Ministerul Apărării Naționale
Academia Tehnică Militară „Ferdinand I”

REZUMATUL TEZEI DE DOCTORAT

„Contribuții privind dezvoltarea sistemelor honeypot auto-adaptive”

Autor: ing. Adrian PĂUNA
Email: adrian.pauna.ro@gmail.com
Conducător de doctorat: prof. univ. dr. ing. Victor-Valeriu PATRICIU

Într un context global, în care amploarea atacurilor cibernetice creste exponențial, detectarea și mai ales înțelegerea acestora este de o importanță vitală. Poate cel mai folosit mecanism pentru studiul elementelor unui atac cibernetic îl reprezintă sistemele honeypot.

Cu o dezvoltare constantă în ultimi patruzeci de ani, sistemele honeypot au evoluat de la simple calculatoare expuse în Internet cu scopul de a fi atacate și simultan monitorizate, ajungând la nivelul la care uzând de dezvoltările curente în domeniul inteligentei artificiale pot interacționa autonom cu atacatorii.

Prezenta lucrare expune o serie de sisteme honeypot denumite auto adaptive, dezvoltate pe parcursul cercetării științifice. Aceste sisteme au la bază folosirea unor algoritmi de învățare prin întărire (Reinforcement Learning), în scopul obținerii unei interacțiuni autonome cu atacatorii. Lucrarea prezintă în fiecare din cele patru capitole de contribuții atât o descriere din punct de vedere teoretic a elementelor de învățare automată folosite, cât și arhitectura sistemelor honeypot dezvoltate, implementarea și o serie de teste și rezultate.

Capitolul 1 Introducere conține o descriere a modulelor ce compun arhitectura sistemelor honeypot auto-adaptive. De asemenea, sunt prezentate și elemente de bază referitoare la algoritmii de învățare automată folosiți pentru dezvoltarea fiecărui sistem honeypot auto-adaptiv.

Capitolul 2 Sisteme honeypot conține o scurtă prezentare a conceptelor referitoare la sistemele honeypot. Este de asemenea detaliată evoluția sistemelor honeypot, de la cele apărute la începutul anilor ’80 până la cele din zilele noastre. De asemenea, este prezentată o clasificare a sistemelor honeypot în șase categorii, în funcție de diferite elemente definitorii. Capitolul continuă cu o prezentare a celor mai uzitate tipuri de sisteme honeypot, și anume sisteme honeypot cu grad redus de interacțiune, respectiv sisteme honeypot cu grad ridicat de interacțiune. Capitolul se încheie cu o prezentare detaliată a modelarii sistemelor honeypot auto-adaptive, ținându-se cont de paradigma învățări automate.

Capitolul 3 RASSH - sistem honeypot auto-adaptiv cu întărire prezintă în prima parte elementele de teorie aferente algoritmilor de învățare prin întărire folosiți pentru modelarea și implementarea sistemului RASSH. În acest capitol sunt detaliate și noțiuni generale precum sunt

cele referitoare la procesul de decizie Markov, funcții Valoare, respectiv funcții Acțiune-Valoare, dilema explorare/exploatare. Prezentarea acestora este necesară pentru înțelegerea modului de funcționare a algoritmilor de învățare automată folosiți. De asemenea, este detaliat și algoritmul SARSA (State-Action-Reward-State-Action), a cărui implementare este folosită în modul de învățare automată folosit de RASSH.

Capitolul continuă cu prezentarea modelarii sistemului honeypot sub forma unui agent de învățare automată și detalierea implementării acestuia. Finalul conține o serie de concluzii referitoare la utilitatea sistemului honeypot implementat.

Capitolul 4 QRASSH - sistem honeypot auto-adaptiv cu întărire profundă analizează elementele definitorii ale algoritmilor de învățare prin întărire profundă (DRL - Deep Reinforced Learning). Algoritmii DRL sunt practic o evoluție a algoritmilor de bază RL prin introducerea de elemente de tip rețele neurale. Acest lucru le îmbunătățește dramatic performanța, făcându-i fezabili pentru implementări în producție. Capitolul continuă cu prezentarea arhitecturii și modelării sistemului QRASSH. Sunt evidențiate elemente aferente algoritmului DQN (Deep – Q – Learning) folosit pentru a determina acțiunile efectuate de sistemul honeypot în contact cu atacatorii. De asemenea, sunt prezentate o serie de teste efectuate cu sistemul honeypot expus în Internet. În final este prezentată o serie de concluzii rezultate în urma implementării și testării QRASSH.

Capitolul 5 CASSH – sistem honeypot auto-adaptiv capabil să raționeze descrie în prima parte o serie de elemente definitorii algoritmilor de Inferență bazată pe cazuri (CBR - Case Based Reasoning). Este detaliată schema ciclului CBR insistând pe cei patru R: Regăsește, Reutilizează, Revizuiește, Reține. În continuare este prezentată arhitectura și implementarea sistemului honeypot auto-adaptiv CASSH. De asemenea, este detaliată paradigma agenților de tip credință-dorință-intenție (BDI – Belief-Desire-Intention) în conjuncție cu algoritmii de inferență bazată pe cazuri (CBR). Capitolul concluzionează cu o serie de elemente referitoare la rezultatele testelor întreprinse.

Capitolul 6 IRASSH – sistem honeypot auto-adaptiv folosit pentru optimizarea funcțiilor de recompensă debutează cu prezentarea detaliată a algoritmilor de Învățare inversă prin întărire de tip Discipol („Apprenticeship Learning via Inverse Reinforcement Learning”). Sarcina acestor algoritmi este aceea de a determina o funcție de recompensă dintr-un comportament observat. În continuare este prezentată modelarea matematică, precum și arhitectura și implementarea sistemului IRASSH. Acest sistem honeypot auto-adaptiv funcționează pe baza unui flux împărțit în trei faze. În Faza 1 sistemul honeypot auto-adaptiv de tip agent este antrenat manual. Practic, sistemului honeypot îi este prezentată secvența de acțiuni ce trebuie urmată în diferite situații de interacțiune cu atacatorii. În Faza 2, pe baza politicii învățate anterior sunt generate, folosind

algoritmii de învățare inversă prin întărire, o serie de ponderi aferente fiecărei caracteristici. Pe baza acestor ponderi este generată funcția de recompensă optimă. În Faza 3, funcția de recompensă obținuta în Faza 2 este folosită de agentul IRASSH în producție, și astfel verificată. Capitolul se încheie o prezentare a unor concluzii și elemente referitoare la utilitatea sistemului IRASSH.

Capitolul 7 Concluzii încheie lucrarea cu prezentarea concluziilor finale, enumerarea contribuțiilor originale ce au fost aduse la întreaga tematică abordată în cadrul lucrării de față, lista publicațiilor de pe perioada doctoratului, precum și cu bibliografia consultată pe durata întregului proces de cercetare științifică.