VECTOR OPTIMIZATION PROBLEM OF HEURISTIC IDS / IPS

Gusnin S.[1], Petukhov A.[2]

ЗАДАЧА ВЕКТОРНОЙ ОПТИМИЗАЦИИ ЭВРИСТИК IDS / IPS

Гуснин С. Ю.[1], Петухов А. Н.[2]

[1]Гуснин Сергей Юрьевич / Gusnin Sergey – кандидат технических наук, доцент,
кафедра информационных и сетевых технологий,
Институт информационных систем и технологий;
[2]Петухов Андрей Николаевич / Petukhov Andrey – кандидат технических наук, доцент,
кафедра информационной безопасности,
Московский институт электронной техники
Национальный исследовательский университет, г. Москва

Аннотация: *в статье анализируется текущая ситуации с переходом от первоначального использования преимущественно сигнатурных методов к все более расширяющемуся привлечению эвристических решений в средствах обнаружения/предотвращения вторжений (IDS/IPS). Возникающая при этом неопределенность порождает ошибки в виде ложных реакций. Рассмотрены возможные постановки задачи векторной оптимизации эвристики обнаружения вторжений. Показано, что формулировка последней задачи свободна от ограничений, присущих задачам, сформулированным ранее, и поэтому такая задача может называться задачей векторной оптимизации эвристик.*

Abstract: *the article analyzes the current state of the transition in the instruments of intrusion detection / prevention systems (IDS / IPS) from the initial use mainly on signatures based methods to more and more expanding involvement of heuristic decisions. A result of this uncertainty causes an error in the form of false positives. The possibility of creating a vector optimization problem of intrusion detection is considered. It is shown that the wording of the latter problem is free from the limitations of the problems outlined above, and therefore, this problem can be called the problem of vector optimization heuristics.*

Ключевые слова: *информационная безопасность, (IDS/IPS), эвристические решения, векторная оптимизация, политика безопасности.*

Keywords: *information security, (IDS / IPS), heuristic solutions, vector optimization, security policy.*

Средства (системы) обнаружения/предотвращения вторжений (IDS/IPS) уже давно занимают свое место в арсенале признанных средств сетевой безопасности. Одним из направлений современного развития этого сервиса является переход от первоначального использования преимущественно сигнатурных методов к все более расширяющемуся привлечению эвристических решений. Наряду с неоспоримой привлекательностью этого подхода (прогнозирование угрозы, оценка степени опасности трафика и сетевой ситуации, фиксация косвенных проявлений опасности и т. п.), анализ результатов работы эвристик позволяет установить в них некоторую долю ошибочных результатов. Причина возникновения такого дефекта состоит в том, что в отличие от сигнатурных методов при создании эвристики фактически моделируется возможное развитие наблюдаемой сетевой ситуации. Поскольку, в зависимости от факторов, не учитываемых эвристикой, таких развитий может быть много, возникающая неопределенность порождает ошибки в виде ложных реакций.

Как и во многих случаях принятия решений в условиях неопределенности, ошибки могут быть разного рода. Хотя современные IDS/IPS используют целый спектр возможных реакций, для дальнейшего обсуждения достаточно будет рассмотреть случай с двумя видами реакции: «ситуация опасна» и «опасности нет». Термин «ложное позитивное срабатывание» чаще всего используется для обозначения реакции, предупреждающей об опасности в то время когда этой опасности реально нет. Если исключить дефекты алгоритма или ошибки анализа, то это происходит в случае, когда подозрительные намерения не были злоумышленными, ситуация не относится к сегменту, который контролируется или даже когда атака не увенчалась успехом. Термин «ложное негативное событие» используется для случаев, когда эвристика не замечает реальную атаку или опасную ситуацию [1].

Интенсивности ложных срабатываний (ошибок) каждого вида можно характеризовать нормированными характеристиками, отражающими долю ошибочных реакций или вероятность их возникновения. Конкретный вид таких критериев качества эвристики не столь важен, как важна их множественность (в нашем случае их два, обозначим их k_1 и k_2) и то, что они не являются независимыми. Действительно, предпринимая меры по улучшению значений одного из них, мы рано или поздно столкнемся с необходимостью жертвовать другим. Повышая уровень «осторожности» эвристики мы вынуждены допускать одновременное увеличение «шума», т. е. ухудшения критерия k_1, а стремясь исключить такой «шум», идем на риск пропуска реальной опасности, снижая качество по критерию k_2. Таким образом, для того, чтобы оптимизируя качество эвристики, необходимо идти на компромисс,

используя некоторые принципы и правила, которые получили название схемы компромисса [2] и должны определяться соответствующими политиками безопасности. Инженерная практика накопила обширный опыт применения различных схем компромисса (приоритеты, весовые коэффициенты, производные критерии и многое другое [3]), объединив его термином векторной (множественность критериев) оптимизации. Нашей целью будет рассмотрение возможных формулировок задачи векторной оптимизации эвристик обнаружения вторжений.

Введем следующие обозначения:

A_i – эвристика, правило, в соответствии с которым в любой ситуации определяется реакция, отображение множества ситуаций на множество реакций;

r(Ai,▪i) ▪ {k1,k2} – решение эвристики, значение векторного критерия, обеспечиваемого эвристикой A_i;

□$_i$ – вектор параметров эвристики A_i, ▪i ▪ {▪i1,▪i2,... ▪isi}, в общем случае изменение значений этих параметром приводит к изменению решения эвристики;

$R(A_i)$ - область допустимой эффективности эвристики A_i, множество всевозможных значений, которые принимает решение эвристики при изменении □$_i$;

w_j - схема компромисса, правило определения преимущественности одного решения перед другими;

R - множество всевозможных решений различных эвристик, в общем случае составляет собственное подмножество единичного квадрата на плоскости с координатами k_1 и k;

В соответствии с общей методологией векторной оптимизации область допустимой эффективности $R(A_i)$ делится на область согласия, в которой улучшения возможны сразу по всем критериям $R^c(A_i)$ и область компромиссов (область Парето) $R^k(A_i)$:

$$R^c(A_i) ▪ R^k(A_i) = ▪ R^c(A_i) ▪ R^k(A_i) = R(A_i) \qquad (1)$$

Выделенная область компромиссов $R^k(A_i)$ определяется эвристикой, поэтому будем называть $R^k(A_i)$ условной областью компромиссов.

Рассмотрим возможные постановки задачи векторной оптимизации эвристики обнаружения вторжений.

Задача 1. Задана эвристика A_i, и на основании содержательного анализа политики безопасности определена схема компромисса w_j. Для некоторых схем компромисса оптимальное решение не является единственным [4], поэтому в общем случае необходимо говорить об области оптимальных решений:

$$R_{opt}(w_j, A_i) ▪ R^k(A_i) \qquad (2)$$

Решение поставленной задачи поставленной задачи заключается в определении компонент, для которых выполняется условие:

$$r(A_i,▪▪_i) ▪ R_{opt}(w_j, A_i) \qquad (3)$$

Задача оптимизации в приведенной формулировке не является общей, т. к. в ней рассматривается единственная эвристика.

Задача 2. Задано некоторое множество эвристик $\{A_i\}$ и схема компромисса w_i. В силу транзитивности отношения квазипорядка эта задача сводится к многократному решению предыдущей и выбору эвристики с наилучшим в смысле w_j оптимальным решением. Другими словами, задача с такими условиями решается путем последовательного выполнения следующих этапов:

- определяется условная область компромиссов $R^k(A_i)$ для каждой эвристики A_i из заданного множества $\{A_i\}$;
- объединение условных областей рассматривается как новая область допустимой эффективности и в ней определяются область компромиссов и область согласия:

$$R^c ▪ R^k = ▪ R^k(A_i) \qquad (4)$$

- в полученной области компромиссов R^k ищется (в смысле заданной схемы компромисса w_i) область оптимальных решений $R_{opt}(w_j, \{A_i\})$.
- из заданного множества эвристик выделяются те, для которых пересечение области допустимой эффективности и найденной области оптимальных решений непусто:

$$R(A_i) ▪▪ R_{opt}(w_j, \{A_i\}) \neq ▪▪▪▪ \qquad (5)$$

- для выделенных эвристик определяются значения векторов параметров □$_i$, которые должны обеспечивать наполнение условия:

$$r(A_i,) ▪▪, \{A_i\}) \qquad (6)$$

Решение поставленной задачи лишь частично снимает ограничения на выбор оптимального решения, т. к. не гарантируется невозможность существования эвристики более эффективной по сравнению с эвристиками из $\{A_i\}$ одновременно в смысле обоих критериев. Ограниченность эффективности, принципиально достижимой с помощью эвристик, входящих в состав $\{A_i\}$, находит свое выражение в виде области компромиссов R^k, которая, естественно, зависит от выбора $\{A_i\}$.

Анализ факторов, порождающих неоднозначности интерпретации политик безопасности, показывает, что существуют ограничения эффективности, независящие от используемых эвристик, и определяемые этими факторами, а точнее степенью вносимой ими неопределенности. Снять эту энтропию нельзя подбором эвристики, т. к. эти ограничения соответствуют уровню наших знаний (характеризуют степень «незнания») о реально вредоносных ситуациях и находят свое отражение в виде некоторой "предельной" области компромиссов R^k_0, которую правомерно назвать безусловной областью компромиссов:

$$R^k_0 \cdot\cdot R \qquad (7)$$

Безусловная область компромиссов R^k_0 характеризуется тем, что никакая эвристика не может обеспечить эффективность более высокую по двум критериям одновременно, чем та, которая соответствует некоторой точке r_0 из области R^k_0.

Задача 3. Определена область R^k_0, задано допустимое для использования множество эвристик$\{A_i\}$ и выбрана схема компромисса w_i. Решение задачи с такими условиями аналогично решению предыдущей за исключением двух первых этапов. Сначала в безусловной области компромиссов R^k_0 выделяется область оптимальных решений R_{opt} (w_i.). Затем из множества эвристик $\{A_i\}$ выделяется те, для которых справедливо условие:

$$R(A_i) \cdot\cdot R_{opt}(w_j) \neq \cdot\cdot\cdot\cdot \qquad (8)$$

И для них определяются значения $\cdot_i$, соответствующие оптимальным решениям.

В предыдущей задаче было гарантировано существование эвристик из $\{A_i\}$, которые реализуют оптимальную индикацию вторжения, т. к. объединение условных областей компромисса состояло из точек областей допустимой эффективности. В поставленной задаче такой гарантии нет, и поэтому она может не иметь решения. Устранить это обстоятельство можно путем включения в задачу оптимизации требования разработки новой эвристики с заданными свойствами.

Задача 4. Как и в предыдущей задаче, определена безусловная область компромиссов R^k_0 и выбрана схема компромисса w_i. Требуемым свойством разрабатываемой эвристики A_0 является справедливость для нее следующего условия:

$$R(A_0) \cdot\cdot R_{opt}(w_j) \neq \cdot\cdot\cdot\cdot \qquad (9)$$

При этом R_{opt} (w_j) определяется на безусловной области компромиссов. После разработки такой эвристики остается найти для нее соответствующие значения вектора параметров.

В поставленной задаче результат разработки эвристики зависит от выбранной схемы компромисса w_j. Выбор такой схемы основан на содержательном анализе конкретной реальной ситуации (политик безопасности) и выполняется неформальными методами, что снижает возможности распространения принимаемых решений, т. е. одна и та же эвристика в условиях различных политик может иметь разную эффективность. Сформулируем задачу, свободную от этого недостатка.

Задача 5. Определена безусловная область компромиссов R^k_0.Требуется разработать эвристику A_0, позволяющую проводить оптимизацию в этой области по любой схеме компромисса. Это эквивалентно выполнению условия:

$$R^k_0 \cdot\cdot R(A_0) \qquad (10)$$

Для этой эвристики R^k_0 совпадает с условной областью компромиссов $R^k(A_0)$, и она обязательно является параметрической, т. е. вектор параметров $\square_i$ имеет размерность, отличную от нуля. После разработки такой эвристики, необходимо разделить область допустимой эффективности $R(A_0)$ на области согласия $R^c(A_0)$ и компромиссов $R^k(A_0) = R^k_0$ в найти значения вектора $\square_0$, соответствующие оптимальным решениям в смысле каких-либо конкретных схем компромисса.

На практике разделение $R(A_0)$ на $R^c(A_0)$ и $R^k(A_0)$ в общем случае требует предварительного определения безусловной области компромиссов R^k_0, что может быть сопряжено со значительными методическими и ресурсными трудностями. Поэтому, привлекательными становятся постановка и решение следующей задачи.

Задача 6. Необходимо разработать эвристику A_0, каждое решение которой является оптимальным в смысле какой-либо схема компромисса. Для такой эвристики должно выполняться условие:

$$R^k_0 = R(A_0) \qquad (11)$$

В силу определения безусловной области компромиссов для эвристики A_0 справедливо утверждение, что оптимальные решения в смысле любой схемы компромисса w_j могут быть получены в результате выполнения эвристики A_0 при соответствующих значениях вектора параметров $\square_0$. Другими словами, эвристика A_0 оптимальна в любом смысле, и все решения, которые A_0 не обеспечивает, хуже решений из его области допустимой эффективности $R(A_0)$, по крайней мере, по одному из скалярных критериев.

Следует заметить, что реализация условий, сформулированных в двух последних задачах, еще не приводит к получению оптимального в традиционном смысле решения эвристики индикации вторжения (если R^k_0 содержит более одного элемента) и не устраняет необходимости выбора конкретной схемы компромисса. Гарантируется лишь возможность достижения с помощью эвристики A_0 оптимальных решений в смысле произвольной схемы компромисса. Тем не менее, формулировка последней задачи

свободна от ограничений, присущих задачам, сформулированным ранее, и поэтому такая задача может называться задачей векторной оптимизации эвристик.

Литература

1. *Большев А. К.* Алгоритмы преобразования и классификации трафика для обнаружения вторжений в компьютерные сети // «ЛЭТИ» им. В. И. Ульянова (Ленина) Санкт-Петербург, 2011.
2. *Злочевский С. И.* Информационное обеспечение в науке // Наукова думка, Киев, 1981.
3. *Емельянов С. В. и др.* Модели и методы векторной оптимизации // Сб. Итоги науки и техники, сер. Техническая кибернетика. Т. 5, 1973.
4. *Красненкер А. С.* Задачи и методы векторной оптимизации // Измерения, контроль, автоматизация. Вып. 1 (3), 1985.