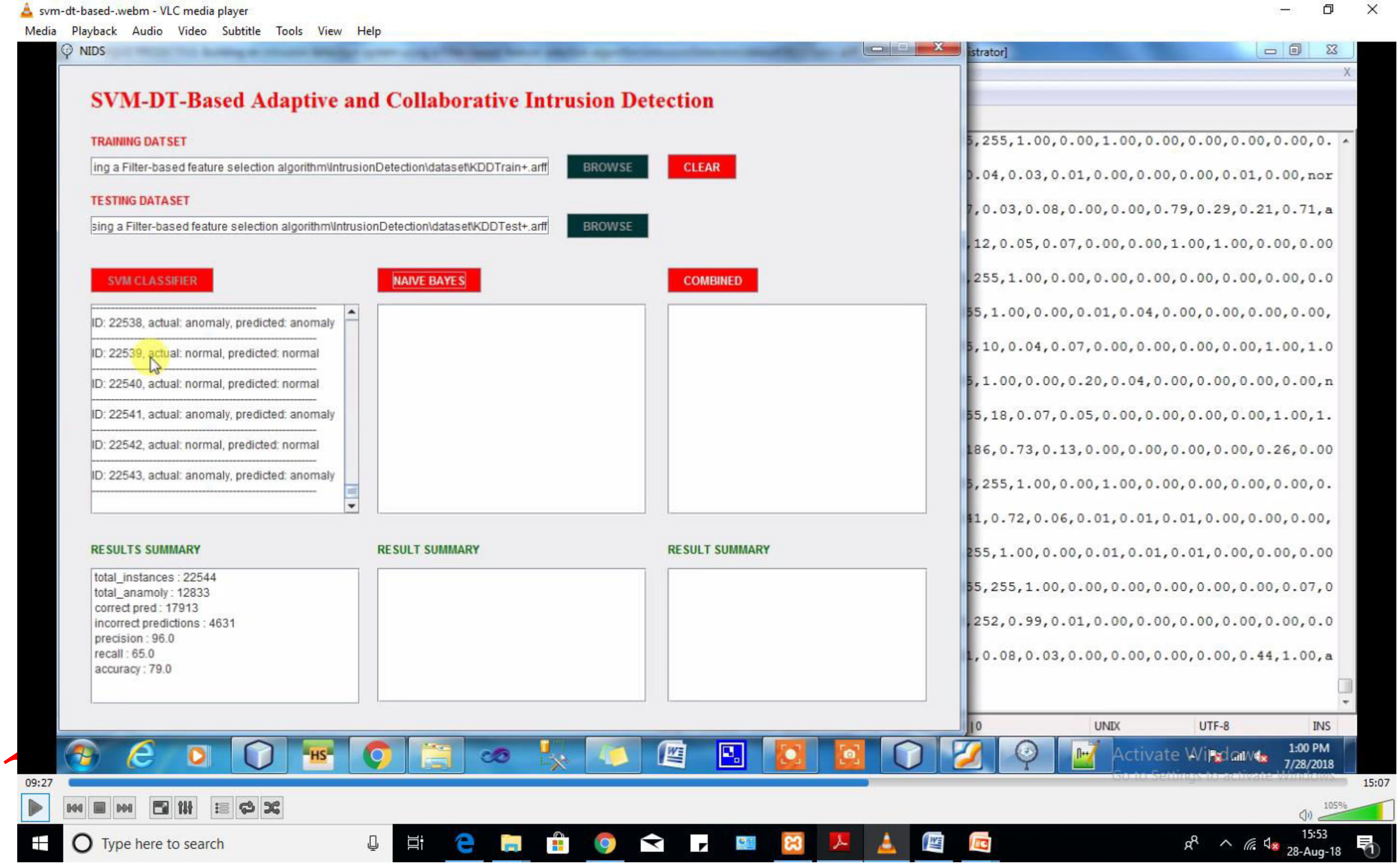


svm-dt-based-.webm - VLC media player

SVM-DT-Based Adaptive and Collaborative Intrusion Detection

here we use svm and naive bayes and also

Step1
svm classifier



SVM-DT-Based Adaptive and Collaborative Intrusion Detection

TRAINING DATSET

ing a Filter-based feature selection algorithm\IntrusionDetection\dataset\KDDTrain+.arff

TESTING DATASET

sing a Filter-based feature selection algorithm\IntrusionDetection\dataset\KDDTest+.arff

```
ID: 22538, actual: anomaly, predicted: anomaly
ID: 22539, actual: normal, predicted: normal
ID: 22540, actual: normal, predicted: normal
ID: 22541, actual: anomaly, predicted: anomaly
ID: 22542, actual: normal, predicted: normal
ID: 22543, actual: anomaly, predicted: anomaly
```

RESULTS SUMMARY

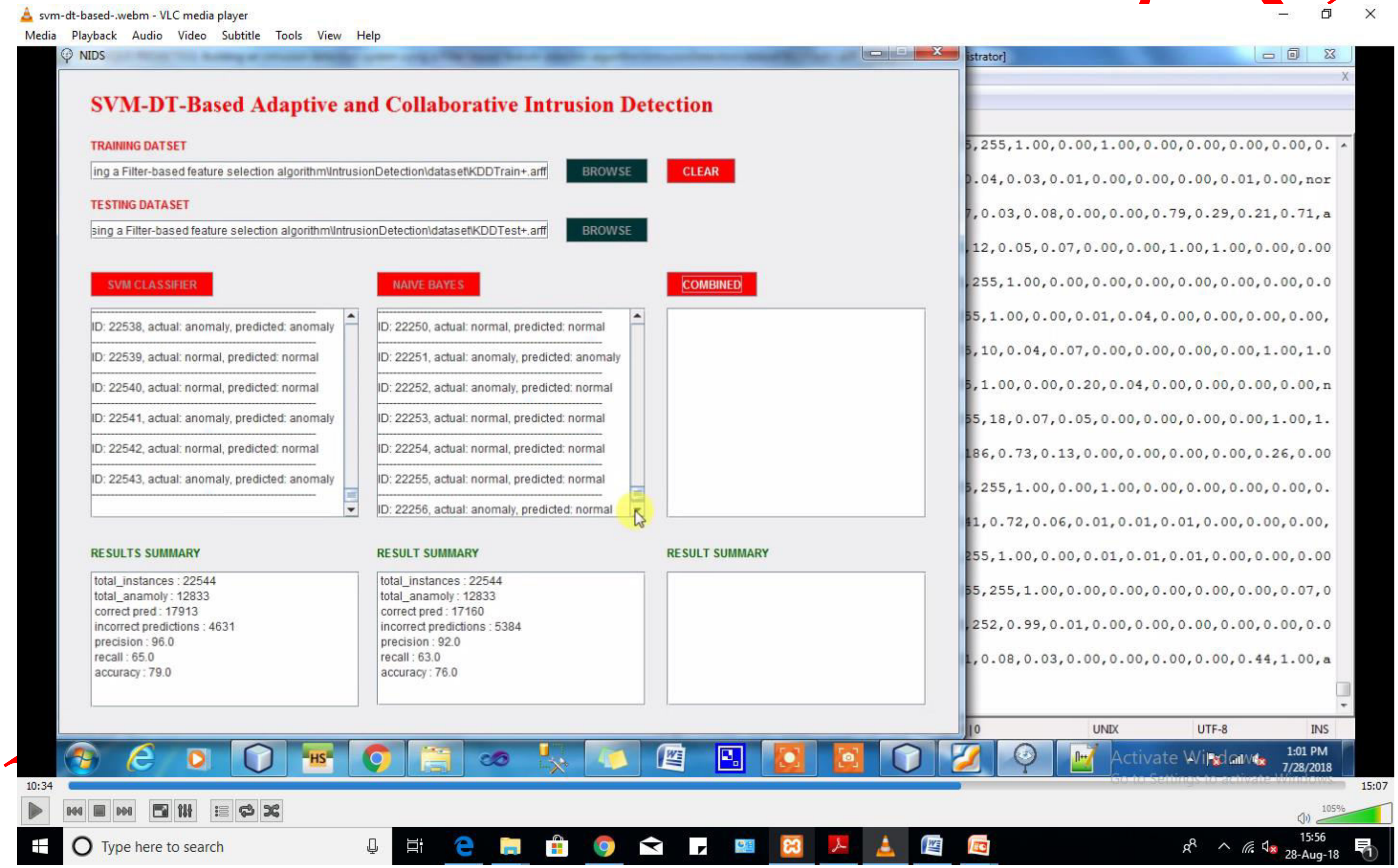
```
total_instances : 22544
total_anamoly : 12833
correct pred : 17913
incorrect predictions : 4631
precision : 96.0
recall : 65.0
accuracy : 79.0
```

RESULT SUMMARY

RESULT SUMMARY

```
5,255,1.00,0.00,1.00,0.00,0.00,0.00,0.00,0.
0.04,0.03,0.01,0.00,0.00,0.00,0.01,0.00,nor
7,0.03,0.08,0.00,0.00,0.79,0.29,0.21,0.71,a
,12,0.05,0.07,0.00,0.00,1.00,1.00,0.00,0.00
,255,1.00,0.00,0.00,0.00,0.00,0.00,0.00,0.0
55,1.00,0.00,0.01,0.04,0.00,0.00,0.00,0.00,
5,10,0.04,0.07,0.00,0.00,0.00,0.00,1.00,1.0
5,1.00,0.00,0.20,0.04,0.00,0.00,0.00,0.00,n
55,18,0.07,0.05,0.00,0.00,0.00,0.00,1.00,1.
186,0.73,0.13,0.00,0.00,0.00,0.00,0.26,0.00
5,255,1.00,0.00,1.00,0.00,0.00,0.00,0.00,0.
41,0.72,0.06,0.01,0.01,0.01,0.00,0.00,0.00,
255,1.00,0.00,0.01,0.01,0.01,0.00,0.00,0.00
55,255,1.00,0.00,0.00,0.00,0.00,0.00,0.07,0
,252,0.99,0.01,0.00,0.00,0.00,0.00,0.00,0.0
1,0.08,0.03,0.00,0.00,0.00,0.00,0.44,1.00,a
```

Step 2
Naïve bayer



SVM-DT-Based Adaptive and Collaborative Intrusion Detection

TRAINING DATSET

ing a Filter-based feature selection algorithm\IntrusionDetection\dataset\KDDTrain+.arff

TESTING DATASET

sing a Filter-based feature selection algorithm\IntrusionDetection\dataset\KDDTest+.arff

SVM CLASSIFIER

```
ID: 22538, actual: anomaly, predicted: anomaly
ID: 22539, actual: normal, predicted: normal
ID: 22540, actual: normal, predicted: normal
ID: 22541, actual: anomaly, predicted: anomaly
ID: 22542, actual: normal, predicted: normal
ID: 22543, actual: anomaly, predicted: anomaly
```

NAIVE BAYES

```
ID: 22250, actual: normal, predicted: normal
ID: 22251, actual: anomaly, predicted: anomaly
ID: 22252, actual: anomaly, predicted: normal
ID: 22253, actual: normal, predicted: normal
ID: 22254, actual: normal, predicted: normal
ID: 22255, actual: normal, predicted: normal
ID: 22256, actual: anomaly, predicted: normal
```

RESULTS SUMMARY

```
total_instances : 22544
total_anamoly : 12833
correct pred : 17913
incorrect predictions : 4631
precision : 96.0
recall : 65.0
accuracy : 79.0
```

RESULT SUMMARY

```
total_instances : 22544
total_anamoly : 12833
correct pred : 17160
incorrect predictions : 5384
precision : 92.0
recall : 63.0
accuracy : 76.0
```

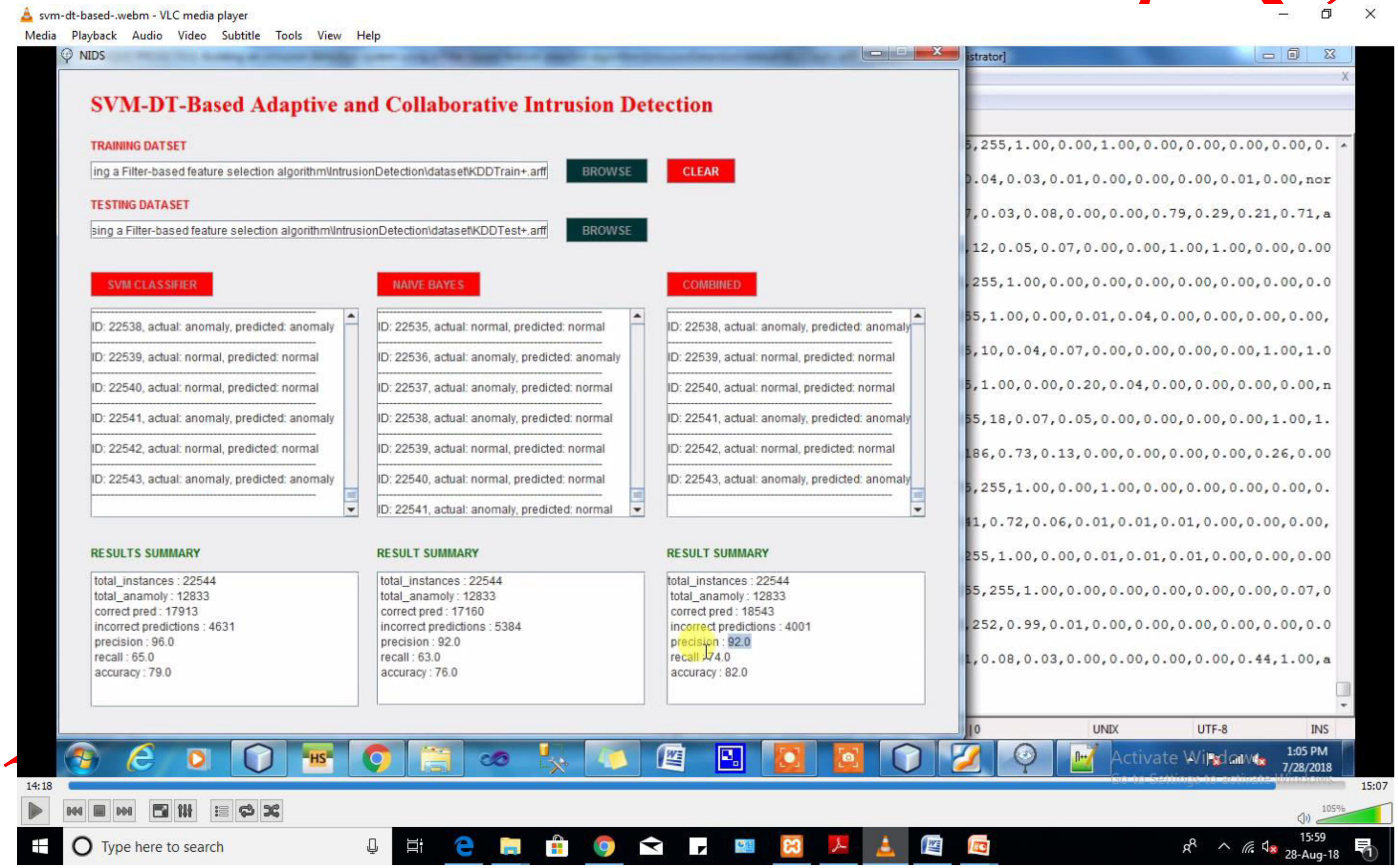
RESULT SUMMARY

istrator]

```
5,255,1.00,0.00,1.00,0.00,0.00,0.00,0.00,0.
0.04,0.03,0.01,0.00,0.00,0.00,0.01,0.00,nor
7,0.03,0.08,0.00,0.00,0.79,0.29,0.21,0.71,a
,12,0.05,0.07,0.00,0.00,1.00,1.00,0.00,0.00
,255,1.00,0.00,0.00,0.00,0.00,0.00,0.00,0.0
55,1.00,0.00,0.01,0.04,0.00,0.00,0.00,0.00,
5,10,0.04,0.07,0.00,0.00,0.00,0.00,1.00,1.0
5,1.00,0.00,0.20,0.04,0.00,0.00,0.00,0.00,n
55,18,0.07,0.05,0.00,0.00,0.00,0.00,1.00,1.
186,0.73,0.13,0.00,0.00,0.00,0.00,0.26,0.00
5,255,1.00,0.00,1.00,0.00,0.00,0.00,0.00,0.
41,0.72,0.06,0.01,0.01,0.01,0.00,0.00,0.00,
255,1.00,0.00,0.01,0.01,0.01,0.00,0.00,0.00
55,255,1.00,0.00,0.00,0.00,0.00,0.00,0.07,0
,252,0.99,0.01,0.00,0.00,0.00,0.00,0.00,0.0
1,0.08,0.03,0.00,0.00,0.00,0.00,0.44,1.00,a
```

|0 UNIX UTF-8 INS

COMINED


svm-dt-based-.webm - VLC media player
Media Playback Audio Video Subtitle Tools View Help
NIDS
istrator]
14:18
15:07
Type here to search
Activate Windows
1:05 PM
7/28/2018
15:59
28-Aug-18

SVM-DT-Based Adaptive and Collaborative Intrusion Detection

TRAINING DATSET

ing a Filter-based feature selection algorithm\IntrusionDetection\dataset\KDDTrain+.arff

TESTING DATASET

sing a Filter-based feature selection algorithm\IntrusionDetection\dataset\KDDTest+.arff

```
ID: 22538, actual: anomaly, predicted: anomaly
ID: 22539, actual: normal, predicted: normal
ID: 22540, actual: normal, predicted: normal
ID: 22541, actual: anomaly, predicted: anomaly
ID: 22542, actual: normal, predicted: normal
ID: 22543, actual: anomaly, predicted: anomaly
```

RESULTS SUMMARY

```
total_instances : 22544
total_anamoly : 12833
correct pred : 17913
incorrect predictions : 4631
precision : 96.0
recall : 65.0
accuracy : 79.0
```

```
ID: 22535, actual: normal, predicted: normal
ID: 22536, actual: anomaly, predicted: anomaly
ID: 22537, actual: anomaly, predicted: normal
ID: 22538, actual: anomaly, predicted: normal
ID: 22539, actual: normal, predicted: normal
ID: 22540, actual: normal, predicted: normal
ID: 22541, actual: anomaly, predicted: normal
```

RESULT SUMMARY

```
total_instances : 22544
total_anamoly : 12833
correct pred : 17160
incorrect predictions : 5384
precision : 92.0
recall : 63.0
accuracy : 76.0
```

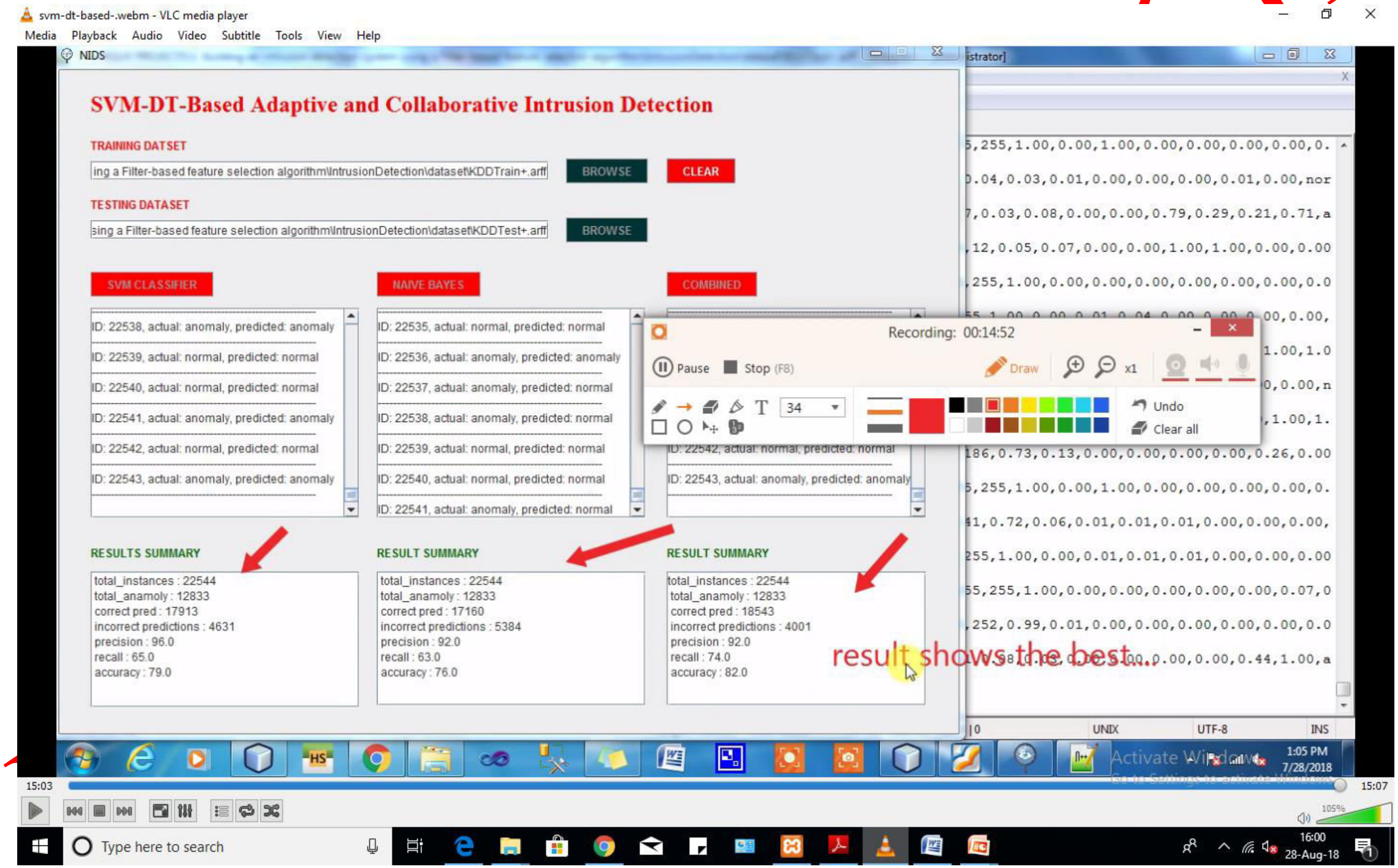
```
ID: 22538, actual: anomaly, predicted: anomaly
ID: 22539, actual: normal, predicted: normal
ID: 22540, actual: normal, predicted: normal
ID: 22541, actual: anomaly, predicted: anomaly
ID: 22542, actual: normal, predicted: normal
ID: 22543, actual: anomaly, predicted: anomaly
```

RESULT SUMMARY

```
total_instances : 22544
total_anamoly : 12833
correct pred : 18543
incorrect predictions : 4001
precision : 92.0
recall : 74.0
accuracy : 82.0
```

```
5,255,1.00,0.00,1.00,0.00,0.00,0.00,0.00,0.
0.04,0.03,0.01,0.00,0.00,0.00,0.01,0.00,nor
7,0.03,0.08,0.00,0.00,0.79,0.29,0.21,0.71,a
,12,0.05,0.07,0.00,0.00,1.00,1.00,0.00,0.00
,255,1.00,0.00,0.00,0.00,0.00,0.00,0.00,0.0
55,1.00,0.00,0.01,0.04,0.00,0.00,0.00,0.00,
5,10,0.04,0.07,0.00,0.00,0.00,0.00,1.00,1.0
5,1.00,0.00,0.20,0.04,0.00,0.00,0.00,0.00,n
55,18,0.07,0.05,0.00,0.00,0.00,0.00,1.00,1.
186,0.73,0.13,0.00,0.00,0.00,0.00,0.26,0.00
5,255,1.00,0.00,1.00,0.00,0.00,0.00,0.00,0.
41,0.72,0.06,0.01,0.01,0.01,0.00,0.00,0.00,
255,1.00,0.00,0.01,0.01,0.01,0.00,0.00,0.00
55,255,1.00,0.00,0.00,0.00,0.00,0.00,0.07,0
,252,0.99,0.01,0.00,0.00,0.00,0.00,0.00,0.0
1,0.08,0.03,0.00,0.00,0.00,0.00,0.44,1.00,a
```

RESULT SHOW



SVM-DT-Based Adaptive and Collaborative Intrusion Detection

TRAINING DATSET

ing a Filter-based feature selection algorithm\IntrusionDetection\dataset\KDDTrain+.arff

TESTING DATASET

sing a Filter-based feature selection algorithm\IntrusionDetection\dataset\KDDTest+.arff

```
ID: 22538, actual: anomaly, predicted: anomaly
ID: 22539, actual: normal, predicted: normal
ID: 22540, actual: normal, predicted: normal
ID: 22541, actual: anomaly, predicted: anomaly
ID: 22542, actual: normal, predicted: normal
ID: 22543, actual: anomaly, predicted: anomaly
```

```
ID: 22535, actual: normal, predicted: normal
ID: 22536, actual: anomaly, predicted: anomaly
ID: 22537, actual: anomaly, predicted: normal
ID: 22538, actual: anomaly, predicted: normal
ID: 22539, actual: normal, predicted: normal
ID: 22540, actual: normal, predicted: normal
ID: 22541, actual: anomaly, predicted: normal
```

```
ID: 22542, actual: normal, predicted: normal
ID: 22543, actual: anomaly, predicted: anomaly
```

RESULTS SUMMARY

```
total_instances : 22544
total_anamoly : 12833
correct pred : 17913
incorrect predictions : 4631
precision : 96.0
recall : 65.0
accuracy : 79.0
```

RESULT SUMMARY

```
total_instances : 22544
total_anamoly : 12833
correct pred : 17160
incorrect predictions : 5384
precision : 92.0
recall : 63.0
accuracy : 76.0
```

RESULT SUMMARY

```
total_instances : 22544
total_anamoly : 12833
correct pred : 18543
incorrect predictions : 4001
precision : 92.0
recall : 74.0
accuracy : 82.0
```

result shows the best...

```
5,255,1.00,0.00,1.00,0.00,0.00,0.00,0.00,0.
.04,0.03,0.01,0.00,0.00,0.00,0.01,0.00,nor
7,0.03,0.08,0.00,0.00,0.79,0.29,0.21,0.71,a
,12,0.05,0.07,0.00,0.00,1.00,1.00,0.00,0.00
,255,1.00,0.00,0.00,0.00,0.00,0.00,0.00,0.0
00,0.00,
1.00,1.0
0,0.00,n
,1.00,1.
186,0.73,0.13,0.00,0.00,0.00,0.00,0.26,0.00
5,255,1.00,0.00,1.00,0.00,0.00,0.00,0.00,0.
41,0.72,0.06,0.01,0.01,0.01,0.00,0.00,0.00,
255,1.00,0.00,0.01,0.01,0.01,0.00,0.00,0.00
55,255,1.00,0.00,0.00,0.00,0.00,0.00,0.07,0
,252,0.99,0.01,0.00,0.00,0.00,0.00,0.00,0.0
0.00,0.00,0.44,1.00,a
```

Conclusion

- In this paper, a collaborative and adaptive intrusion detection method based on 2-class SVMs and DTs is proposed. A detection model called CAIDM is created and implemented.
- The E-CARGO model is used as a tool for describing the
- intrusion detection and modeling. In this paper, roles, groups, and agents are all studied and applied, for instance, the response unit role, the suspicious event detection role, the generating suspicious event role, etc. A role is assigned to some agents. A group (SmallGroup) contains many agents that perform the same role. TCP/IP protocols can be decomposed into four categories: TCP, UDP, ICMP, and application layer protocols. These protocols include different attributes

Reference

- [1] S. H. Teng, N. Q. Wu, W. Zhang, and X. F. Fu, "Cooperative intrusion detection based on object monitoring," *Acta Sci. Nat. Univ. Suny.*, vol. 47, no. 6, pp. 76¡81, Nov. 2008.

- [2] E. Alpaydin, *Introduction to Machine Learning*. 3rd ed. New York, NY, USA: The MIT Press, 2014.

- [3] S. H. Teng, H. L. Du, N. Q. Wu, W. Zhang, and J. Y. Su, "A cooperative network intrusion detection based on fuzzy SVMs," *J. Netw.*, vol. 5 no. 4, pp. 475¡483, Jan. 2010.