Intrusion Detection System using Blockchain and Federated Learning

Aarthi N - 1950001002
Joseph Immanuel Amirtharaj - 195001044

SSN College of Engineering, Chennai

November 8, 2022

Introduction

Introduction

- **An Intrusion Detection System** is used to detect anomalies in the network traffic patterns. It is classified into two categories, namely signature-based and anomaly-based IDSs.

Introduction

- **An Intrusion Detection System** is used to detect anomalies in the network traffic patterns. It is classified into two categories, namely signature-based and anomaly-based IDSs.
- **Signature-based IDS** is trained to detect an attack based on signatures of known attacks. A signature defines a footprint or pattern associated to the malicious attack.

Introduction

- **An Intrusion Detection System** is used to detect anomalies in the network traffic patterns. It is classified into two categories, namely signature-based and anomaly-based IDSs.
- **Signature-based IDS** is trained to detect an attack based on signatures of known attacks. A signature defines a footprint or pattern associated to the malicious attack.
- Say Propositional Logic (PL).

Introduction

- **An Intrusion Detection System** is used to detect anomalies in the network traffic patterns. It is classified into two categories, namely signature-based and anomaly-based IDSs.
- **Signature-based IDS** is trained to detect an attack based on signatures of known attacks. A signature defines a footprint or pattern associated to the malicious attack.
- Say Propositional Logic (PL).
- Given a formula α in PL,
- Does there exists a **valuation** ν such that $\nu(\alpha) = T$ (i.e., $\nu \models \alpha$)?

Propositional Logic

- M teaches AI: M
- S teaches AI: S
- M & S write a book on AI: WB

Propositional Logic

- M teaches AI: M
- S teaches AI: S
- M & S write a book on AI: WB
- $R = (M \wedge S) \Rightarrow WB$

Propositional Logic

- M teaches AI: M
- S teaches AI: S
- M & S write a book on AI: WB
- $R = (M \land S) \Rightarrow WB$

$$\{R, \neg WB, S\} \text{ entails } \neg M$$

Propositional Logic

- M teaches AI: M
- S teaches AI: S
- M & S write a book on AI: WB
- $R = (M \wedge S) \Rightarrow WB$

$$\{R, \neg WB, S\} \text{ entails } \neg M$$

if each of the $\{R, \neg WB, S\}$ are true then does $\neg M$ hold?

Propositional Logic

- Does there exist a valuation ν such that

$$\nu \models \{R, \neg WB, S, M\}$$

Propositional Logic

- Does there exist a valuation ν such that

$$\nu \models \{R, \neg WB, S, M\}$$

- What is a valuation?

Propositional Logic

- Does there exist a valuation ν such that

$$\nu \models \{R, \neg WB, S, M\}$$

- What is a valuation? Assignment of **truth values** to M, S, WB.

Propositional Logic

- Does there exist a valuation ν such that

$$\nu \models \{R, \neg WB, S, M\}$$

- What is a valuation? Assignment of **truth values** to M, S, WB.
- Does there exist a valuation ν such that

$$\nu \models R \wedge \neg WB \wedge S \wedge M$$

Propositional Logic

- Countable set of proposition symbols $P = \{p_1, p_2, p_3, \cdots\}$
- Set of propositional connectives $\{\neg, \vee, \wedge, \Rightarrow\}$.

Propositional Logic

- Countable set of proposition symbols $P = \{p_1, p_2, p_3, \cdots\}$
- Set of propositional connectives $\{\neg, \vee, \wedge, \Rightarrow\}$.

The set of all **well-formed formulas** (**wff**s) of propositional logic are defined inductively as the smallest set satisfying the following conditions:

- Every $p_i \in P$ is a wff, (such wffs are called **atomic formulas**)
- If α is a wff then $(\neg\alpha)$ is a wff,
- If α, β are wffs then so are $(\alpha \vee \beta), (\alpha \wedge \beta), (\alpha \Rightarrow \beta)$ and
- Nothing else is a wff.

Propositional Logic

- Countable set of proposition symbols $P = \{p_1, p_2, p_3, \cdots\}$
- Set of propositional connectives $\{\neg, \vee, \wedge, \Rightarrow\}$.

The set of all **well-formed formulas** (**wff**s) of propositional logic are defined inductively as the smallest set satisfying the following conditions:

- Every $p_i \in P$ is a wff, (such wffs are called **atomic formulas**)
- If α is a wff then $(\neg\alpha)$ is a wff,
- If α, β are wffs then so are $(\alpha \vee \beta), (\alpha \wedge \beta), (\alpha \Rightarrow \beta)$ and
- Nothing else is a wff.

Alternatively:

$$\alpha, \beta \in \Phi ::= p_i \in P \mid (\neg\alpha) \mid (\alpha \vee \beta) \mid (\alpha \wedge \beta) \mid (\alpha \Rightarrow \beta).$$

Propositional Logic:Semantics

- **valuations** $\nu : P \rightarrow \{T, F\}$.
- Every symbol in P gets exactly one of the truth values $\{T, F\}$.

Propositional Logic:Semantics

- **valuations** $\nu : P \rightarrow \{T, F\}$.
- Every symbol in P gets exactly one of the truth values $\{T, F\}$.

ν can be extended inductively to the set of all wffs as follows:

- $$\nu(\neg\beta) = \begin{cases} T & \nu(\beta) = F \\ F & \nu(\beta) = T \end{cases}$$
- $$\nu(\alpha \vee \beta) = \begin{cases} T & \text{when } \nu(\alpha) = T \text{ or } \nu(\beta) = T \\ F & otherwise \end{cases}$$
- $$\nu(\alpha \wedge \beta) = \begin{cases} T & \text{when } \nu(\alpha) = T \text{ and } \nu(\beta) = T \\ F & otherwise \end{cases}$$
- $$\nu(\alpha \Rightarrow \beta) = \begin{cases} F & \text{when } \nu(\alpha) = T \text{ and } \nu(\beta) = F \\ T & otherwise \end{cases}$$

Propositional Satisfiability

Given α, how do we check the satisfiability of α

- Find the set of all propositions occurring in α, P_α,
- Generate all possible valuations over P_α,
- There will be $2^{|P_\alpha|}$ such valuations,
- Check the satisfiability for each such valuation one after another,
- If at least one valuation satisfies α (i.e., $\nu(\alpha) = T$, for some ν), report **success**.
- If all valuations fail to satisfy α (i.e., $\nu(\alpha) = T$, for all ν), report **failure**.

Temporal Logic

- if M and S teach AI for two consecutive years then eventually they will write the AI book.

$$\Box\Big(\big((M \wedge S) \Rightarrow \bigcirc(M \wedge S)\big) \Rightarrow \Diamond WB\Big)$$

Temporal Logic

- if M and S teach AI for two consecutive years then eventually they will write the AI book.

$$\Box\Big(((M \wedge S) \Rightarrow \bigcirc(M \wedge S)) \Rightarrow \Diamond WB\Big)$$

- Temporal Modalities
  - $\bigcirc$, $\bigcirc\alpha$ now if α holds in the immediate future.
  - $\Box$, $\Box\alpha$ now if α holds **always** in future.
  - $\Diamond$, $\Diamond\alpha$ now if α holds **sometimes** in future.

LTL Syntax and Semantics

$$\psi \in \Psi ::= p \in P \mid \neg\psi \mid \psi_1 \vee \psi_2 \mid \bigcirc\psi \mid \Box\psi \mid \Diamond\psi$$

LTL formulas are interpreted over sequence of valuations

$$\nu = \nu_0\nu_1\nu_2 \cdots \nu_i \cdots, \text{ where } \forall i \in \omega, \nu_i \subset_{fin} P$$

Satisfiability Relation

- $\nu, i \models p$ iff $p \in \nu_i$.
- $\nu, i \models \neg\psi$ iff $\nu, i \not\models \psi$.
- $\nu, i \models \psi \vee \psi'$ iff $\nu, i \models \psi$ or $\nu, i \models \psi'$.
- $\nu, i \models \bigcirc\psi$ iff $\nu, i+1 \models \psi$.
- $\nu, i \models \Diamond\psi$ iff $\exists j \geq i$, $\nu, j \models \psi$.
- $\nu, i \models \Diamond\psi$ iff $\forall j \geq i$, $\nu, j \models \psi$.

$$Models(\psi) = \{\nu = \nu_0\nu_1\nu_2\cdots \mid \nu, 0 \models \psi\}$$

LTL Satisfiability

Given an LTL formula ψ, does there exist a ν such that

$$\nu, 0 \models \psi$$

- Construct a Büchi Automaton A_ψ over $\Sigma = 2^{P_\psi}$ such that

$$Lang(A_\psi) = Models(\psi)$$

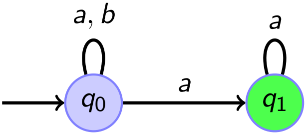
- If $Lang(A_\psi)$ is non-empty then ψ is satisfiable.

Büchi Automata

NFA over infinite words:

$$B = (Q, \Sigma, \Delta, I, G)$$

B accepts an infinite word $w \in \Sigma^\omega$ if there exists an infinite run ρ of B on w such that some good state $q \in G$ occurs infinitely many times in ρ.



LTL to Büchi Automata

Given LTL formula ψ_0

- Construct the closure set *cl* containing
  - all subformulas of ψ_0
  - their negations
  - additional formulas, $\bigcirc\Diamond\alpha$ if $\Diamond\alpha \in cl$
- Define $UR = \{\Diamond\alpha \in cl\}$
- Construct the atom set *AT* as subsets of *cl* satisfying following criteria:
  - for all $\alpha \in cl$, $\alpha \in A$ iff $\neg\alpha \notin A$
  - for all $\alpha \vee \beta \in cl$, $\alpha \vee \beta \in A$ iff $\alpha \in A$ or $\beta \in A$
  - for all $\Diamond\alpha \in cl$, $\Diamond\alpha \in A$ iff $\alpha \in A$ or $\bigcirc\Diamond\alpha \in A$

LTL to Büchi Automata Continued

- Define $Q = AT \times UR$
- Define $I = \{(A, u) \mid \psi_0 \in A, u = \emptyset\}$
- Define $G = \{(A, u) \mid u = \emptyset\}$
- Define $(A, u) \xrightarrow{P'} (A', u')$ if the following conditions hold:
    - $P' = A \cap P$
    - for every $\bigcirc\alpha \in cl$, $\bigcirc\alpha \in A$ iff $\alpha \in A'$
    - $$u' = \begin{cases} \{\Diamond\alpha \in u \mid \alpha \notin A'\} & u \neq \emptyset \\ \{\Diamond\alpha \in A' \mid \alpha \notin A'\} & u = \emptyset \end{cases}$$

Thank You