

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.

NCI

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

J.P.

- Processor
- Speed
- RAM
- Hard Disk
- Floppy Drive
- Key Board
- Mouse

.

• Monitor

- Pentium –III
- 1.1 Ghz
- 256 MB(min)
- 20 GB
- 1.44 MB

SVGA

- Standard Windows Keyboard
 - Two or Three Button Mouse

Software requirement

- Operating System
- Application Server

()

- Front End
- IDE
- Back-End

- Windows 7/8
- Tomcat 5.0
- JAVA
- NETBEANS 7.1HEIDISOL 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 CAHDM 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-.webm - VLC media player



Media Playback Audio Video Subtitle Tools View Help I NIDS - 0 23 Q - Search (Ctrl+I) **SVM-DT-Based Adaptive and Collaborative Intrusion Detection** TRAINING DATSET <u>____</u> BB BROWSE . ш TESTING DATASET BROWSE COMBINED RESULT SUMMARY RESULT SUMMARY RESULTS SUMMARY T INS 1:1 ۵. 12:38 PM HS e 0 0 Activate Windows 7/28/2018 15:07 144 E 144 E (\$ XC o < 🔽 🔤 Ļ × 201 Type here to search 83 8ª ~ (1

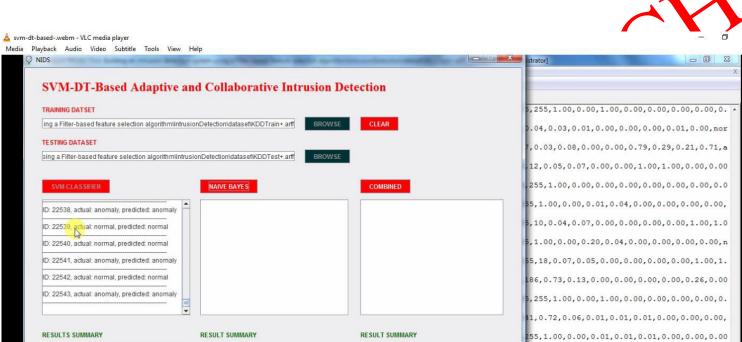
SVM-DT Based adaptive and collaborative Detection



SVM-DT-Based Adaptiv	e and Collaborative Intru	sion Detection		Q Search (Ctrl+I)
TRAINING DATSET		here we use		4.8.0
		BROWSE CLEAR SVM and naive		
TESTING DATASET				
		BROWSE bayes and also		
SVM CLASSIFIER	NAIVE BAYES	COMBINED		
				,
RESULTS SUMMARY	RESULT SUMMARY	RESULT SUMMARY		
RESULTS SUMMARY	RESULT SUMMARY	RESULT SUMMARY		
RESULTS SUMMARY	RESULT SUMMARY		Recording: 00:05:19	- *
RESULTS SUMMARY	RESULT SUMMARY			- × • • • •
RESULTS SUMMARY	RESULT SUMMARY	□ 1) Pause ■ Stop (F8) 2 → 2 & T 34 ▼		
	RESULT SUMMARY	□ 1) Pause ■ Stop (F8) 2 → 2 & T 34 ▼ □ ○ ▷+ 1 10		
RESULTS SUMMARY		□ 1) Pause ■ Stop (F8) 2 → 2 & T 34 → □ ○ ▷+ 1 0		D x1 D x1 D vido D vido Clear all

Step1 svm classifier

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





	5,255	5,1.00,	0.00,1.0	00,0.00,	,0.00,0.0	10,0.00,0
	0.04,	0.03,0	.01,0.00	,0.00,0	0.00,0.01	.,0.00,n
	7,0.0	03,0.08	,0.00,0.	.00,0.79	9,0.29,0.	21,0.71
	,12,0	0.05,0.	07,0.00,	0.00,1.	.00,1.00,	0.00,0.
	,255,	1.00,0	.00,0.00	,0.00,0	0.00,0.00	,0.00,0
	55,1.	.00,0.0	0,0.01,0	0.04,0.0	00,0.00,0	.00,0.0
	5,10,	0.04,0	.07,0.00	,0.00,0	0.00,0.00	,1.00,1
	5,1.0	00,0.00	,0.20,0.	.04,0.00	0,0.00,0.	00,0.00
	55,18	3,0.07,	0.05,0.0	00,0.00,	,0.00,0.0	10,1.00,
	186,0	0.73,0.	13,0.00,	0.00,0.	.00,0.00,	0.26,0.0
	5,255	5,1.00,	0.00,1.0	00,0.00,	,0.00,0.0	10,0.00,0
	41,0.	.72,0.0	6,0.01,0	0. <mark>01,</mark> 0.0	01,0.00,0	
	255,1	L.00,0.	00,0.01,	0.01,0.	.01,0.00,	0.00,0.0
	55,25	55,1.00	,0.00,0.	.00,0.00	0,0.00,0.	00,0.07
	. 252,	0.99,0	.01,0.00	,0.00,0	0.00,0.00	,0.00,0
	1,0.0	08,0.03	,0.00,0.	.00,0.00	0,0.00,0.	44,1.00
	10		UNIX		UTF-8	I
\mathbf{n}	2	Q	P A		Window	1:00 P
2	10		Ø	A LINE	0100	

Step 2 Naïve bayer

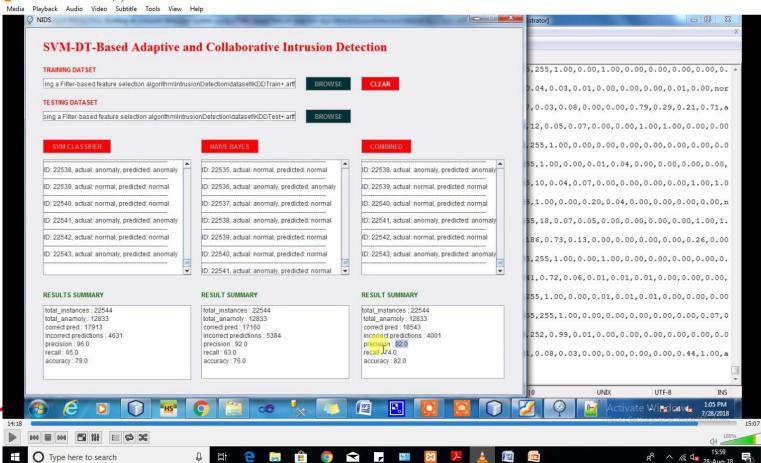
📤 svm-dt-based-.webm - VLC media player



TRAINING DATSET	sionDetection\dataset\KDDTrain+.arff BROWSE	CLEAR	,,203,1.00,0.00,1.0	0,0.00,0.00,0.00,0.00,
ing a Filter-based feature selection algorithm\Intru:	sionDetection/dataset/KDD1rain+.am	CLEAR	0.04,0.03,0.01,0.00	,0.00,0.00,0.01,0.00,n
TESTING DATASET	sionDetection\dataset\KDDTest+.arff BROWSE		7,0.03,0.08,0.00,0.	00,0.79,0.29,0.21,0.71
sing a Filter-based feature selection algorithm\Intru	IsionDetection/dataset/KDD1est+.am	-	.12,0.05,0.07,0.00,	0.00,1.00,1.00,0.00,0.
SVM CLASSIFIER	NAIVE BAYES	COMBINED	,255,1.00,0.00,0.00	,0.00,0.00,0.00,0.00,0
ID: 22538, actual: anomaly, predicted: anomaly	ID: 22250, actual: normal, predicted: normal	-	55,1.00,0.00,0.01,0	.04,0.00,0.00,0.00,0.0
ID: 22539, actual: normal, predicted: normal	ID: 22251, actual: anomaly, predicted: anomaly		5,10,0.04,0.07,0.00	,0.00,0.00,0.00,1.00,1
ID: 22540, actual: normal, predicted: normal	ID: 22252, actual: anomaly, predicted: normal		5,1.00,0.00,0.20,0.	04,0.00,0.00,0.00,0.00
ID: 22541, actual: anomaly, predicted: anomaly	ID: 22253, actual: normal, predicted: normal		55,18,0.07,0.05,0.0	0,0.00,0.00,0.00,1.00,
ID: 22542, actual: normal, predicted: normal	ID: 22254, actual: normal, predicted: normal		186,0.73,0.13,0.00,	0.00,0.00,0.00,0.26,0.
ID: 22543, actual: anomaly, predicted: anomaly	ID: 22255, actual: normal, predicted: normal		5,255,1.00,0.00,1.0	0,0.00,0.00,0.00,0.00,
	ID: 22256, actual: anomaly, predicted: normal		11.0.72.0.06.0.01.0	.01,0.01,0.00,0.00,0.0
RESULTS SUMMARY	RESULT SUMMARY	RESULT SUMMARY		0.01,0.01,0.00,0.00,0.
total_instances : 22544 total_anamoly: 12833	total_instances : 22544 total_anamoly : 12833		55,255,1.00,0.00,0.	00,0.00,0.00,0.00,0.07
correct pred : 17913 incorrect predictions : 4631	correct pred : 17160 incorrect predictions : 5384		.252.0.99.0.01.0.00	,0.00,0.00,0.00,0.00,0
precision : 96.0 recall : 65.0	precision : 92.0 recall : 63.0			00,0.00,0.00,0.44,1.00
accuracy: 79.0	accuracy: 76.0		1,0.00,0.03,0.00,0.	00,0.00,0.00,0.44,1.00
· · ·				
			IO UNEX	UTF-8

COMINED

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





RESULT SHOW



a svm-dt-based-.webm - VLC media player Media Playback Audio Video Subtitle Tools View Help NIDS X istrator] SVM-DT-Based Adaptive and Collaborative Intrusion Detection TRAINING DATSET ing a Filter-based feature selection algorithm\IntrusionDetection\dataset\KDDTrain+.arff BROWSE CLEAR 0.04,0.03,0.01,0.00,0.00,0.00,0.01,0.00,nor TESTING DATASET 7,0.03,0.08,0.00,0.00,0.79,0.29,0.21,0.71,a sing a Filter-based feature selection algorithm\IntrusionDetection\datasetKDDTest+.arff 12,0.05,0.07,0.00,0.00,1.00,1.00,0.00,0.00 5 1 00 0 00 0 01 0 04 0 00 0 00 0 00,0.00, ID: 22538, actual: anomaly, predicted: anomaly ID: 22535, actual: normal, predicted: normal O Recording: 00:14:52 1.00,1.0 ID: 22539, actual: normal, predicted: normal ID: 22536, actual: anomaly, predicted: anomaly ⊕ ⊖ x1 _ • (II) Pause Stop (F8) 0,0.00,n ID: 22540, actual: normal, predicted: normal ID: 22537, actual: anomaly, predicted: normal 🖋 🔿 🗊 🖉 T 34 M Undo ID: 22541, actual: anomaly, predicted: anomaly ID: 22538, actual: anomaly, predicted: normal ,1.00,1. 0 4 f Clear all ID: 22542, actual: normal, predicted: normal ID: 22539, actual: normal, predicted: normal ID: 22542, actual: normal, predicted: normal 86.0.73.0.13.0.00.0.00.0.00.0.00.0.00.0.26.0.00 ID: 22543, actual: anomaly, predicted: anomaly ID: 22540, actual: normal, predicted: normal ID: 22543, actual: anomaly, predicted: anomaly -ID: 22541, actual: anomaly, predicted: normal --\$1,0.72,0.06,0.01,0.01,0.01,0.00,0.00,0.00, RESULTS SUMMARY **RESULT SUMMARY** RESULT SUMMARY total_instances : 22544 total_instances : 22544 total_instances : 22544 total_anamoly: 12833 total_anamoly: 12833 total_anamoly: 12833 correct pred : 17160 correct pred : 17913 correct pred : 18543 incorrect predictions : 4631 incorrect predictions : 5384 incorrect predictions : 4001 precision : 96.0 precision: 92.0 precision: 92.0 recall: 65.0 recall: 63.0 recall: 74.0 accuracy: 79.0 accuracy: 76.0 accuracy: 82.0 UNIX UTF-8 INS 1:05 PM WE ctivate Window 7/28/2018 15:03 15:07 H 🖬 🚻 📰 😂 🛇 844 < ► 🛄 0 Type here to search an a G Sx

Conclusion

- In this paper, a collaborative and adaptive intrusion detection method based on 2class 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. I. 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.