UNIVERSITÀ
DEGLI STUDI
FIRENZE

Scuola di Scienze Matematiche, Fisiche e Naturali
Corso di Laurea in Informatica

Tesi di Laurea

UTILIZZO DI SOFT-BROWNIAN-OFFSET PER LA GENERAZIONE DI ATTACCHI AI FINI DELL'ADDESTRAMENTO DI RILEVATORI DI INTRUSIONI

APPLICATION OF SOFT-BROWNIAN-OFFSET TO GENERATE CYBER-ATTACKS TO TRAIN INTRUSION DETECTORS

GUGLIELMO BARTELLONI

Relatore: *Relatore*
Correlatore: *Correlatore*

Anno Accademico 2022-2023

INDICE

ELENCO DELLE FIGURE

"Inserire citazione"
— Inserire autore citazione

1

INTRODUZIONE

Un sistema di rilevamento di intrusioni, anche detto intrusion detection system (IDS), è un'applicazione o un dispositivo volta a monitorare continuamente la rete per identificare attività malevole.

In particolare un IDS controlla il traffico di rete oppure i log di sistema, alla ricerca di possibili anomalie che potrebbero indicare la presenza di attacchi.

Per migliorare il rilevamento delle intrusioni, nell'ultimo decennio, si è iniziato ad utilizzare algoritmi di Machine Learning e Deep Learning attingendo informazioni dai Big Data. [2]

Questo però questo ha portato a nuove problematiche, come ad esempio il fatto che i modelli di Machine Learning e Deep Learning sono molto sensibili ai dati di addestramento.

Un dataset contenente pacchetti di rete sarà composto per la maggior parte da pacchetti "normali", cioè pacchetti di traffico abituale e, per la restante parte, da pacchetti di attacchi. I vari dataset sul traffico di rete presenti oggi però, non hanno una quantità sufficiente di attacchi per poter addestrare al meglio i modelli.

Un modello addestrato su un dataset con una percentuale di attacchi troppo bassa, non sarà in grado di rilevare bene gli attacchi.

Un metodo per sopperire a questa mancanza è quello di generare nuovi dati a partire da quelli già esistenti (Data Augmentation). I dati generati devono essere però sufficientemente differenti di modo da rappresentare meglio le anomalie che si hanno nella rete durante un attacco.

In questa tesi esploreremo un algoritmo di Data Augmentation chiamato Soft-Brownian-Offset (SBO) [3] e lo utilizzeremo per generare nuovi dati per addestrare un IDS.

In particolare Soft-Brownian-Offset permette di generare campioni così detti out-of-distribution (OOD), cioè campioni che non fanno parte della distribuzione dei dati di partenza. Questo è coerente col fatto che di solito i pacchetti di attacchi sono fuori dalla distribuzione dei pacchetti comuni.

2

FONDAMENTI

2.1 INTRUSION DETECTION SYSTEM

Un intrusione può essere definita come un evento che causa danni ad un sistema informatico [1].

Gli Intrusion Detection System (IDS) sono delle soluzioni hardware o software che, posti all'interno di una rete o di un sistema, rilevano eventuali intrusioni.

[4] Le principali funzioni degli IDS sono:

- Monitorare ed analizzare sia le attività utente che di sistema
- Tracciare le violazioni delle policy utente
- Analizzare le configurazioni e le vulnerabilità del sistema
- Rilevare tipici attacchi di rete
- Analisi di attività anomale

[5] Solitamente gli IDS vengono classificati in base al tipo di analisi che effettuano e come questi rilevano le minacce. Ne esistono di tre tipi principali:

- Signature-Based Detection (SD)
- Anomaly-based Detection (AD)
- Stateful Protocol Analysis (SPA)

2.1.1 *Signature-Based Detection*

Questo tipo di rilevamento utilizza la firma di un attacco per poterlo rilevare. Quindi conoscendo questa firma, gli IDS la comparano agli eventi catturati della rete. Dato che questi attacchi hanno bisogno di una conoscenza pregressa sono anche chiamati Knowledge-based.

2.1.2 *Anomaly-based Detection*

Gli AIDS sono stati introdotti per sopperire alle mancanze del Signature-Based Detection. Questo tipo di rilevamento utilizza un modello che rappresenta il normale comportamento della rete. Quindi, se viene rilevato un evento che non è coerente con il modello di riferimento, allora viene segnalata un'anomalia. Questo tipo di rilevamento è chiamato anche Behavior-Based.

Il principale vantaggio di questo tipo di IDS è la possibilità di rilevare gli attacchi zero-day [**?**], in quanto questi sistemi, non si basano sulla firma dei dati o su regole rigide. Inoltre un altro vantaggio è che risulta essere difficile, per un eventuale criminale, capire quale sia il comportamento normale di un utente senza produrre un segnale da parte del sistema [1].

˜[**?**]SurveyIntrusionDetection2019 Gli AIDS possono essere classificati in base al metodo per la loro implementazione:

- Basati sulla Statistica (Statistical-Based)
- Basati sulla Conoscenza (Knowledge-Based)
- Basati sull'apprendimento automatico (Machine Learning-Based)

Gli AIDS Statistical-Based dopo aver registrato i dati di una porzione di elementi, ne derivano il modello statistico di un normale utente nella rete. I Knowledge-based invece, utilizzano regole predefinite per generare il modello di riferimento. Dall'altra parte troviamo gli AIDS Machine Learning-Based, che utilizzano un algoritmo di apprendimento automatico per generare il modello di riferimento.

La figura 1 mostra più in dettaglio questo tipo di classificazione e i metodi di implementazione associati.

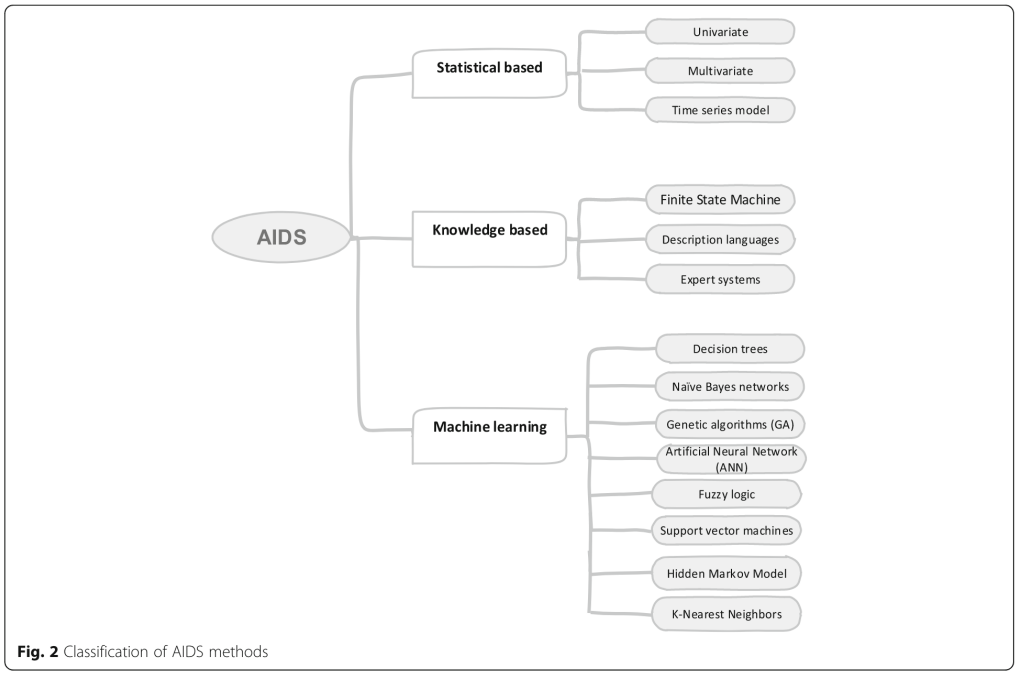

Fig. 2 Classification of AIDS methods

Figura 1: Schema che riassume i vari metodi di implementazione degli AIDS, da [1]. I modelli sono divisi nelle tre categorie descritte precedentemente, ma sono presenti anche i vari tipi di algoritmi utilizzati.

2.1.3 *Stateful-Protocol-Analysis*

In questo caso gli IDS conoscono lo stato e le specifiche del protocollo utilizzato. Vengono quindi rilevati degli eventi che non rispettano gli standard del protocollo, generalmente quelli da specifica e.g. IEEE.

Potrebbe sembrare che gli AD e gli SPA siano simili, in realtà i primi, conoscono il comportamento di una specifica rete, mentre i secondi, conoscono solo gli standard dei protocolli.

2.2 MACHINE LEARNING PER RILEVAMENTO DI INTRUSIONI

2.3 XGBOOST

2.4 DATASET

3

SOFT BROWNIAN OFFSET

4

GENERAZIONE DI ATTACCHI USANDO SOFT BROWNIAN OFFSET

5

RISULTATI

6

CONCLUSIONI

BIBLIOGRAFIA

[1] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: Techniques, datasets and challenges," *Cybersecurity*, vol. 2, p. 20, July 2019. (Citato nelle pagine 3, 9, 10, and 11.)

[2] Z. Ahmad, A. Shahid Khan, C. Wai Shiang, J. Abdullah, and F. Ahmad, "Network intrusion detection system: A systematic study of machine learning and deep learning approaches," *Transactions on Emerging Telecommunications Technologies*, vol. 32, Jan. 2021. (Citato a pagina 7.)

[3] F. Moller, D. Botache, D. Huseljic, F. Heidecker, M. Bieshaar, and B. Sick, "Out-of-distribution Detection and Generation using Soft Brownian Offset Sampling and Autoencoders," in *2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, (Nashville, TN, USA), pp. 46–55, IEEE, June 2021. (Citato a pagina 7.)

[4] A. S. Ashoor and S. Gore, "Importance of Intrusion Detection System," vol. 2, no. 1, 2010. (Citato a pagina 9.)

[5] H.-J. Liao, C.-H. Richard Lin, Y.-C. Lin, and K.-Y. Tung, "Intrusion detection system: A comprehensive review," *Journal of Network and Computer Applications*, vol. 36, pp. 16–24, Jan. 2013. (Citato a pagina 9.)