Модель системы обнаружения вторжений в радиоканал управления робототехническим комплексом

С. А. Матвеев
Военно-космическая академия имени А.Ф. Можайского
serg15332m@yandex.ru

***Аннотация*. Предложен подход к процессу обнаружения вторжений, основанный на использовании временных раскрашенных сетей Петри, представлена модель многоуровневой системы обнаружения вторжений в радиоканал управления робототехническим комплексом.**

Ключевые слова: многоуровневая система обнаружения вторжений; врменные раскрашенные сети Петри; робототехнический комплекс; радиоканал управления

I. Инофомационная безопасность радиоканала управления робототехническим комплексом

В связи с увеличением сложности решаемых задач и высокими требованиями к качеству их выполнения, в настоящее время во всех областях человеческой деятельности широкое применение находят робототехнические комплексы, управление и передача данных в которых осуществляется по радиоканалам связи [1]. Характерная особенность любого радиоканала заключается в пространственной электромагнитной доступности, которая создает условия для осуществления деструктивных воздействий нарушителя к циркулируемой в ней информации [2]. Исходя из этого, к радиоканалам предъявляются высокие требования по обеспечению информационной безопасности.

Обеспечение информационной безопасности радиоканала связи осуществляется с помощью систем обнаружения вторжений (СОВ), которые представляет собой программное или программно-аппаратные средства, предназначенные для выявления фактов неавторизованного доступа либо несанкционированного управления ими в компьютерных сетях [3, 4].

Однако, для обеспечения безопасности радиоканала управления робототехническим комплексом (РК) данные системы в настоящее время не используются. Цель статьи заключается в том, чтобы показать возможность применения и функционирования многоуровневой СОВ для обнаружения вторжений в радиоканал управления РК.

Процесс обнаружения вторжений в радиоканал управления РК представляет собой блокирование имитируемой злоумышленником ложного управляющего сообщения. Следовательно, данный процесс является достаточно сложным антагонистическим процессом, для описания которого необходимо математическое моделирование. Наиболее универсальным способом является использование временных раскрашенных сетей Петри [5].

Универсальной моделирующей системой, основанной на использование временных раскрашенных сетей Петри, является программный продукт *CPN Tools*, который имеет свободное распространение.

II. Моделирование обнаружения вторжений в радиоканал управления робототехническим комплексом в программном продукте *CPN TOOLS*

Рассмотрим модель обнаружения вторжений в радиоканал управления РК, реализованную в программном продукте *CPN Tools*. Описание осуществляется на основе графического представления временными раскрашенными сетями Петри и специального языка программирования *CPN ML* [6].

На рис. 1 представлена многоуровневая модель СОВ в радиоканал управления РК на основе временных раскрашенных сетей Петри в программном продукте *CPN Tools* [7, 8].

Методологической основой для разработки многоуровневой СОВ является Эталонная модель взаимодействия открытых систем (ЭМВОС). ЭМВОС лежит в основе современных технологий информационно-телекоммуникационных систем [9].

В представленной модели предлагается последовательный анализ признаков обнаружения вторжений в радиоканал управления РК на 4 уровнях: физическом, канальном, представления и прикладном. Каждому уровню функционирования СОВ соответствует свой признак обнаружения вторжений в радиоканал управления РК и соответствующее решение, обеспечивающее выполнение функций по обнаружению и блокированию ложного управляющего сообщения.

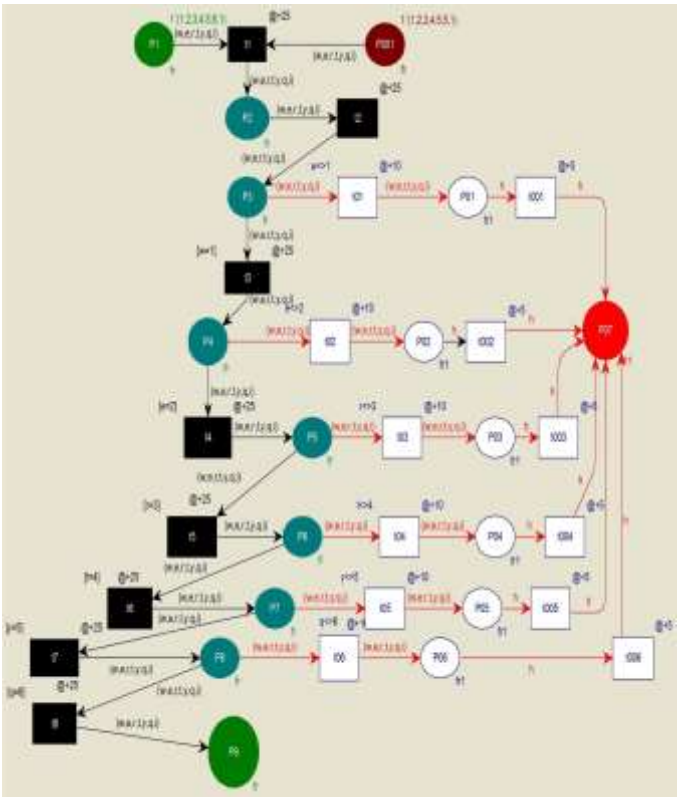

Рис. 1. Модель многоуровневой системы обнаружения вторжений в радиоканал управления робототехническим комплексом

Теоретико-графовым представлением временных раскрашенных сетей Петри является двудольный ориентированный мультиграф, в котором позициям соответствуют вершины, изображаемые кружками, а переходам – вершины, изображаемые утолщенными линиями; функциям I соответствуют дуги, направленные от позиций к переходам, а функциям O – дуги, направленные от переходов к позициям.

На графе позиции и переходы представлены следующим образом:

$P1$ Передача управляющего сообщения легитимным пользователем РК;

$P001$ Передача ложного управляющего сообщения злоумышленником;

$P2$ Обнаружение и захват радиосигнала частотой F бортовой аппаратурой РК;

$P3$ Оценка принятой и ожидаемой частоты радиосигнала

$P4$ Декодирование;

$P5$ Аутентификация;

$P6$ Контроль текущего технического состояния (ТТС) бортовой аппаратуры РК;

$P7$ Контроль логики управления РК;

$P8$ Контроль выполнения текущих целевых задач РК;

$P9$ Выполнение принятого управляющего сообщения;

$P01$, $P02$, $P03$, $P04$, $P05$, $P06$ Блокирование выполнения принятого управляющего сообщения на соответствующих уровнях;

$P07$ Регистрация попытки вторжения;

$t1$ Загрузка альманаха признаков попыток вторжения;

$t2$ Активация системы обнаружения попыток вторжения;

$t3$ Отклонение принятой частоты радиосигнала не обнаружено;

$t4$ Ошибки в результате декодирования не превысили установленного порога

$t5$ Аутентификация выполнена;

$t6$ Нарушение ТТС РК не обнаружено;

$t7$ Нарушение логики управления не обнаружено;

$t8$ Нарушение выполнения текущих целевых задач не обнаружено;

$t01$ Обнаружено отклонение принятой частоты радиосигнала;

$t001$ Отправка признака «отклонение принятой частоты» о попытке вторжения;

$t02$ Обнаружено превышение установленного порога ошибок при декодировании

$t002$ Отправка признака «превышение установленного порога ошибок»;

$t03$ Аутентификация не пройдена;

$t003$ Отправка признака «ошибка аутентификация»;

$t04$ Обнаружено нарушение ТТС;

$t004$ Отправка признака вторжения «нарушение ТТС»;

$t05$ Обнаружено нарушение логики управления;

$t005$ Отправка признака «нарушение логики управления»;

$t06$ Обнаружено нарушение выполнения текущих целевых задач;

$t006$ Отправка признака «нарушение выполнения текущих целевых задач».

В представленной модели многоуровневой СОВ в радиоканал управления РК позиции и переходы соответствуют следующим уровням обнаружения:

1. $P3$, $t3$, $t01$, $t001$ - физическому;
2. $P4$, $P5$, $t02$, $t03$, $t002$, $t003$ - канальному;
3. $P6$, $t04$, $t004$ - представления;
4. $P6$, $P7$, $t05$, $t06$, $t005$, $t006$ - логическому.

Распределение меток по позициям называют маркировкой. Метки – это примитивное понятие сетей Петри, они присваиваются позициям и могут перемещаться в сети.

Обозначим четверкой $<P, T, I, O>$, где P и T – конечные множества позиций и переходов, I и O – множества входных и выходных функций. Входная функция I отображает переход t_j в множество позиций $I(t_j)$, называемых входными позициями перехода. Выходная функция O отображает переход t_j в множество позиций $O(t_j)$, называемых выходными позициями перехода.

К статистическим свойствам временных раскрашенных сетей Петри относятся: конечное множество позиций, конечное множество состояний, множество входных позиций переходов, множество выходных позиций переходов, начальная маркировка.

Начальная маркировка:

$\mu_0 = \{1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0\}$.

Множество входных позиций переходов

$I = \{I(t_1), I(t_2), I(t_3), I(t_4), I(t_5), I(t_6), I(t_7), I(t_8), I(t_{01}), I(t_{02}), I(t_{03}), I(t_{04}), I(t_{05}), I(t_{06}), I(t_{001}), I(t_{002}), I(t_{003}), I(t_{004}), I(t_{005}), I(t_{006})\}$.

$I(t_1)=\{p_1\}$, $I(t_2)=\{p_2\}$, $I(t_3)=\{p_3\}$, $I(t_4)=\{p_4\}$, $I(t_5)=\{p_5\}$, $I(t_6)=\{p_6\}$, $I(t_7)=\{p_8\}$, $I(t_8)=\{p_9\}$.

Множество выходных позиций переходов

$O = \{O(t_{01}), O(t_{02}), O(t_{03}), O(t_{04}), O(t_{05}), O(t_{06}), O(t_{07}), O(t_{08}), O(t_{01}), O(t_{02}), O(t_{03}), O(t_{04}), O(t_{05}), O(t_{06}), O(t_{001}), O(t_{002}), O(t_{003}), O(t_{004}), O(t_{005}), O(t_{006}\}$.

$O(t_1)=\{p_2\}$, $O(t_2)=\{p_3\}$, $O(t_3)=\{p_4\}$, $O(t_4)=\{p_5\}$, $O(t_5)=\{p_6\}$, $O(t_7)=\{p_8\}$, $O(t_8)=\{p_9\}$, $O(t_{01})=\{p_{01}\}$, $O(t_{001})=\{p_{07}\}$, $O(t_{02})=\{p_{02}\}$, $O(t_{002})=\{p_{07}\}$, $O(t_{03})=\{p_{03}\}$, $O(t_{003})=\{p_{07}\}$, $O(t_{04})=\{p_{04}\}$, $O(t_{004})=\{p_{07}\}$, $O(t_{05})=\{p_{05}\}$, $O(t_{005})=\{p_{07}\}$, $O(t_{06})=\{p_{06}\}$, $O(t_{006})=\{p_{07}\}$.

Конечное множество позиций переходов

$P= \{p_{001}, p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8, p_9, p_{01}, p_{02}, p_{03}, p_{04}, p_{05}, p_{06}, p_{07}\}$.

Для оценки вероятностно-временных характеристик функционирования многоуровневой СОВ зададим начальное время передачи по радиоканалу и выполнение управляющего сообщения легитимным пользователем РК равным 30 секунд.

Так как в программном продукте *CPN Tools* время представляется в виде целого числа, а в реальности оно непрерывно, для установления взаимосвязи между значениями модельного времени и их реальными эквивалентами воспользуемся следующей методикой: некоторому интервалу реального времени (1 секунда) соответствует количество тактов модельного времени равное 10. Если время доведения и выполнения управляющего сообщения равно 30 секунд, то в модели оно будет длиться 300 тактов модельного времени.

Таким образом, для всех действий в представленной модели многоуровневой СОВ установлены временные задержки, обозначенные @+10, где цифра обозначает такт модельного времени для соответствующего перехода.

На рис. 2 представлен фрагмент пространства сильно связанных состояний в программном продукте *CPN Tools* модели многоуровневой системы обнаружения вторжений в радиоканал управления РК, который определяет все достижимые маркировки временной раскрашенной сети Петри, а также все возможные последовательности запусков её переходов.

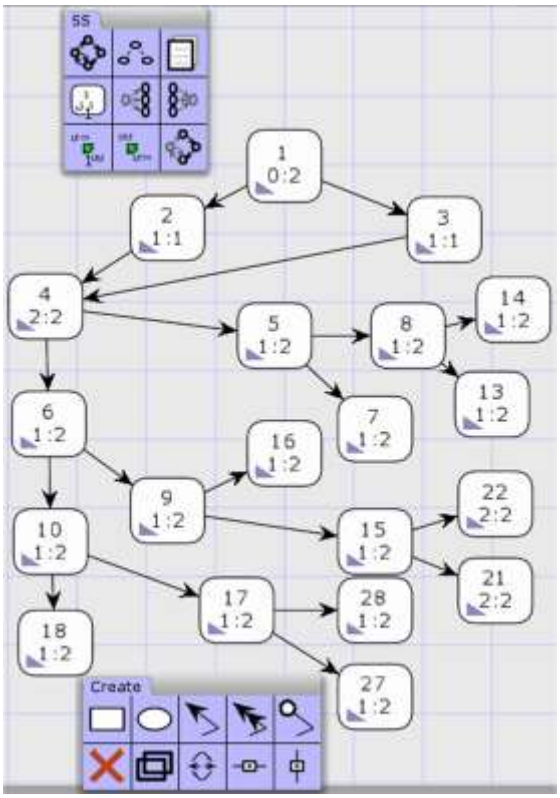

Рис. 2. Фрагмент пространства сильно связанных состояний модели многоуровневой системы обнаружения вторжений в радиоканал управления робототехническим комплексом

Шаг построения пространства сильно связанных состояний состоит в добавлении к каждой граничной вершине – маркировке веера, образованного множеством всех маркировок, непосредственно достижимых из данной граничной маркировки. На первом шаге граничной является вершина, соответствующая начальной маркировке. Каждая дуга помечена запускаемым переходом, при переходе из одной маркировки в другую. Всякий путь в пространстве сильно связанных состояний, начинающийся в корне, соответствует допустимой последовательности переходов

В результате моделирования процесса обнаружения вторжений в радиоканал управления РК, получены вероятностно-временные характеристики функционирования многоуровневой СОВ, представленные в таблице.

ТАБЛИЦА I ВЕРОЯТНОСТНО-ВРЕМЕННЫЕ ХАРАКТЕРИСТИКИ ФУНКЦИОНИРОВАНИЯ МНОГОУРОВНЕВОЙ СОВ

T_i	P	t, c
T1	0,25	0,69
T2	0,25	0,69
T3	0,25	0,69
T4	0,82	0,74
T5	0,18	0,74
T6	0,21	1,35
T7	0.22	1,35
T8	1	0,17
T01	0,79	0,83
T02	0,12	0,75
T03	0,12	0,79
T04	0,76	0,79
T05	0,5	0,75
T06	0,5	0,75
T001	0,27	0,83
T002	0,27	0,83
T003	0,31	1,35
T004	0,38	1,35
T005	0,31	3,32
T006	1	3,32

В данном случае цель состоит в том, чтобы показать совокупность уровней и наличие признаков, необходимых для успешного обнаружения вторжений в радиоканал управления РК. Если эти признаки выявлены, то можно говорить о том, что вторжение обнаружено. Однако если их нет, или они присутствуют частично, то можно говорить о том, что вторжение отсутствует, либо присутствует с некоторой долей вероятности соответственно.

В процессе функционирования разработанная модель многоуровневой СОВ может находиться только в одном из множества состояний, для которого с определенной долей вероятности можно определить наличие или отсутствие вторжения в радиоканал управления РК.

Таким образом, представление многоуровневой СОВ в виде временной раскрашенной сети Петри и последующего анализа этой сети позволяет получить информацию о структуре и динамическом поведении моделируемой системы. Данная информация может использоваться для оценки моделируемой системы и выработки предложений по ее усовершенствованию.

Разработанная модель многоуровневой СОВ на основе аппарата временных раскрашенных сетей Петри, позволяет осуществить всестороннее моделирование процесса обнаружения вторжений в радиоканал управления РК на одном из четырех уровнях по наличие соответствующих признаков.

СПИСОК ЛИТЕРАТУРЫ

[1] Спутниковая связь и вещание. Справ. / Под ред. Л.Я Кантора. М.: Радио и связь, 1997. 528 с.

[2] Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. М.: Горячая линия–Телеком, 2004. 280 с.

[3] Устинов Г.Н. Основы информационной безопасности систем и сетей передачи данных. М.: СИНТЕГ, 2000. 248 с.

[4] Мальцев Г.Н., Лесняк Д.А. Применение стратегий поддержания защищенности в информационных системах // Информационно-управляющие системы. 2017. №3 (88). С.67–74.

[5] Питерсон Дж. Теория сетей Петри и моделирование систем /пер. с англ. М.: Мир, 1984. 264 с.

[6] Зайцев Д.А., Шмелева Т.Р. Моделирование телекоммуникационных систем в CPN Tools. Одесса, 2008. 68 с.

[7] Лесняк Д.А., Матвеев С.А. Моделирование комплекса средств защиты информации радиоканалов временными раскрашенными сетями Петри // Труды 75-ой научно-технической конференции. 2020. №1 (75). С.127–131.

[8] Свидетельство о государственной регистрации ПЭВМ № 2020662710 Программа для моделирования бортовой системы обнаружения вторжений в радиоканал управления робототехническим комплексом / С.А. Матвеев, Г.Н. Мальцев, Д.А. Лесняк. М.:ФИПС, 2020.

[9] Куприянов А.И., Макаров В.Ф. Защита информации в телекоммуникационных системах: учебное пособие. М: Вузовская книга, 2017. 158 с.