визначити атаку, якщо вона почнеться в період невеликої мережевої активності, або, якщо зловмисник шукає потенційно вразливі місця на сервері, проводячи міні- DDOS-атаки і вивчаючи поведінки сервера. У разі якщо верхня межа задана строго і зловмисник проводить міні-атаки в період найменшої мережевої активності, він може не порушувати задану кордон, і його дії будуть не виявлені. Атака буде виявлена тоді, коли зловмисник знайде потенційно вразливе місце, і зробить на нього атаку. Постійний моніторинг активності і перерахунок допустимих меж дозволяє цього уникнути. У період меншою мережевий активності верхня межа знизиться.

Перелік посилань

1. Долішний В.С. Аналіз і моніторинг сучасних DDoS - атак / В.С. Долішний, В.М. Чешун. - Тези доповідей Всеукраїнської науково-практичної конференції молодих вчених, ад'юнктів, слухачів, курсантів і студентів "Молодіжна військова наука у Київському національному університеті імені Тараса Шевченка" [Текст] / за заг. редакцією І.В. Толока. – К. : ВІКНУ, 2018. – С. 147 - 148.

2. DDoS Definitions - DdoSPedia, [Електронний ресурс]. http://security.radware.com/knowledge- center/DDoSPedia/http-flood

3. Zinchenko, V. V, Zinchenko, M. V (2017), Viyavlennya ddos-atak prikladnogo rivnya [Detection of application layer DDoS attacks], Mizhnarodna naukovo-tehnichna konferentsiya «RadIotehnichni polya, signali, aparati ta sistemi», Kyiv, pp. 262-264.

4. Системи і методи виявлення вторгнень: сучасний стан і напрями вдосконалення [Електронний ресурс]. URL:http://citfomm.ni/security/ intemet/ids_overview/#3

5. Холявка Є. П.; Метод виявлення мережевих атак в комп'ютеризованих системах управління: наукова робота, Хмельницький національний університет. - Хмельницький, 2019, [Електронний ресурс]. URL: http://konkurs.khnu.km.ua/wp-content/uploads/sites/25/2019/04/ DP3Eugen.pdf

Прогнозування ризиків завадостійкості в телекомунікаційних системах

Хмельницький Ю.В.
Хмельницький національний університет

Більшість сучасних телекомунікаційних систем визначаються значною кількістю параметрів, функціональними можливостями, вимогами до забезпечення захисту інформації, високою надійністю, розгалуженою інфраструктурою. Для якісної та надійної передачі інформаційних даних у телекомунікаційних системах задача забезпечення завадостійкості та захисту

інформації є однією із головних задач. Сама система має бути запроектована та експлуатуватись так, щоб у разі наявності завад вона забезпечила задану якість передавання інформаційних сигналів. Практично всі розрахунки впливу завад на передавання сигналів та розробка способів зменшення цього впливу є основними задачами, що вирішуються при проектуванні завадостійкості телекомунікаційних систем. Під завадостійкістю каналу передачі інформації тут розуміють здатність такої системи розрізняти та відновлювати сигнали із заданою достовірністю за наявності зовнішніх та внутрішніх завад.

В ряді витоків визначення поняття завадостійкості це здатність системи протистояти шкідливій дії завад, хоча воно більше наближається до розуміння фізичної суті завадостійкості - тут мається на увазі не просто стійкість системи передачі до завад, а її спроможність правильно функціонувати за їх наявності. Завдання визначення завадостійкості усієї телекомунікаційної системи досить складне, тому досить часто визначають завадостійкість окремих ланок системи, наприклад приймача, перетворювача для заданих способів передачі, системи кодування, модуляції. Тому сама завадостійкість телекомунікаційної системи залежить від виду повідомлень, рівня та характеристик завад, параметрів окремих складових частин систем [1]. В умовах реальних динамічних інформаційних завад збільшується ймовірність помилки, стає неможливим забезпечення заданого рівня надійності та вірогідності інформації за допомогою простого використання відомих методів кодування.

Маючи ж необхідну надійність та завадостійкість телекомунікаційної системи можуть забезпечити задану стабільність, захист інформації та безперервність управління. При досліджені та розгляді методів і засобів забезпечення завадостійкої передачі та захисту інформації в телекомунікаційних системах необхідно розглянути, що в широкому розумінні являє собою передача різного роду повідомлень із декількох пунктів у ряд пунктів. В технологіях та засобах передачі і захисту інформації семантична особливість повідомлень не враховується, тому задачею системи передачі інформації в сучасній телекомунікаційній системі є лише транспортування даних у визначене місце, так як оцінка змісту отриманих повідомлень це справа самого одержувача такої інформації.

Теорія та техніка передачі інформації в таких телекомунікаційних системах складалися протягом багатьох років і на сьогодні продовжують швидко та якісно розвиватися. Особливе місце канали передачі інформації займають у сучасних системах управління, в яких необхідно забезпечувати передачу досить великих обсягів потоків інформації із високою швидкістю, достовірністю і надійністю. У процесі функціонування на сучасні телекомунікаційні системи впливають багато різних факторів, що порушують нормальну роботу каналу передачі інформації. Ці фактори призводять до

порушення роботи каналів передачі інформації, фізичного виходу із ладу елементів та компонентів телекомунікаційних систем та інших негативних наслідків. Саму ж основу теорії потенційної завадостійкості розробив ще у 1946 р. академік В.О. Котельников[1]. В теорії потенційної завадостійкості вирішуються такі три основні задачі передачі інформації:

- синтез оптимального приймача – це знаходження правила його роботи та структурної схеми, що забезпечують найкращу якість приймання інформації;
- аналіз роботи оптимального приймача – це обчислення якості приймання сигналів, яка забезпечується цим приймачем потоків інформації;
- порівняння потенційної та реальної завадостійкості такої системи передачі інформації в телекомунікаційній системі.

В цих дослідженнях для практичного використання порівняння завадостійкості має особливе значення. Тут порівнювати реальну завадостійкість різних систем, схем, пристроїв, методів оброблення, видів модуляції не має ніякого сенсу. Таких схем та методів існують досить багато та зростання їх числа триває, а мала завадостійкість якоїсь системи чи схеми ще не означає, що вона є невдала чи неякісна. За таких завад кращої якості вже неможливо досягти. Тому порівняння реальної та потенційної завадостійкості системи дає можливість оцінювати якість реальної телекомунікаційної системи та знайти ще не використані резерви. Аналіз показує, якщо знати потенційну завадостійкість приймача каналу передачі інформації, можна завжди оцінити, наскільки близька до неї реальна завадостійкість існуючих способів приймання та наскільки доцільне їх подальше удосконалення для заданого методу передавання по каналах передачі інформації у системі.

Знання про потенційну завадостійкість за різними методами передавання потоків інформації дають змогу порівнювати ці методи між собою та знайти, які із них у цьому відношенні є найбільш оптимальними. Розглянемо кількісну міру завадостійкості. Для теоретичних розрахунків як потенційної, так і реальної завадостійкості застосовуються прямі методи оцінки якості передачі інформації. У разі передавання дискретних первинних сигналів для обчислень використовують ймовірність помилки.

Також розглянемо деякі принципи та засоби побудови систем передачі інформації по каналам із деякими шумами та перешкодами. В загальному випадку [2] структурна схема системи передачі інформації із завадами складається із джерела та одержувача повідомлень, перетворювачів повідомлення в сигнал та сигналу в повідомлення, каналу зв'язку. Джерелом повідомлень та одержувачем в одних системах передачі може бути людина, в інших різного роду пристрої – автомат приймання, комп'ютер, периферія тощо. Перетворення повідомлення у сигнал повинне бути оборотним.

В досліджені видно, що в цьому випадку по вихідному сигналу можна відновити вхідний первинний сигнал, тобто одержати усю інформацію, що є

в переданому повідомленні. В противному випадку деяка частина інформації буде загублена при передачі потоку. При передачі необхідних потоків інформації канальний сигнал може спотворюватися та на нього можуть накладатися завади. Приймальний пристрій системи обробляє прийняте коливання, яке є сумою перекрученого сигналу та завади, відновлює по ньому повідомлення, що із деякою похибкою відображає передане повідомлення. Тобто приймач повинен на основі аналізу коливання визначити, яке із можливих повідомлень у системі передавалось.

Аналіз показує, що одноразове використання каналу передачі інформації полягає у тому, що передавач певним чином впливає на канал передачі, а приймач спостерігає деякі характеристики каналу, що відображають цей вплив. Якщо ж канал передачі інформації дискретний, то для передавача існує кінцеве число впливів, які називаються вхідними сигналами [2]. Приймач розрізняє тільки визначене число класів результатів спостереження, що називаються загалом вихідними сигналами. В системі співвідношення між вхідними та вихідними сигналами у загальному випадку має імовірнісний характер. Канал передачі визначається встановленням умовних ймовірностей для кожної вхідної і вихідної послідовності.

Дослідивши основні взаємовпливи перешкод на головні елементи каналів передачі інформації телекомунікаційної системи із позиції теорії імовірності, можливо оцінити коефіцієнти за «технічною надійністю» основних компонентів та елементів телекомунікаційної системі за допомогою відомого співвідношення. Ступінь очікуваних ризиків функціонування телекомунікаційної системи можна подати як добуток імовірності небажаних наслідків на відповідну величину втрат аналогічно як у працях [2]:

$$R = \sum_{i=1}^{n} R_i = \sum_{i=1}^{n} p_i \cdot Z_i \quad , \qquad (1)$$

де R – величина ризику передачі;

p_i – ймовірності небажаних впливів каналу передачі інформації;

Z_i – величини втрат каналу передачі.

Для реального оцінювання ризику якості функціонування телекомунікаційної системи також використовують величину середньозваженого модуля відхилення ΔZ (тут n=12):

$$\Delta Z = \sum_{i=1}^{n} p_i \cdot (Z_i - \overline{Z}) \cdot \qquad \overline{Z} = \frac{1}{n} \sum_{i=1}^{n} Z_i \qquad (2)$$

Також визначають середньоквадратичне відхилення [3]:

$$\sigma = \sqrt{\sum_{i=1}^{n} p_i \cdot (Z_i - \overline{Z})^2}, \qquad (3)$$

Якщо ж взяти до уваги негативні відхилення від запланованих даних від параметра $\overline{Z}$, то ступінь ризику якості функціонування та захисту інформації телекомунікаційної системи оцінюється показником варіації S_Z і його значення визначається за допомогою такого відомого співвідношення:

$$S_Z = \sqrt{\sum_{i=1}^{n} p_i \cdot (Z_i - \overline{Z})^2 \cdot I_{vi}} \Big/ \sum_{i=1}^{n} p_i \cdot I_{vi}, \qquad (4)$$

де $I_i = \{I_{vi}\}$ – індикатор несприятливих відхилень якості роботи телекомунікаційної системи, якому відповідають:

0, для сприятливого відхилення $I_{vi} = 0$,

1, для несприятливого відхилення $I_{vi} = 1$.

Основним показником оцінювання ризику передачі невірогідної інформації в телекомунікаційних системах може бути також коефіцієнт можливих втрат каналу передачі, який враховує обсяг втрат по відношенню до суми абсолютних значень ймовірних втрат в завадостійких системах [3]:

$$K_Z = M_{ZV} / (M_{ZV} + M_{ZP}). \qquad (5)$$

де M_{ZV}, M_{ZP} – відповідно ймовірні величини сприятливих та несприятливих відхилень відносно значень показників θ_V, θ_P при розгляді рівнів втрат при передачі інформації Z і позитивних результатів.

Якщо тут розглядати завадостійкість телекомунікаційної системі як здатність системи протидіяти завадам, для цього треба знати, чим протидіяти та на що протидіяти, тобто для боротьби із завадами потрібні апріорні відомості про властивості носія потоків інформації і про самі завади. До таких властивостей у системі можливо віднести [3]:

– величина струму та напруги вхідного сигналу та завади в каналі передачі телекомунікаційної системи;

– середні потужності сигналу та завади в системі;

– вид та структура переносника інформації в телекомунікаційній системі;

– закон розподілу сигналу передачі тощо.

Дослідження та розгляд таких методів, способів та засобів забезпечення завадостійкої передачі інформації в телекомунікаційних системах показав, що завдання оптимального прийому полягає у використанні властивостей корисного сигналу, завади та каналу передачі для збільшення ймовірності правильного прийому. Для збільшення ймовірності правильного прийому потоків інформації має бути проведене попереднє оброблення прийнятого сигналу, яке забезпечує збільшення відношення сигнал та завада. Метод же накопичення застосовується у тому випадку, коли корисний сигнал протягом часу прийому є постійним та являє собою періодичну функцію. Він полягає у багаторазовому повторенні сигналу та підсумовуванні окремих його реалізацій в приймальному пристрої телекомунікаційної системи. Величину відношення сигнал та завада можна підвищити, якщо використати різницю між кореляційними функціями сигналу та завади. Цей метод є ефективним у випадку застосування в системах передачі періодичних та квазіперіодичних інформаційних сигналів.

Таким чином, на основі досліджень і аналізу методів та засобів забезпечення завадостійкої передачі інформації в сучасних телекомунікаційних системах можливо зробити висновок, що завдання прогнозування ризиків завадостійкої передачі, оптимального та якісного прийому та захисту інформації полягає у використанні властивостей корисного сигналу, завади та каналу передачі інформації для збільшення ймовірності правильного прийому. Для збільшення ймовірності правильного прийому має бути проведене попереднє оброблення прийнятого сигналу, яке забезпечує збільшення спів відношення величини сигнал та завада. Канали передачі інформації, що застосовують технології, які дозволяють у режимі реального часу гарантувати якісну, надійну та вірогідну передачу інформації в умовах впливу завад, краще забезпечують величину заданих значень показників вірогідної передачі інформації здійснюється за рахунок використання необхідного кодування. Знаючи властивості сигналу і завади, можна встановити певні відмінності між ними та використати їх для розроблення способів, засобів та методів забезпечення завадостійкої передачі. На відміну від спотворень завади носять випадковий характер та заздалегідь невідомі і тому не можуть бути повністю усунені. Таким чином, можна зробити висновок про те, що знання методів та засобів побудови сучасних каналів передачі телекомунікаційних систем в умовах дії завад, дозволить будувати надійні канали передачі інформації.

Перелік посилань

1. Бабич В. Д. Завадостійкість каналів зв’язку : навч. посібн. / В.Д.

Бабич, О.Д. Кувшинов, О.П. Лежнюк, С.П. Лівенцев // К. : КВІУЗ, 2001. - 150 с.

2. Хмельницький Ю.В. Забезпечення вірогідної передачі інформації при впливі перешкод в телекомунікаційних мережах / Ю.В Хмельницький, Г.Б.Жиров, Н.В. Кульпак // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2018. – Вип. № 59. – С. 161-170.

3. Хмельницький Ю.В Методи та засоби забезпечення завадостійкої передачі інформації в телекомунікаційних мережах / Ю.В Хмельницький, О.А. Каблуков, Л.О. Ряба, Л.В. Солодєєва, А.О. Ткач // Збірник наукових праць Військового інституту Київського нац. університету імені Тараса Шевченка. - К.: ВІКНУ, 2019. - № 64. – 133-144 с.

Оцінка ефективності роботи генератора криптоключів підвищеної ентропії для системи клієнт-банк

Чешун В.М., Чорненький В.І.[1], Яцків В.В.[2]
Хмельницький національний університет [1]
Західноукраїнський національний університет[2]

Після виконаної розробки засобів реалізації алгоритму роботи системи клієнт-банк із застосуванням генераторів криптоключів підвищеної ентропії, важливим етапом стає апробація здатності засобів, що реалізують алгоритм, виконувати передбачені функції відповідно до наявних вимог.

Розроблені алгоритм і засоби орієнтовані на накопичення пулу ентропії від джерел з передачею даних в систему клієнт–банк. Парадокс оцінки ентропії полягає в тому, що вона потребує зазначення того, наскільки непередбачувана послідовність. Якби можна було зробити абсолютний доказ непередбачуваності, то за визначенням послідовність була б передбачуваною.

Слід зазначити, що далеко не всі гіпотези про підвищену ентропію застосовуваних джерел і отримуваних на їх базі даних проходять перевірку на відповідність вимогам випадковості значень, тому черговою задачею дослідження постає оцінка якості отримуваного від джерел ентропії пулу тестами на випадковість.

Перевірка якості генерованих різними методами чисел на випадковість є однією із найактуальніших і найскладніших задач при розробці і впровадженні генераторів псевдовипадкових чисел.

Актуальність задачі зумовила до активного пошуку її розв’язку, а складність – до відсутності єдиного універсального рішення.

Як наслідок, на сьогоднішній день розроблено велику кількість методів перевірки якості послідовностей псевдовипадкових чисел, що