Захист інформації та кібернетична безпека

УДК 004.724 DOI: 10.30748/soi.2017.151.14

Н.В. Борисова, Л.В. Шабанова-Кушнаренко

Национальный технический университет "ХПИ", Украина, Харьков

ГИБРИДНЫЕ СИСТЕМЫ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ СЕТЕЙ

В статье рассматриваются два различных метода решения децентрализованного частично наблюдаемого процесса принятия решений Маркова (decentralized partially observable Markov decision process, DEC-POMDP) на основе политик. В отличие от традиционных подходов, основанных на политике, итерация политики (policy iteration, PI) не используется в наших методах для поиска оптимальной политики. В частности, предлагаемый алгоритм на основе нелинейного программирования (nonlinear programming, NLP) устанавливает новое направление – внедрение методов решения NLP в оптимизацию средних POMDP. Предложена полностью распределенная схема гибридной безопасности с использованием технологий IDS и Honeypot, которая не полагается на централизованный контроллер, что делает схему общей, гибкой и эффективной. Возможности этих двух средств безопасности позволяют получить баланс между эффективностью безопасности и использованием ресурсов. Показано, как расширить предлагаемый подход POMDP на основе nonlinear programming (NLP) к планированию DEC-POMDP. Основная причина объединения IDS с Honeypot заключается в дополняющем характере двух технологий: IDS пассивно отслеживают трафик сети для подозрительных действий, в то время как Honeypot активно обнаруживают и анализируют интрузии. С другой стороны, то, что у них есть в общем децентрализованном развертывании и неопределенности в наблюдении, объясняет полезность моделирования системы как DEC-POMDP.

Ключевые слова: *сетевая безопасность, обнаружение сетевых атак, DEC-POMDP, IDS, Honeypot, нелинейное программирование.*

Введение

С быстрым развитием Интернета и резким увеличением сетевой преступности безопасность сети стала очень важной и привлекает все большее внимание. Накладными расходами, введенными мерами безопасности, нельзя пренебрегать. Например, ставки intrusion detection systems false positive (IDSs FP) привели некоторых к сомнению их полезности. Мы предлагаем полностью распределенную схему управления, которая не полагается на централизованный контроллер. Это делает нашу схему общей и гибкой.

Предложена схема гибридной безопасности с использованием технологий IDS и Honeypot (активная система защиты, предназначенная для преодоления недостатков IDS). Введение этих двух технологий фокусируется на связанных с безопасностью функциях. Анализ возможностей этих двух средств безопасности указывает на необходимость достижения баланса между эффективностью безопасности и использованием ресурсов. Существует два альтернативных подхода к управлению: централизованное и распределенное управление. С точки зрения безопасности распределенная версия предпочтительнее. Мы представляем формулу DEC-POMDP для схемы гибридной сетевой безопасности, которая объединяет IDS и Honeypot. Затем мы покажем, как расширить предлагаемый подход POMDP на основе nonlinear programming (NLP) к планированию DEC-POMDP.

1 Распределенное планирование для гибридов

Основная причина объединения IDS с Honeypot заключается в дополняющем характере двух технологий: IDS пассивно отслеживают трафик сети для подозрительных действий, в то время как Honeypot активно обнаруживают и анализируют интрузии. С другой стороны, то, что у них есть в общем децентрализованном развертывании и неопределенности в наблюдении, объясняет полезность моделирования системы как DEC-POMDP.

1.1 Система обнаружения вторжений

Системы обнаружения вторжений непрерывно контролируют компьютерную систему или сеть и генерируют аварийные сигналы для информирования системного администратора о подозрительных событиях. IDS теперь считаются необходимым дополнением к инфраструктуре безопасности организации [1]. Цель обнаружения вторжений – выявить злонамеренные действия и точно отделить их от доброкачественных действий. Согласно общей структуре обнаружения вторжений [2], общая архитектура IDS имеет четыре модуля:

– датчики Event-box (E-box) контролируют и собирают информацию о целевой системе;

– ящик базы данных (D-box) хранит информацию из E-box;

– блок анализа (A-box) анализирует данные, хранящиеся в D-box, и при необходимости генерирует аварийные сигналы;

– блок ответов (R-box) реализует контрмеры, чтобы помешать злонамеренным вторжениям.

Основные классы методологий обнаружения включают обнаружение на основе сигнатур, обнаружение аномалий и анализ протоколов состояния [1]. IDS, которые используют обнаружение на основе сигнатур, идентифицируют атаки путем сравнения существующих сигнатур известных атак с сохраненным сетевым трафиком. Когда совпадение найдено, IDS вызывают соответствующую контрмеру для противодействия обнаруженному вторжению. Обнаружение на основе сигнатур обеспечивает точные результаты обнаружения для хорошо определенных атак, а также эффективные известные контрмеры. Основным недостатком обнаружения на основе сигнатур является его неспособность обнаруживать новые, неизвестные атаки. При появлении новых атак, которые появляются непрерывно, методы обнаружения на основе сигнатур с высокой частотой ложных отрицательных (false negative, FN) неэффективны. Обнаружение аномалии может находить новые типы атак путем оценки отклонения наблюдаемой информации от предопределенной базовой линии «нормального». Однако по-прежнему существует несколько существенных проблем, связанных с обнаружением аномалий, включая высокие коэффициенты FP, низкую пропускную способность, высокую стоимость, отсутствие соответствующих показателей и т.д. [3]. Анализ состояния протокола может обеспечить более точные результаты обнаружения, чем обнаружение аномалий, но значительно более ресурсоемкий из-за сложного анализа и накладных расходов, вызванных отслеживанием состояния [1]. Как правило, чем больше точность обнаружения IDS может быть улучшена по сравнению с конфигурацией по умолчанию, тем она меньше. В результате непрерывный мониторинг может вызвать чрезмерную пропускную способность вычислений, что нежелательно для любой компьютерной системы и сети.

Кроме того, в IDS реализованы различные технологии предотвращения вторжений, такие как ведение журнала неавторизованного пользователя, закрытие системы или, если возможно, переконфигурирование сети [4] и т.д. Несмотря на усиление безопасности информационных и коммуникационных систем, возможности предотвращения вторжений влекут за собой высокую стоимость энергии и ресурсов хоста.

Нетрудно видеть из приведенного выше введения, что, для инструмента против кибератак, защищающего критическую информацию системы, необходимо учитывать стоимость ресурсов IDS. Планирование IDS необходимо для баланса между эффективностью безопасности и потреблением ресурсов.

Существует три основных типа IDS, а именно сетевые IDS (NIDS), на основе хоста IDS (HIDS) и на основе стека IDS (SIDS). Мы выбираем HIDS, поскольку HIDS можно выборочно развертывать на критичных машинах, таких как серверы управления, серверы данных и консоли администратора и т.д.

1.2 Honeypot

Honeypots необходимы для дополнения IDS в предлагаемой схеме безопасности, поскольку они дополняют большинство других технологий безопасности, принимая активную позицию. Honeypot – это тщательно контролируемый вычислительный ресурс, используемый в качестве ловушки для захвата злоумышленников. Как определено Шпицнером в [5], «Honeypot – это ресурс безопасности, ценность которого заключается в том, что его исследуют, атакуют или компрометируют». Основные цели Honeypot – отвлечь злоумышленников от критических ресурсов и исследовать атаки злоумышленников для создания подписей для обнаружения вторжений. Привлекательность Honeypot для злоумышленников смягчает угрозу злонамеренных атак и, таким образом, помогает обеспечить безопасность ценной информации и важных услуг, расположенных на реальных объектах.

Основываясь на уровне взаимодействия между Honeypots и нападающими, Honeypots можно в общем разделить на Honeypot высокопоточные и с низким взаимодействием. Типичными примерами являются honeyd и honeynet [5]. Honeyd позволяет пользователям настраивать несколько виртуальных Honeypots с различными характеристиками и услугами на одной машине. Honeynet контролирует большую и разнообразную сеть, когда один Honeypot не может быть достаточным. Очень сложно и дорого развертывать и поддерживать высокопоточную Honeypot, поскольку она эмулирует почти все действия, обнаруженные в обычной операцион-

ной системе. Развертывание и конфигурация Honeypot с низким взаимодействием намного проще и дешевле, поскольку она имитирует только некоторые системные службы. «BitSaucer» [6] представляет собой гибридную Honeypot, состоящую из возможностей взаимодействия с низким взаимодействием и высокой мощностью.

Honeypots также можно разделить на: исследования и производство honeypots [7]. Основная функция исследовательской honeypot заключается в извлечении подписи новых атак, которые могут быть использованы для повышения точности обнаружения IDS. Полное понимание наблюдаемых данных о трафике требует больших затрат времени и всестороннего опыта от аналитиков практически во всех связанных с сетью областях. Более того, развертывание исследовательских honeypots мало способствует укреплению безопасности системы. Производственные honeypots помещаются в производственную сеть для снижения риска. Большинство производственных honeypots являются honeypots с низким взаимодействием и фиксируют ограниченную информацию. Пример производства honeypot – Nepenthes [8]. Поскольку наша схема предназначена для повышения безопасности, мы используем производственные honeypots в сочетании с IDS.

В honeypots в основном не рассматриваются ложные срабатывания, такие как IDS, поскольку все услуги, имитируемые honeypots, не имеют производственной стоимости. Весь трафик, который входит и выходит из honeypots, является подозрительным и должен контролироваться и анализироваться [9]. Однако не все попытки доступа к honeypots являются злонамеренными. Например, человек может ошибочно ввести адрес компьютера и случайно подключиться к развернутой honeypot. В результате неопределенность также участвует в планировании honeypots.

1.3 Модель системы

И HIDS, и honeypots обнаруживают вторжения и могут работать в любое время. Тем не менее, обнаружение в режиме intrusion и эмуляция системы потребляют большое количество энергии и других ресурсов, включая память, использование процессора и дисковое хранилище.

Нам необходимо сбалансировать эффективность безопасности и стоимость ресурсов, планируя действия IDS и honeypot. Задача планирования моделируется как процесс с дискретным временем. В предлагаемой схеме более одного HIDS или honeypot могут быть активны в течение каждого периода времени.

Рассмотрим теперь пример гибридной системы. Предположим, что локальная сеть (ЛВС) оснащена $K-H$ -HIDS и H honeypots. Это приводит к тому, что общее количество устройств безопасности до K. Без потери общности мы также предполагаем, что топология сети статична, и есть больше машин, чем доступных HIDS. Неизбежно, только на некоторых машинах установлены HIDS. Пример сети показан на рис. 1.

Предположим, что каждая HIDS может работать в трех режимах: мониторинг, профилактика и сон, который является местом действия для HIDS. HIDS настроен на мониторинг обнаружения вторжений и может спать для экономии энергии. Профилактическое действие может быть принято путем переключения в режим предотвращения, если обнаружена несанкционированная или злонамеренная деятельность, в котором потребляется больше ресурсов. Аналогично, пространство действий развернутой honeypot может быть определено как мониторинг, анализ и сон. Дальнейший анализ будет проведен, если обнаружен аномальный трафик.

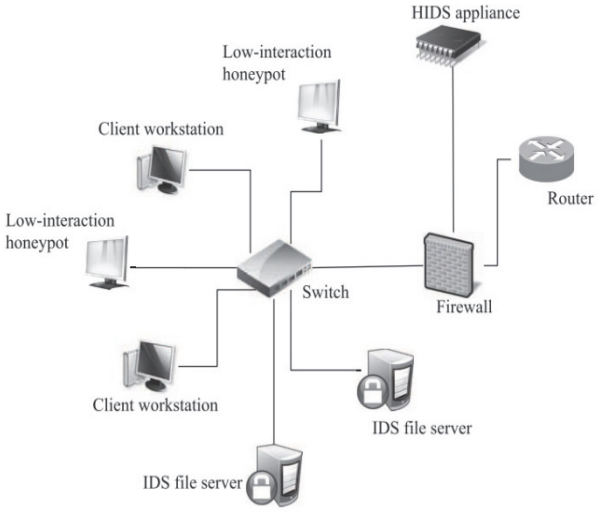

Рис. 1. Пример распределенной гибридной схемы безопасности, объединяющей HIDS с honeypots

Пусть $S^{(k)}(t)$ обозначает состояние произвольного устройства k (HIDS или honeypot) в момент t, мы предполагаем, что $S^{(k)}(t) = \langle X^{(k)}(t), Y^{(k)}(t) \rangle$, где $X^{(k)}(t)$ представляет условие безопасности, а $Y^{(k)}(t)$ представляет уровень потребления ресурсов. Например, состояние безопасности можно просто разделить на: «безопасный» и «скомпрометированный». Если мы будем использовать обозначение X для обозначения пространства состояний $X^{(k)}(t)$, то X ={безопасный, скомпрометированный}. Пространство состояний $Y^{(k)}(t)$, обозначаемое Y, включает три уровня потребления: {низкий, средний, высокий}. Соответствие между различными уровнями потребления и рабочими состояниями:

– низкий: устройство не выбрано, то есть в режиме ожидания;

– средний: устройство работает в режиме монитора;

– высокий: HIDS/honeypot работает в режиме предотвращения / анализа.

Поскольку используемые IDS являются HIDS, каждый HIDS только контролирует машину, на которой он находится, игнорируя остальную сеть. В качестве децентрализованной схемы управления решение об активации определенного устройства безопасности основано на местных наблюдениях. Чтобы завершить задачу, предположим, что пространство наблюдений идентично пространству условий безопасности, то есть $O = X = \{$«безопасно», «скомпрометировано»$\}$. Обратите внимание, что аварийный сигнал вторжения не обязательно означает, что есть атака, и наоборот. Обнаружение вторжений может производить два типа ошибок: ложноположительные (FP) и ложноотрицательные (FN). Большой объем FP приводит к большому количеству времени, потраченного на то, чтобы определить, является ли предупреждение нападением, когда оно действительно доброкачественное [10]. В результате FN возникают дыры в безопасности из-за невозможности поднять сигналы тревоги при возникновении интрузий. Поскольку цель обнаружения вторжений заключается в том, чтобы точно отделить интрузии от законного поведения, обе ошибки являются значительными индексами производительности IDS и были воплощены в вероятностях наблюдений. Например, следующая вероятность наблюдения

$$\begin{gathered}\Pr\{O(k)(t+1) = \text{«скомпрометировано»},\\ | A^{(k)}(t) = \text{«режим ожидания»},\\ S^{(k)}(t+1) = \text{«монитор»}.\end{gathered} \quad (1)$$

равна скорости FP устройства k.

Локальное состояние каждого хоста в сети тесно связано с положением безопасности всей сети. Анализ разделен на два случая:

– переключение между различными режимами HIDS приведет к изменению уровня энергопотребления локального компьютера, но не повлияет на действия атаки в локальной сети;

– активация honeypot положительно повлияет на работу и безопасность сети, отвлекая противников от ценных ресурсов в локальной сети и, соответственно, уменьшит угрозу, создаваемую для остальной сети.

Из предыдущего анализа очевидно, что выбор каждого агента может влиять на состояние всей сети. Это делает DEC-POMDP более подходящим инструментом для моделирования планирования для распределенной системы [11].

Некоторые могут утверждать, что в этом случае также может быть принят централизованный контроллер. Однако в большинстве централизованных средств управления существует общий недостаток: он может потреблять непомерно высокую пропускную способность и мгновенную связь между агентами и контроллером. Кроме того, возможны нарушения безопасности, поскольку передаваемая информация может быть перехвачена противниками. Поэтому DEC-POMDP обычно более предпочтительнее.

2 Представление DEC-POMDP для распределенного гибрида системы безопасности, объединяющего IDS и Honeypot

Мы определяем состояние формулировки DEC-POMDP в момент времени t, обозначаемый $S(t)$, как комбинацию $S^{(k)}(t), i = 1, 2, ..., K$:

$$S(t) = [S^{(1)}(t), S^{(2)}(t), ..., , S^{(K)}(t)].$$

Аналогично, мы можем записать действие времени t как

$$A(t) = [A^{(1)}(t), A^{(2)}(t), ..., , A^{(K)}(t)].$$

Теперь рассмотрим закон перехода состояния. Состояние $S(t)$ эволюционирует на основе принципа принятия решения Маркова $(|X| \times |Y|)$. Пусть W обозначает вероятностную функцию перехода состояния, то

$$W(\bar{s}, \bar{a}, \bar{s}') = \Pr\{S(t+1) = \bar{s}' \mid S(t) = \bar{s},\ A(t) = \bar{a}\},$$

где $\bar{s}, \bar{s}' \in S^K$ и $\bar{a} \in A^K$.

Наблюдаемые вероятности формулировки DEC-POMDP несколько отличаются от стандартной модели. Как указано в (1), величины вероятностей наблюдений назначаются в соответствии со скоростями FP и FN устройств. Следовательно, наблюдение каждого агента зависит только от локальной информации. Отсюда следует, что $V^{(k)}(a, s', o')$, вероятность наблюдения устройства i задается выражением

$$\begin{gathered}V^{(k)}(a, s', o') = \Pr\{O^{(k)}(t+1) =\\ = o' \mid A^{(k)}(t) = a, S^{(k)}(t+1) = s'\}.\end{gathered}$$

Наконец, немедленное вознаграждение в момент времени t определяется как сумма каждого местного немедленного вознаграждения

$$\begin{gathered}r(S(t), A(t)) =\\ = \sum_{k=1}^{K} r(S^{(k)}(t), S^{(k)}(t)).\end{gathered} \quad (2)$$

Значения немедленных вознаграждений назначаются в соответствии со следующими правилами:

успешное обнаружение атаки приводит к большой награде; Напротив, ненужный дальнейший анализ, поставленный из-за неправильного суждения, вызовет большой штраф, так же, как и неправильное определение атаки; Кроме того, мониторинг не является бесплатным и мониторинг безопасной машины происходит с небольшим штрафом.

Модель планирования для гибридной системы – DEC-POMDP. Таким образом, нам нужно увеличить метод решения POMDP [12] до ситуаций с несколькими контроллерами. Решение DEC-POMDP состоит из набора графиков политики, по одному для каждого агента. Соответственно, целью является оптимизация набора FSC. Ниже мы покажем, что расширение решения на основе NLP до DEC-POMDP очень просто. Чтобы представить алгоритм для DED-POMDP, сделаем следующие предположения:

– в DEC-POMDP есть K -агенты;

– пространство состояний DEC-POMDP обозначается S. Каждый агент имеет одно и то же пространство действий A («предотвращение» IDS соответствует «анализу» honeypot) и пространству наблюдения O;

– каждый агент выбирает действия в соответствии с FSC фиксированного размера. Набор узлов в FSC агента k обозначается через $N^{(k)}$;

– мы используем обозначение n для обозначения вектора длины K, где $\overline{n}(k) \in N^{(k)}$. Аналогичным образом определяются вектор наблюдения $\overline{o}$ и вектор действия $\overline{a}$;

– $x_k(n.a)$ и $y_k(n,o',n')$ – управляющие переменные FSC агента k.

Формальное представление решения DEC-POMDP на основе NLP, удовлетворяющего указанным выше предположениям:Для переменных π_{nsa} и $g^{(k)}(n_k, o'_k, n'_k, a'_k)$, где $g^{(k)}(n_k, o'_k, n'_k, a'_k) = x_k(n', a')y_k(n, o', n')$, максимизируем $\sum_{\overline{n}} \sum_{s \in S} \sum_{\overline{a} \in A} \pi_{\overline{n}s\overline{a}} \cdot r(s, \overline{a}^K)$ при условии для $\forall s' \in S, \forall \overline{n} \in \Delta, \forall \overline{a} \in A^K$:

$$\pi_{\overline{n}'s'\overline{a}'} = \sum_{\overline{o} \in O} \sum_{s \in S} \sum_{\overline{a} \in A^K} \pi_{\overline{n}s\overline{a}} \sum_{\overline{o} \in O^K} P(s, \overline{a}, s') \times$$
$$\times Q(\overline{a}, s', \overline{o}') \prod_k g^{(i)}(n_k, o'_k, n'_k, a'_k),$$
$$\forall n'_k \in N^{(k)}, \forall o'_k \in O, \qquad (3)$$
$$\sum_{n'_k} \sum_{a'_k \in A} g^{(k)}(n_k, o'_k, n'_k, a'_k) = 1,$$
$$\text{for } k = 1, 2, ..., K.$$

Оптимальное решение для NLP в (3) обеспечивает оптимальный набор FSC данного размера.

Решение представляет свою доступность к одному критическому фактору: каждый агент ведет себя независимо. То есть все графики политики независимы друг от друга.

Выводы

Рассмотрены две технологий безопасности, принятые в предлагаемой схеме безопасности. Мы выбрали HIDS в сочетании с honeypot с целью интеграции преимуществ обоих инструментов в нашей системе. Сформулирован децентрализованный контроль над системой как DEC-POMDP. Показано, как расширить алгоритм POMDP на основе FSC, для решения DEC-POMDP.

Список литературы (References)

1. Scarfone, K. and Mell, P. (2007), *Guide to Intrusion Detection and Prevention Systems (IDPS)*, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD, February 2007, National Institute of Standards and Technology special publication 800-94.
2. Tung, B. (1999), *The common intrusion detection framework*, http://gost.isi.edu/cidf/.
3. Draper, D., Hanks, S. and Weld, D. (1994), Probabilistic planning with information gathering and contingent execution, *Proceedings of the Second International Conference on AI Planning Systems*, pp. 31-36.
4. Zheng, J. and Jamalipour, A. (2009), *Wireless Sensor Networks: A Networking Perspective*, A John & Sons, Inc and IEEEE.
5. Spitzner, L. (2002), *Honeypots: Tracking Hackers*, 1st edition, Addison-Wesley, Boston, MA.
6. Adachi, Y. and Oyama, Y. (2009), Malware analysis system using process-level virtualization, *Proceedings of IEEE Symposium on Computers and Communications*, pp. 550-556.
7. Mokube, I. and Adams, M. (2007), Honeypots: Concepts, approaches, and challenges, *ACMSE 2007*, Winston-Salem, NC, pp. 321-325.
8. Baecher, P., Koetter, M., Dornseif, M. and Freiling, F. (2006), The nepenthes platform: An efficient approach to collect malware, *Proceedings of the 9 th International Symposium on Recent Advances in Intrusion Detection (RAID)*, Springer, pp. 165-184.
9. Garcia-Teodoroa, P., Diaz -Verdejoa, J., Macia-Fernandeza, G. and Vazquezb, E. (2009), Anomaly based network intrusion detection: Techniques, systems and challenges. *Computer & Security*, Feburary – March 2009, No. 28(1 – 2), pp.18-28.
10. Bakar, N.A., Belaton, B. and Samsudin, A. (2005), False positives reduction via intrusion alert quality framework, *Joint IEEE Malaysia International Conference on Communications and IEEE International Conference on Networks*, November 2005, pp. 547-552.

11. Cassandra, A.R. (2009), *The distributed agent system problem*, http://www.cassandra.org/pomdp/talks/who-needs-pomdps/agent-simple.POMDP.

12. Xin, L., . Cheung, W.K. and Liu, J. (2010). Improving POMDP's Tractability Via Belief Compression and Clustering, *IEEE Transactions on Systems, Man and Cybernetics*, Part B, 40(1), pp. 125-136.

Поступила в редколлегию 2.08.2017
Одобрена к печати 19.10.2017

Відомості про авторів:

Борисова Наталя Володимирівна
кандидат наук доцент кафедри
Національного технічного університету
"Харківський політехнічний інститут",
Харків, Україна
https://orcid.org/0000-0002-8834-2536
e-mail: borisova_nv@mail.ru

Шабанова-Кушнаренко Любов Володимирівна
кандидат наук асистент кафедри
Національного технічного університету
"Харківський політехнічний інститут",
Харків, Україна
https://orcid.org/0000-0002-2080-7173
e-mail: l.v.shabanova.kushnarenko@gmail.com

Information about the authors:

Borisova Natalya
Candidate of Sciences Associate Professor of
Department of National Technical University
"Kharkiv Polytechnic Institute",
Kharkov, Ukraine
https://orcid.org/0000-0002-8834-2536
e-mail: borisova_nv@mail.ru

Shabanova-Kushnarenko Lyubov
Candidate of Sciences Assistant Lecturer of
Department National of Technical University
"Kharkiv Polytechnic Institute",
Kharkov, Ukraine
https://orcid.org/0000-0002-2080-7173
e-mail: l.v.shabanova.kushnarenko@gmail.com

ГІБРИДНІ СИСТЕМИ БЕЗПЕКИ ІНФОРМАЦІЙНИХ ТА КОМУНІКАЦІЙНИХ МЕРЕЖ

Н.В. Борисова, Л.В. Шабанова-Кушнаренко

У статті розглядаються два різних методи вирішення децентралізованого частково спостерігаємого процесу прийняття рішень Маркова (decentralized partially observable Markov decision process, DEC-POMDP). Запропонована цілком розподілена схема гібридної безпеки з використанням технологій IDS та Honeypot, яка не спирається на централізований контролер, що робить схему загальною, гнучкою та ефективною. Основна причина об'єднання IDS з Honeypot – це дві доповнюючі технології. IDS пасивно відстежує трафік мережі для підозрілих дій, у той час як Honeypot активно знаходить та аналізує інтрузії. Можливості цих засобів безпеки дозволяють отримати баланс між ефективністю безпеки та використанням ресурсів. Показано, як розширити запропонований підхід POMDP на базі nonlinear programming (NLP) до планування DEC-POMDP.

Ключові слова: *мережева безпека, визначення мережевих атак, DEC-POMDP, IDS, Honeypot, нелінійне програмування.*

HYBRID SECURITY SYSTEMS IN INFORMATION AND TRANSMISSION NETWORKS

N. Borisova, L. Shabanova-Kushnarenko

In article the decentralized partially observed decision-making process of Markov (DEC-POMDP) two various methods of a solution are considered completely distributed circuit of hybrid safety with use of the IDS and Honeypot technologies which is not necessary on the centralized controler that does the scheme of the general, flexible and effective is offered. The main reason for the association IDS with Honeypot consists in the supplementing nature of two technologies: IDS passively trace a network traffic for suspicious actions while Honeypot actively find and analyze intrusions. Opportunities of these two security aids are allowed to have balance between efficiency of resources safety and use. It is shown how to expand the offered approach of POMDP on the basis of nonlinear programming (NLP) to planning of DEC-POMDP.

Keywords: *network security, network intrusion detection, DEC-POMDP, IDS, Honeypot, nonlinear programming.*