Перехопити будь-який незашифрований (а деколи і зашифрований) призначений для користувача трафік з метою отримання паролів і іншої інформації.

Локалізувати несправність мережі або помилку конфігурації мережних агентів (для цієї мети сніфери часто застосовуються системними адміністраторами)

Оскільки в «класичному» сніфері аналіз трафіку відбувається вручну, із застосуванням лише простих засобів автоматизації (аналіз протоколів, відновлення TCP -потоку), то він підходить для аналізу лише невеликих його обсягів.

Одержано 17.04.2018

УДК 004.056.53

Євгенія Юріївна СПОРИШ,
студент групи Ф-6-3Ідср-14-1 ХНУВС
Науковий керівник: доцент кафедри інформаційних технологій факультету № 4 ХНУВС кандидат технічних наук, доцент Тулупов В. В.

ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ ВІДЕОСПОСТЕРЕЖЕННЯ

Актуальність обраної теми полягає в тому, що в сучасних умовах основна частина атак зловмисників здійснюється через комп'ютерні мережі, постійно ускладнюється їх структура, швидко збільшується кількість комп'ютерів та мережевого обладнання у тому числи систем відеоспостереження.

Захист інформації є складовою частиною забезпечення національної безпеки будь-якої держави і забезпечується правовими, організаційними, програмними та інженерно-технічними заходами.

На державному та регіональних рівнях впроваджуються різні програми та заходи безпеки. Так, наприклад у березні 2018 року на сесії Харківської обласної ради була прийнята «Програма забезпечення публічної безпеки і порядку та протидії злочинності на території Харківської області на 2018–2019 роки», відповідно до якої будуть придбатися системи відеоспостереження, стаціонарні переговорні пристрої для термінового виклику спецслужб, електронні планшети, відеореєстратори, відеотехніка та сучасні засоби зв'язку для груп швидкого реагування та правоохоронців.

Серед завдань програми є:

– удосконалення науково-методичного, матеріально-технічного та інформаційного забезпечення правоохоронних та інших органів, що беруть участь у забезпеченні публічної безпеки та порядку;

– безперервний моніторинг криміногенної ситуації в області, в т.ч. за рахунок соціологічних технологій та забезпечення своєчасного реагування на негативні зміни;

– здійснення посиленого контролю за ситуацією у публічних місцях, передусім при проведення заходів за участю значної кількості громадян;

– запобігання правопорушенням, що вчиняються з використанням телекомунікаційних мереж та мережі Інтернет.

На теперішній час у системі Міністерства внутрішніх справ впроваджено низку аналітичних систем з можливістю проведення глибокого аналізу великих масивів інформації, включаючи відкриті джерела де на першому рівні є система відеомоніторингу наприклад – єдиний аналітичний сервісний центр (UASC) поліції, створений за прикладом системи безпеки Абу-Дабі при ГУНП в Донецькій області.

Метою даної роботи є дослідження можливості побудови безпечної мережі відеоспостереження за об'єктами.

Відповідно до поставленої мети визначимо наступні завдання:

– охарактеризувати стан проблем існуючих систем відеоспостереження та їх використання суб'єктами господарювання;

– дослідити канали витоку інформації та сучасні методи й засоби захисту мереж відеоспостереження;

– проаналізувати технічні завдання на проектування мереж відеоспостереження та існуючи системи на сучасному ринку готового обладнання.

Одержано 17.04.2018

УДК 004.728:519.87

Павло Сергійович ВЄЛЬКІН,
студент групи КІТз-72м Національного технічного університету «Харківський політехнічний інститут»
Науковий керівник: професор кафедри інформаційних технологій факультету № 4 ХНУВС доктор технічних наук, професор Можаєв О. О.

МОДЕЛЮВАННЯ ПЕРЕДАЧІ МУЛЬТИМЕДІЙНОЇ ІНФОРМАЦІЇ В ГЕТЕРОГЕННИХ КОМП'ЮТЕРНИХ МЕРЕЖАХ

При проектуванні, реалізації та обслуговуванні інформаційних телекомунікаційних систем і мереж зв'язку часто зустрічаються випадки, коли аналітичне рішення задачі практично неможливо в силу значних математичних труднощів, а проведення експериментальних досліджень та натурних випробувань вимагає досить великих витрат часу і коштів. Питання моделювання інформаційних процесів, систем і мереж розглядаються в даній роботі.

В результаті аналізу традиційних методів та моделей опису мережевого трафіку та визначення характеристик мережевого трафіку були наведені вимоги до якості обслуговування мережі, к яким відносяться – прозорість, доступність і надана пропускна здатність мережі. Детально розглянуті види мережевого трафіку та оцінки параметрів мережі.

Також проведено математичне аналітичне моделювання мережевого трафіку. Наведені Пуассонівські процеси та процеси Бернуллі. Приведен індекс дисперсії який використовується для опису пульсуючої структури трафіку. Розглянуті трафікові принципи PTSi ISE які виходять з аналізу проектування телетрафіка. Також отримана ефективна пропускна здатність трафікового потоку.

У роботі проаналізована можливість моделювання мережевого трафіку на основі марківських моделей. Детально розглянуті марківські та вбудовані марківські моделі, а такж ON/OFF та IPP моделі. Наведені марківські, відновлювальні моделі трафіку, до яких відносяться – процеси, керовані марківськими; пуассонівські процеси керовані марківськими; N – піковий процес; 1 – піковий процес.

Розглянуті текучі моделі трафіку, характеристики яких мають аналітичне трактування, однак такі моделі мають велику кількість параметрів і експоненціально згасаючу кореляційну функцію. Також розглянено частий випадок марківських моделей – це трафікові моделі керовані марківськими моделями. Приведені лінійні стохастичні моделі, а саме DARtaGBAR моделі. Розглянуті трафікові моделі TESi принципи на яких базується TES – моделювання.

Приведені основні поняття марківського віпадкового процесу, його основні характеристики та властивості, а також параметри що характеризують безперервний марківський ланцюг.

В результаті аналітичного моделювання марківських випадкових процесів був проведен облік дискретизації процеса у часі, а також запропоновано алгоритм дискретизації. Враховуючи скалярний і векторний характер досліджуваних процесів получено вираз для многовимірних марківських процесів.

Отримані співвідношення дозволяють спростити розрахунок статистичних характеристик випадкового процесу що дозволяю скоротити час дослідженя параметрів трафіку телекомунікаційної мережі.

Було запропоновано моделювати марківські процеси за допомогою формующіх фільтрів, які дозволяють створити більш адекватну модель процесу передачі даних.

Одержано 17.04.2018

УДК 004.77:621.39(043.3)

Юлія Миколаївна САЛФЕТНІКОВА,
студент групи КІТз-72м Національного технічного університету
«Харківський політехнічний інститут»
Науковий керівник: професор кафедри інформаційних технологій факультету № 4 ХНУВС доктор технічних наук, професор Можаєв О. О.

МОДЕЛІ ТРАФІКУ СИСТЕМИ АВТОМАТИЧНОЇ ІДЕНТИФІКАЦІЇ СУДЕН

Різноманітні комп'ютерні системи і мережі є невід'ємною частиною більшості служб та сервісів, якими користується людство. Ці служби і сервіси виконують значну кількість функцій та повинні відповідати певним критеріям, в залежності від власних функціональних обов'язків. Для забезпечення безпеки застосовуються різні підходи та дороги рішення. Одним з них може бути створення автоматичної системи ідентифікації, яка використовується для розпізнавання суден та керування їх рухом. Ця система повинна в реальному часі оброблювати інформацію, що збирається з множини джерел та повинна забезпечити її ефективну передачу в комп'ютерній мережі, яка має розподілену структуру.

Така система дозволяє проводити постійний обмін даними між судами, судами і береговими службами, а також здійснювати постійний моніторинг регіональних систем безпеки мореплавання і інформаційного забезпечення судноплавства за допомогою інформаційної інтеграції локальних систем регулювання руху судами, систем суднових повідомлень і відповідних інформаційно-обчислювальних мереж.

В умовах істотного збільшення обсягів переданої в мережі інформації особлива роль приділяється вдосконалюванню й розробці нових технологій передачі та розподілу інформації, у тому числі й технологій керування інтегральними інформаційними потоками, що забезпечують оперативність обміну інформацією в АІС.

Існуючі методи керування перевантаженнями, які використовувались на виникаючих критичних ділянках, також не враховують властивостей трафіка ІП, тому процес керування не завжди адекватний профілю трафіка. При виникненні пікових значеннях інтенсивності даними методами неможливо врахувати їхню короткочасність і сам момент часу виникнення пікових значень. Ця обставина визначає необхідність удосконалення класичного математичного інструментарію аналізу та синтезу розподілених комп'ютерних систем та мереж для підвищення оперативності передачі інформації.

Відмінною рисою мереж передачі даних АІС (СПД АІС) є динамічне збільшення обсягів циркулюючої інформації, а також виникнення критичних ділянок при виході з ладу каналів зв'язку. Значну роль в роботі ідентифікаційної системи відіграє пропускна здатність інформаційних каналів комп'ютерної мережі, яка обумовлена обсягом буферної пам'яті мережевого пристрою й продуктивністю процесора мережевого пристрою.

У результаті проведених досліджень встановлена можливість оцінки вірогідності результатів моделювання трафіка комп'ютерної мережі. Проаналізовано базові функції вейвлет – перетворення та визначено вейвлет-перетворення для різних типів самоподібного сигналу в КМ АІС. Найбільш ефективні для агрегування моделі будуються при використанні вейвлет-перетворення, зокрема із використанням функцій, які є подібними сплескам трафіка КМ АІС за параметрами: зміни інтенсивності та зміни похідної інтенсивності і відрізняються від базових функцій Хаара. При цьому можливо прогнозування трафіка на основі статистичних характеристик із врахуванням властивості масштабної інваріантності. Аналіз використання сингулярного вейвлет-аналізу для моделювання фрактального трафіка зі значною похідною сплеску встановив, що отримані на його базі моделі суттєво відризняються від отриманих за допомогою класичного вейвлет-аналізу, ступінь адекватності розроблених моделей підвищена до 10 %.

Одержано 17.04.2018