Кобус О.С., к.ф.-м. н., доцент
Бондаренко С.Ю., фахівець
Національна академія Служби безпеки України

МОДЕЛЮВАННЯ СТОХАСТИЧНОГО ПРОЦЕСУ В ДИНАМІЧНИХ МЕРЕЖЕВИХ СИСТЕМАХ ІЗ МЕХАНІЗМАМИ ЗВОРОТНОГО ЗВ'ЯЗКУ В РЕАЛЬНОМУ ЧАСІ ДЛЯ ДОДАТКІВ КІБЕРБЕЗПЕКИ

Стохастичне моделювання процесів у динамічних мережевих системах із механізмами зворотного зв'язку в режимі реального часу для програм кібербезпеки є вершиною складності та критичною потребою в сучасному кіберзахисті. В епоху ескалації кіберзагроз, коли стратегії змагання розвиваються непередбачувано та стають все більш витонченими, статичні моделі кібербезпеки вкрай не можуть забезпечити належний захист. Стохастичні моделі процесів, що використовують імовірнісні рамки, пропонують надійний спосіб пристосування до властивої мінливості та непередбачуваності кіберсередовища. Моделюючи загрози як імовірнісні події в стохастичній структурі, ці моделі запроваджують динамічну адаптивність, уможливлюючи можливості прогнозування, які розвиваються в міру появи нових даних.

Механізми зворотного зв'язку в реальному часі в стохастичних моделях є вирішальними для того, щоб модель залишалася адаптивною та реагувала на поточні умови мережі. Ці механізми створюють безперервний цикл зворотного зв'язку, який оновлює параметри моделі на основі спостережуваної поведінки в режимі реального часу, дозволяючи динамічно перекалібрувати свої прогнози та пороги виявлення загроз. Такі механізми зворотного зв'язку перетворюють модель із пасивного спостерігача на активного учасника виявлення загроз і реагування на них, дозволяючи їй передбачати загрози та реагувати на них, коли вони розгортаються. Цей підхід важливий у середовищі, де кіберзловмисники не тільки стають все більш досконалими, але й використовують методи машинного навчання, щоб змінювати свої стратегії атак на льоту.

Реалізація моделей стохастичних процесів із зворотним зв'язком у реальному часі в динамічних мережевих системах вимагає передових обчислювальних методів для управління як складністю моделей, так і швидкістю обробки даних, необхідних для операцій у реальному часі. Кожен компонент системи, від збору даних і попередньої обробки до аналізу загроз і відповіді на них, повинен функціонувати злагоджено, щоб підтримувати адаптивність моделі. Алгоритми машинного навчання, особливо оптимізовані для обробки великомасштабних високошвидкісних потоків даних, є невід'ємною частиною вдосконалення цих стохастичних моделей. Вони дозволяють системі аналізувати величезні обсяги даних у режимі реального часу, виявляючи шаблони та аномалії, які можуть вказувати на потенційні загрози.

Крім того, ці моделі повинні бути розроблені для роботи з мінімальною затримкою, оскільки будь-яка затримка в обробці може зробити модель неефективною для запобігання або пом'якшення кіберзагроз у реальному часі. Багатовимірна обробка даних і багаторівнева аналітична структура зазвичай використовуються для підвищення точності та швидкості моделі. Механізми зворотного зв'язку також повинні мати можливість інтегрувати інформацію з різних джерел даних, включаючи мережевий трафік, поведінкову аналітику та зовнішню розвідку про загрози, щоб створити цілісне уявлення про потенційні вразливості та ландшафти загроз [1, с. 17]. У цьому контексті часто застосовуються методи байєсівського висновку, що дозволяє системі постійно оновлювати свої ймовірнісні оцінки в міру включення нових даних.

Один із найскладніших аспектів цього дослідження полягає в розробці алгоритмів, які можуть збалансувати обчислювальну ефективність і складність моделі. Механізми зворотного зв'язку в реальному часі вимагають, щоб модель налаштовувала свої параметри, не вимагаючи надмірних обчислювальних ресурсів. Такі методи, як зменшення розмірності та розподілене обчислення, часто використовуються для оптимізації конвеєра обробки даних, що дозволяє моделі підтримувати високий рівень точності, не перевантажуючи ресурси системи. Крім того, здатність системи інтерпретувати відгуки та змінювати свої прогнози у відповідь на дані в реальному часі залежить від точно налаштованих алгоритмів, які керують балансом між чутливістю даних і швидкістю відповіді.

Практичні наслідки цього дослідження величезні й виходять за межі кібербезпеки в будь-яку область, де динамічна обробка даних у реальному часі є важливою. У кібербезпеці, зокрема, моделі стохастичних процесів із зворотним зв'язком у реальному часі представляють зміну парадигми від реактивних до проактивних стратегій захисту. Ці моделі дозволяють системам кібербезпеки вийти за рамки простого виявлення та реагування, дозволяючи їм передбачати потенційні загрози та завчасно коригувати захист. Цей підхід є особливо цінним у захисті від передових постійних загроз (APT), які характеризуються своєю скритністю та адаптивністю [2, с. 52].

Підсумовуючи, стохастичне моделювання процесів у динамічних мережевих системах із механізмами зворотного зв'язку в реальному часі пропонує багатообіцяючу основу для вдосконалення захисту кібербезпеки. Інтеграція зворотного зв'язку в реальному часі в ці моделі не тільки покращує їхню адаптивність, але й забезпечує більш проактивний підхід до виявлення загроз і пом'якшення. Однак розробка та впровадження цих систем вимагають значного вдосконалення обчислювальної ефективності та можливостей інтеграції даних. Оскільки кіберзагрози продовжують розвиватися, важливість динамічних, адаптивних механізмів захисту буде тільки зростати, позиціонуючи стохастичні моделі процесів як наріжний камінь майбутніх стратегій кібербезпеки. Це дослідження, хоч і складне, має потенціал для переосмислення ландшафту кіберзахисту, створюючи системи, які не тільки стійкі до атак, але й здатні розвиватися у відповідь на тактику кіберсупротивників, що постійно змінюється.

Список використаних джерел

1. Lee I. W. C., Fapojuwo A. O. Stochastic processes for computer network traffic modeling. Computer Communications. 2005. Т. 29, № 1. С. 1–23. URL: https://doi.org/10.1016/j.comcom.2005.02.004 (дата звернення: 12.11.2024).

2. X. Liu та ін. Network Defense Decision-Making Based on a Stochastic Game System and a Deep Recurrent Q-Network. Computers & Security. 2021. С. 24-80. URL: https://doi.org/10.1016/j.cose.2021.102480 (дата звернення: 12.11.2024).