УДК 519.6

[1]*Игорь Викторович Рубан (д-р техн. наук, профессор)*
[2]*Антон Александрович Смирнов*

[1]*Харьковский национальный университет радиоэлектроники, Харьков, Украина*
[2]*Харьковский университет Воздушных Сил имени И. Кожедуба, Харьков, Украина*

МОДЕЛЬ ОБРАБОТКИ TCP-СОЕДИНЕНИЙ ДЛЯ СТЕГАНОГРАФИЧЕСКОЙ ПЕРЕДАЧИ ДАННЫХ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

В данной статье предложена модель обработки TCP соединений для стеганографической передачи данных в информационно-телекоммуникационных сетях. Определены требования к модификации протокола TCP для корректной работы стеганографической системы. Обоснован факт отсутствия временных задержек в функционировании модифицированного TCP по отношению к его стандартным версиям.

Ключевые слова: *сетевая стеганография; стегоконтейнер; начальный номер последовательности.*

Вступление

Кибернетическая безопасность является одним из ключевых направлений по обеспечению государственной безопасности [1]. Это определяет развитие методов как защиты информации при её обработке в информационно-телекоммуникационных сетях (ИТКС), так и средств обеспечения информационной безопасности автоматизированных систем управления (АСУ).

Постановка задачи. В последнее время, приобрели популярность методы скрытной передачи данных в ИТКС за счёт использования особенностей протоколов базовой эталонной модели сетевого взаимодействия (БЭМСВ) [2, 3]. Стандарты RFC (Request For Comments) носят рекомендательный характер, не принуждая к реализации протоколов во всех тонкостях, но акцентируя внимание на возможности утилизации любой разработанной версии. Множество таких методов объединяет в себе "сетевая стеганография". Основной задачей, при этом, является сокрытие самого факта передачи сообщения, что усилит криптографические методы защиты информации дополнительным уровнем защиты [2].

Целью статьи является обоснование выбора графовой модели обработки TCP-соединений для скрытной передачи данных позволяющей исследовать процесс функционирования стеганографической системы (СГС) в динамике и выявить уязвимости к возможным атакам.

Основная часть

В основу модели обработки TCP-соединений для стеганографической передачи данных в ИТКС, заложен перехват управления генерацией начальных номеров последовательности при организации соединения [3, 4]. Для детального анализа модели обработки TCP-соединений процесс стеганографической передачи данных условно разделён на две части: передача и приём сообщения.

Передача сообщений включает в себя формирование стегоконтейнеров и их отправку получателю. Приём сообщения включает в себя приём стегоконтейнеров и извлечение сообщения. Подробная структурная схема модели изображена на рис.1. Для моделирования системы стеганографической передачи данных в ИТКС, выбран аппарат сетей Петри, как мощный инструмент для описания функционирования динамических систем [5].

В соответствии с [5], сеть Петри – ориентированный двудольный граф. На таких графах используются два типа вершин: позиции и переходы. При этом однотипные вершины не могут быть инцидентными. Позиции соответствуют событиям, происходящим в процессе функционирования моделируемой системы, а переходы – условиям наступления соответствующего события.

С целью придания графовой модели обработки TCP – соединений нужных свойств, исходными условиями при моделировании являются:

1. Множество текстов, представляемых для сравнения, всегда обладает достаточной мощностью. Такое условие позволяет отобразить режимы работы системы при посимвольном сравнении сообщения с множеством опорных текстов.

2. Обработка множества опорных текстов сводится к двум возможным действиям над ними: смещение 128-символьного окна, используемого для сравнения опорного текста и замена опорного текста следующим во множестве представляемых для сравнения.

3. Выполнению тупиковой разметки предшествует передача четырёх неинформативных значений в сдвиговый регистр и генерация

соответствующего номера ISN. Такое действие обуславливает информирование принимающей стороны о том, что сообщение передано полностью.

Рис. 1. Структурная схема модели обработки TCP – соединений для стеганографической передачи данных

Графовая модель обработки TCP – соединений для приёма сообщения по стеганографическому каналу отображает свойства описываемого объекта исходя из следующих условий:

1. Вершина графа, которая отображает процесс накопления в текстовом файле символов сообщения, является небезопасной, то есть может принимать любое значение. Это связано с тем, что получатель заранее не знает длину получаемого сообщения.

2. Мощность множества опорных текстов, предназначенных для извлечения символов сообщения является фиксированным.

3. Счётчик неинформативных значений в актуальном номере ISN, должен обнуляться при условии наличия хотя бы одного информативного.

Под информативным, понимается такое значение r, что определено в пределах $0 \le r \le 127$. Под неинформативным понимается такое значение r, что определено в пределах $128 \le r \le 255$. Такие значения используются: в качестве «маркера», при условии отсутствия текущего символа сообщения в очередном блоке из 128 символов опорного текста; при дополнении очередного блока необходимых для вычисления нужного номера ISN до четырёх значений; при обозначении окончания сообщения четырьмя неинформативными значениями.

В соответствии с принципами стеганографической передачи данных, каждому элементу из множества позиций P, соответствует одно из возможных событий, которые могут происходить в исследуемой системе при формировании и отправке стегоконтейнеров. Граф сети Петри, отображающий порядок обработки TCP-соединений для стеганографической передачи данных, изображен на рис.2

p_1 – данная позиция содержит одну фишку в начальной разметке сети, что соответствует непрерывному поступлению символов опорного текста для сравнения с текущим символом сообщения.

p_2 – получен очередной символ из множества символов, содержащихся в сообщении.

p_3 – очередной символ опорного текста не соответствует текущему символу сообщения или не найден при полном переборе в актуальном блоке из 128 символов опорного текста.

p_4 – очередное восьмиразрядное значение поступило в регистр сдвига. В зависимости от того, какой из переходов сработал, может быть информативным или неинформативным.

p_5 – вычислено необходимое значение ISN. Степень данной позиции 4 (4–безопасная позиция). Это говорит о том, что она может принять до четырёх фишек, что соответствует четырём байтам полного номера ISN.

p_6 – выполняется передача последнего символа сообщения. При этом, вводится дополнительное ограничение, которое заключается в том, что из позиции p_6 может сработать только тот переход, для которого позиция p_4 является выходной с кратностью $k = 4 - n$, где n – количество фишек в позиции

p_4 в актуальной разметке сети. Если $n = 0$, то сработать может только переход t_{12}.

Каждому элементу из множества переходов, соответствует одно из возможных условий перехода СГС из входного (входных) в выходное (выходные) состояние.

t_1 – получен очередной символ сообщения для сравнения с множеством символов опорного текста. Данный переход срабатывает один раз, из начальной разметки, и помещает в позицию p_2 одну фишку.

t_2 – текущий символ сообщения и опорного текста соответствуют. При срабатывании, данный переход помещает в позицию p_4 одну фишку, что соответствует поступлению в регистр сдвига информативного значения.

t_3 – если позиция p_4 содержит четыре фишки, то при срабатывании, данный переход помещает в позицию p_5 одну и извлекает из p_4 все фишки. Это соответствует тому, что четыре значения, размещённые в регистре сдвига, преобразуются в 32-разрядный номер ISN.

t_4 – данный переход извлекает из позиции p_5 одну фишку. Это соответствует отправке очередного стегоконтейнера.

t_5 – срабатывает, если текущий символ опорного текста не соответствует текущему символу сообщения и помещает в позицию p_3 одну фишку.

t_6 – извлекает из позиции p_6 и помещает в позицию p_1 одну фишку. Срабатывает, если выбран следующий символ опорного текста для сравнения с текущим символом сообщения.

t_7 – извлекает из позиции p_3 одну фишку и помещает в позиции p_1 и p_4 по одной фишке. Такое событие отображает случай, когда номер (в порядке следования) очередного символа опорного текста достиг значения $(2^7 - 1)$. При этом, в регистр сдвига поступает случайно сгенерированное значение в пределах от 2^7 до $(2^8 - 1)$, а для сравнения поступает первый символ из следующего 128 – символьного блока опорного текста.

t_8 – извлекает из позиции p_2 и помещает в позицию p_6 одну фишку. Это соответствует тому, что символы в сообщении закончились.

t_9, t_{10}, t_{11} – извлекает из позиции p_6 одну и помещает в позицию p_4 $(k_4 - m)$ фишек, где k_4 – степень позиции p_4, m – фактическое количество фишек в позиции p_4. Отображает случай, когда необходимо дополнить 32-разрядный регистр сдвига одним, двумя, тремя 8-разрядным значениями соответственно, случайно сгенерированными в пределах от 2^7 до $(2^8 - 1)$. Данный переход срабатывает только после срабатывания перехода t_8.

t_{12} – срабатывает только после срабатывания переходов t_8 и t_9 (t_{10} или t_{11}). Данный переход извлекает из позиции p_6 и помещает в позицию p_5 по одной фишке. Срабатывание данного перехода соответствует отправке стегоконтейнера, который информирует получателя о том, что сообщение передано полностью.

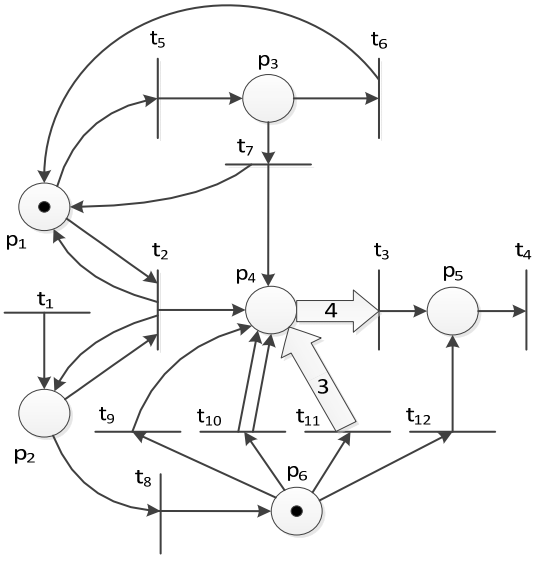

Рис. 2. Граф сети Петри в начальной разметке (формирование СГК и отправка сообщений)

Процесс получения стегоконтейнеров и извлечения сообщения является обратным процессу формирования и отправки стегоконтейнеров, а сеть Петри, соответствующая функционированию системы имеет следующий вид (рис.4).

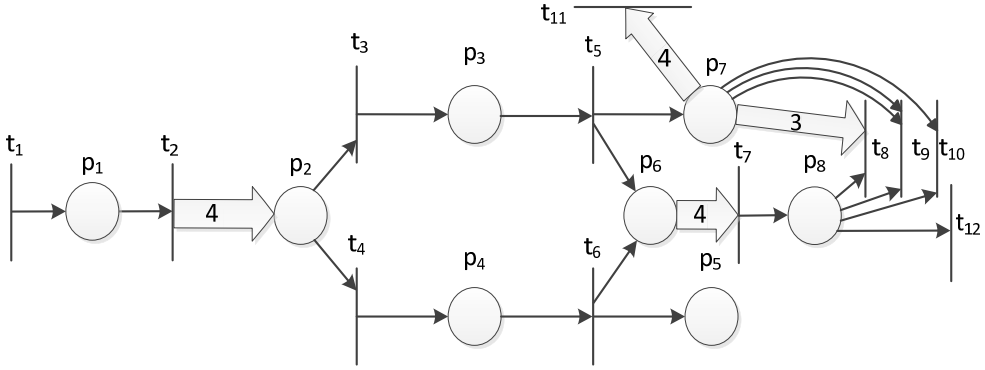

Рис. 3. Граф сети Петри в начальной разметке (приём СГК и восстановление сообщений)

Для данной сети необходимо определить значения позиций и переходов.

Позициям сети соответствуют следующие события, которые могут происходить в исследуемой системе при приёме стегоконтейнеров и восстановлении сообщений.

p_1 – получен очередной стегоконтейнер.

p_2 – на вход регистра сдвига поступил очередной блок из четырёх 8–разрядных значений.

p_3 – очередное значение из блока определено как неинформативное.

p_4 – очередное значение из блока определено как информативное.

p_5 – очередное информативное значение записано в текстовый файл.

p_6 – производится подсчёт обработанных значений. Данное событие необходимо для фиксации момента окончания обработки номера ISN очередного стегоконтейнера.

p_7 – производится подсчёт неинформативных значений. При поступлении четвёртой фишки в позицию p_7, соответствует приёму четырёх подряд неинформативных значений, что говорит об окончании символов в принимаемом по стеганографическому каналу сообщении.

p_8 – при условии обработки четырёх значений, полученных из номера ISN, обеспечивает обнуление счётчика неинформативных значений, при условии, что его значение менее четырёх.

Переходы сети определяют причинно-следственные связи между событиями. Им соответствуют следующие условия перемещения фишек из входной (входных) в выходную (выходные) для перехода позицию (позиции).

t_1 – срабатывание данного перехода соответствует факту поступления на вход системы очередного стегоконтейнера.

t_2 – соответствует выполнению условия для перехода системы в состояние p_2. Соответствует получению очередного блока из четырёх необходимых для восстановления сообщения значений.

t_3 – установлен факт того, что очередное значение в текущем блоке является неинформативным.

t_4 – установлен факт того, что очередное значение в текущем блоке является информативным.

t_5 – данный переход соответствует подсчёту неинформативных значений в пределах очередного блока из четырёх полученных из номера ISN значений.

t_6 – условие, обеспечивающее накопление фишек в позиции p_5. Соответствует условию поступления информативных значений в текстовый файл.

t_7 – обеспечивает обнуление счётчика обработанных значений при условии, что их количество не меньше четырёх в очередном блоке обрабатываемых значений.

t_8 – условие для обнуления счётчика неинформативных значений, при том, что их три из четырёх в очередном блоке.

t_9 – условие для обнуления счётчика неинформативных значений, при том, что их два из четырёх значений в очередном блоке.

t_{10} – условие для обнуления счётчика неинформативных значений, при том, что оно одно из четырёх значений в очередном блоке.

t_{11} – условие для обнуления счётчика неинформативных значений. Данный переход изымает из позиции p_8 одну фишку и необходим для фиксации момента окончания выполнения графа сети;

t_{12} – условие, выполнение которого, изымает одну фишку из позиции p_8.

Выводы

Предложенная модель обладает всеми свойствами разрабатываемой стеганографической системы. Это позволило детально изучить и учесть все особенности функционирования СГС в динамике.

Описана возможность функциональной декомпозиции полного цикла передачи одного сообщения на три этапа: формирование

стегоконтейнеров и отправки сообщения, передача стегоконтейнеров в общедоступной глобальной сети, приём стегоконтейнеров и восстановление сообщения. Наличие такой возможности позволяет сделать вывод о том, что для стороннего наблюдателя функционирование разрабатываемой стеганографической системы не внесёт временных задержек в функционирование протокола TCP, как сигнатуры для принятия решения о наличии скрытного канала передачи данных в пределах анализируемого виртуального соединения.

Исходя из полученных сведений о разрабатываемой стеганографической системе, продолжением исследований является получение алгоритма и программная реализация обработки TCP – соединений для скрытной передачи данных в ИТКС.

Литература

1. Рубан И.В. An approach to cyber security support / И. В. Рубан // Системи обробки інформації. – 2015. – № 11 (136). – С. 6–8. **2. Орлов В. П.** Методы скрытой передачи информации в телекоммуникационных сетях: дис. кандидата технических наук: 05.12.13 / Орлов Владимир Владимирович. – Самара, 2012. – 166 с. **3. Рубан И. В.** Метод стеганографической передачи данных в информационно-телекоммуникационных сетях на основе генерации ISN tcp-соединений / И. В. Рубан, А. О. Смирнов // Системи обробки інформації. – Харків: ХУПС, 2015. – № 9 (134). – С. 99–101. **4. "Internet** protocol - DARPA Internet Program Protocol Specification" RFC-793. TCP. USC / Information Sciences Institute, September 1981 [Electr. resource]. – Accessed to: https://www.rfc-editor.org/rfc/rfc793.txt. **5. Питерсон Дж.** Теория сетей Петри и моделирование систем: Перевод с английского. – М. : Мир, 1984. – 264 с.

МОДЕЛЬ ОБРОБКИ TCP-З'ЄДНАНЬ ДЛЯ СТЕГАНОГРАФІЧНОЇ ПЕРЕДАЧІ ДАНИХ В ІНФОРМАЦІЙНО-ТЕЛЕКОММУНІКАЦІЙНИХ МЕРЕЖАХ

***[1]Ігор Вікторович Рубан** (д-р техн. наук, професор)*
[2]Антон Олександрович Смірнов

[1]Харківський національний університет радіоелектроніки, Харків, Україна
[2]Хурківський університет Повітряних Сил імені І. Кожедуба, Харків, Україна

У даній статті запропонована модель обробки TCP-з'єднань для стеганографічної передачі даних в інформаційно-телекомунікаційних мережах. Визначено вимоги до модифікації протоколу TCP для коректної роботи стеганографічної системи. Обгрунтовано факт відсутності тимчасових затримок у функціонуванні модифікованого TCP по відношенню до його стандартних версій.

***Ключові слова:** мережева стеганографія; стегоконтейнер; початковий номер послідовності.*

THE TCP-CONNECTIONS PROCESSING MODEL FOR STEGANOGRAPHIC DATA TRANSFER IN INFORMATION TELECOMMUNICATION NETWORKS

***[1]Ihor V. Ruban** (Doctor of Technical Sciences, Professor)*
[2]Anton O. Smirnov

[1]Kharkiv National University of Radio Electronics , Kharkiv, Ukraine
[2]Kharkiv University of Air Forces, Kharkiv, Ukraine

The model of TCP-connections processing for steganographic data transfer in information-telecommunication networks has been proposed in this article. The requirements for the modification of the TCP for correct working of the steganographic system has been defined. The functioning of steganographic system when forming and sending of steganographic containers, receiving and extracting of messages has been considered in details. The notions of informative and uninformative values, which calculated during of search of correlations the symbols of open-text (the payload of TCP) with the symbols of the message has been introduced. The model includes blind marking, the implementation of which corresponds to the end of the process of sending (receiving) messages. Justified the lack of time delays in the functioning of the modified TCP relative to its standard version.

***Keywords:** network steganography; steganographic container; initial sequence number.*

References

1. Ruban I.V. (2015), An approach to cyber security support. Systemy obrobky informatsii, No. 11 (136), pp. 6–8. **2. Orlov V.P.** (2012), Methods for secure data transmission in telecommunication networks: dissertation [*Metodyi skryitov peredachi informatsii v telekommunikatsionnyih setyah*: *dis*. *kand. techn. nauk*], Samara, 166 p. **3. Ruban I.V.,** Smirnov A.A. (2015), The method of steganographic data transfer in information telecommunication networks based on the generation of ISN of tcp-connections. [*Metod steganograficheskoy peredachi dannyih v informatsionno-telekommunikatsionnyih setyah na osnove generatsii ISN tcp-soedineniy*], Systemy obrobky informatsii, No. 9 (134), pp. 99–101. **4. "Internet** protocol - DARPA Internet Program Protocol Specification. RFC-793. TCP. USC / Information Sciences Institute, September 1981", available at: https://www.rfc-editor.org/rfc/rfc793.txt. **5. James L. Peterson** (1984), Petri Net Theory and the Modeling of Systems: translation from English. [*Teoriya setey Petri i modelirovanie sistem: Perevod s angliyskogo*], Mir, Moscow, 264 p.

Отримано: 25.09.2015 року