УДК 621.391

МОДЕЛИРОВАНИЕ ПРОКОЛОВ МАРШРУТИЗАЦИИ ПРИ АТАКЕ ЧЁРНОЙ ДЫРЫ В МОБИЛЬНЫХ AD-HOC СЕТЯХ

Нгуен Ч.Т, магистрант гр.215101

Белорусский государственный университет информатики и радиоэлектроники[1]

г. Минск, Республика Беларусь

Цветков В.Ю. – Доктор. тех. наук

Аннотация. В статье представлено моделирование протоколов маршрутизации: AODV, IDSAODV в мобильных ad-hoc сетях при атаке чёрной дыры.

Ключевые слова. Атака чёрной дыры, AODV, IDSAODV.

Введение. При атаке чёрной дыры [1] злонамеренный узел утверждает, что у него есть действительный маршрут ко всем другим узлам в сети для перехвата трафика между узлами. После получения переданных данных он не пересылает, а отбрасывает все эти пакеты. Следовательно, этот узел чёрной дыры может отслеживать и анализировать трафик всех узлов в сети, на которую он напал.

AODV (Ad hoc On-demand Distance Vector) – Это протокол маршрутизации с одним маршрутом, использующий проактивное обнаружение маршрута. Исходный узел обнаруживает маршрут только тогда, когда ему нужно переслать данные. При каждом обнаружении маршрута исходный узел устанавливает уникальный маршрут к месту назначения и имеет наилучшую стоимость маршрута. Расходы маршрутизации протокола AODV определяется на основе количества переходов для достижения пункта назначения. Протокол AODV часто становится жертвой атак чёрной дыры. В каждом пакете маршрутизации AODV некоторые важные поля, такие как количество переходов HC, порядковый номер назначения, SN источника и получателя, заголовок IP, IP-адреса источника и получателя AODV, идентификационный номер RREQ. Ошибки в любом из вышеперечисленных полей могут привести к сбою AODV. Для выполнения атаки чёрной дыры в протоколе AODV злонамеренный узел ждет пакета RREQ, отправленного от его соседей. Когда он получает пакет RREQ, он немедленно отправляет ответ на пакет RREP с ложным содержимым, устанавливая самое высокое значение SN и минимальное значение HC, не выполняя проверку таблицы маршрутизации, чтобы увидеть, существует ли маршрут к месту назначения, прежде чем другие узлы отправят ответ о маршруте. Затем любые данные, передаваемые от исходного узла к узлу назначения, полностью отбрасываются злоумышленником, вместо того, чтобы пересылаться в соответствующий пункт назначения.

Протокол IDSAODV (Intrusion Detection System Ad hoc On-demand Distance Vector) – это безопасный протокол маршрутизации против атак чёрной дыры. Протокол IDSAODV основан на идее, что рабочий механизм протокола AODV заключается в проверке номера SN ответного пакета RREP. Если в сети присутствует узел чёрной дыры, то этот узел чёрной дыры немедленно ответит на пакет RREP с наивысшим присвоенным номером SN и, конечно же, немедленно ответит узлу-источнику, отправившем запрос RREQ. Следовательно, необходимо только отбросить первый полученный пакет RREP и принять второй пакет RREP с наивысшим SN, чтобы установить маршрут связи с использованием механизма буферизации пакетов.

В этой статье представлено моделирование протоколов AODV и IDSAODV при атаке чёрной дыры с помощью программного обеспечения для моделирования NS2. Затем сравните производительность протоколов маршрутизации на основе параметра коэффициента успешной доставки пакетов (Packet Delivery Ratio) и накладных расходов на маршрутизацию.

Основная часть. Сценарий моделирования построен на 20 узлах со случайным расположением инициализации в географической области размером 1000 м × 1000 м с дальностью радиопередачи каждого узла 250 м (радиус). Координаты каждого узла в месте области моделирования имеют форму (x, y, z), где z имеет значение 0. Узлы двигаются в соответствии с моделью Random Waypoint [2], что означает, что узел сначала занимает случайное положение в области моделирования и остается там в течение периода, называемого временем паузы. По истечении этого временного интервала узел случайным образом выбирает пункт назначения в области моделирования и скорость, которая равномерно распределяется между [мин. скорость, макс. скорость]. Затем узел перемещается в новое место с выбранной скоростью. При достижении нового местоположения узел делает паузу на выбранный период времени согласно равномерному

распределению между [Pmin, Pmax], а затем возобновляет процесс. При моделировании инициализация позиций узлов и процесс движения в соответствии с приведенной выше моделью выполняется с помощью инструмента «./setdest» – инструмент, которры был установлен в эмуляторе NS-2. Запуска setdest для создания топодогии сети с различными скоростями движения 10, 15 м/с. Параметры моделирования представлены в таблице 1.

Таблица 1 – Параметры моделирования

Параметры	Значения
Область моделирования	1000 м × 1000 м
Количество узлы	20
Радиус покрытия	250 м
Контракт трафика	CBR
Количество соединений	10
Скорость доставки пакетов	4 пакета/с
Скорость движения	10, 15 м/с
Количество злонамеренных узлов	0, 2, 4
Размер пакетов	512 bytes

Для каждой скорости движения будут установлены протоколы AODV и IDSAODV с увеличением доли узлов чёрной дыры по сравнению с общим количеством сетевых узлов. Результаты анализа протоколов с учетом скорости движения узлов сети и увеличения доли узлов-чёрных дыр в общем количестве узлов представлены на рисунках 1, 2, 3, 4.

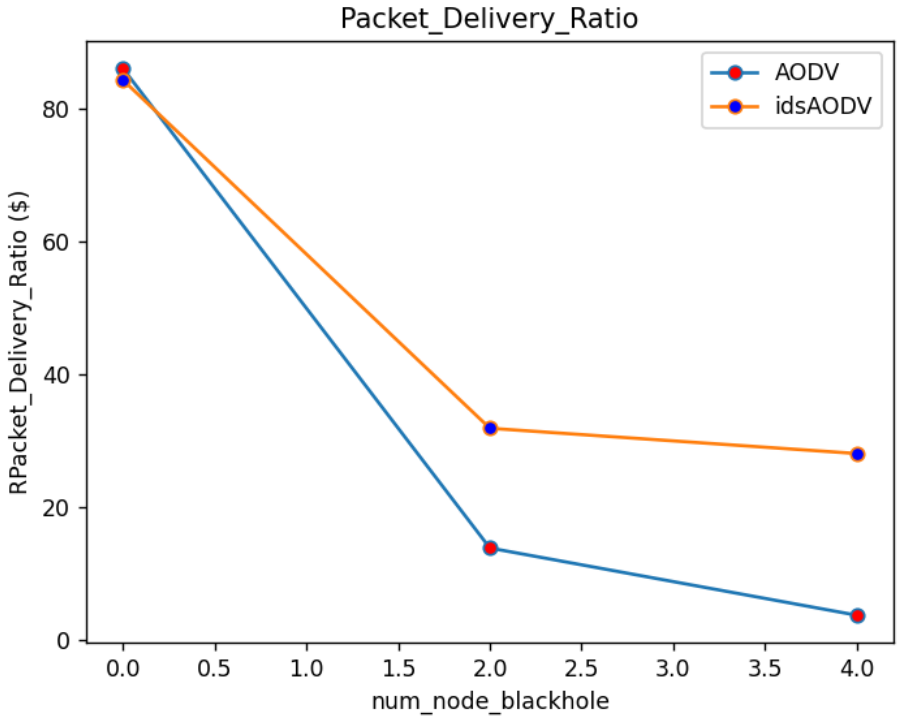

Рисунок 1 – Коэффициент успешной доставки пакетов при движении узлов 10 м/с

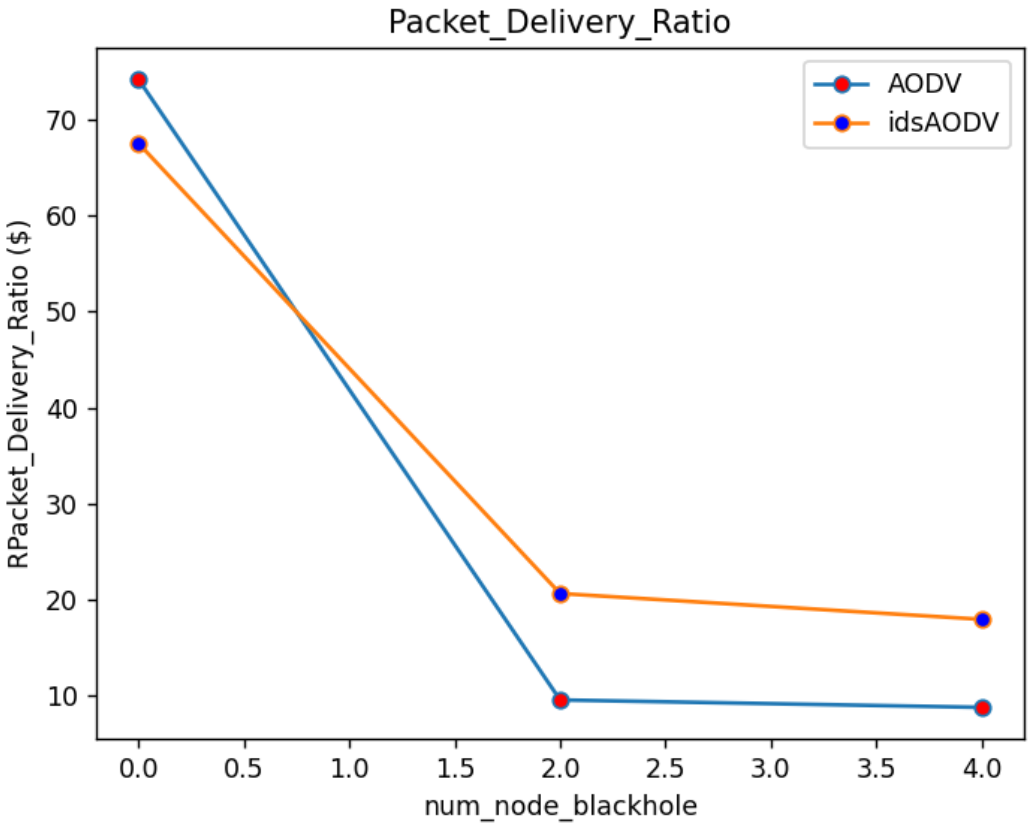

Рисунок 2 – Коэффициент успешной доставки пакетов при движении узлов 15 м/с

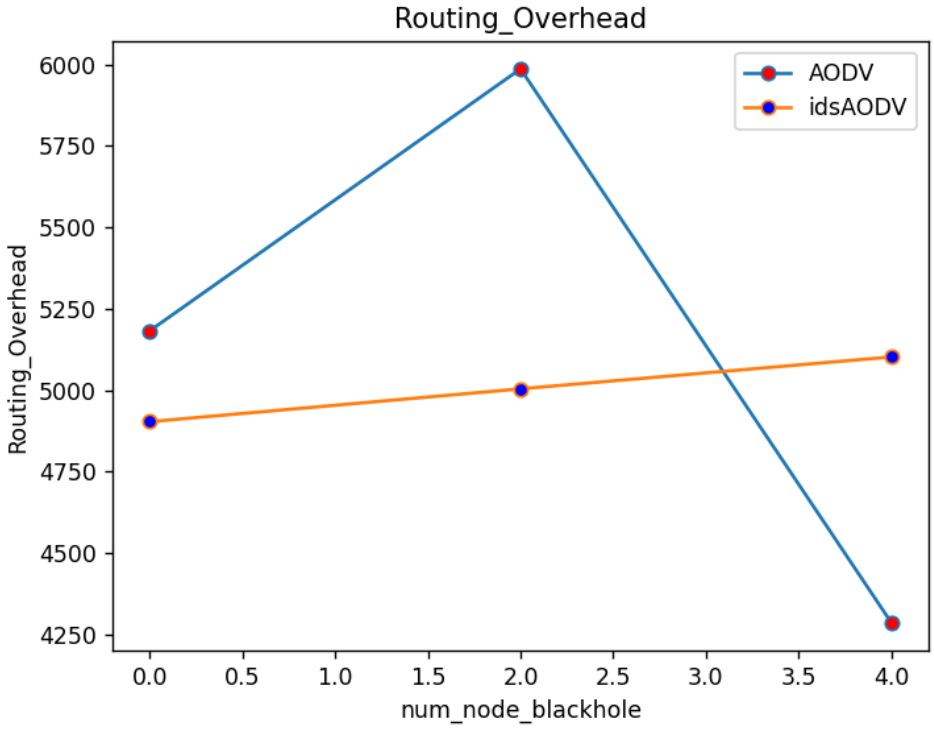

Рисунок 3 – Расходы на маршрутизацию, когда узлы перемещаются со скоростью 10 м/с

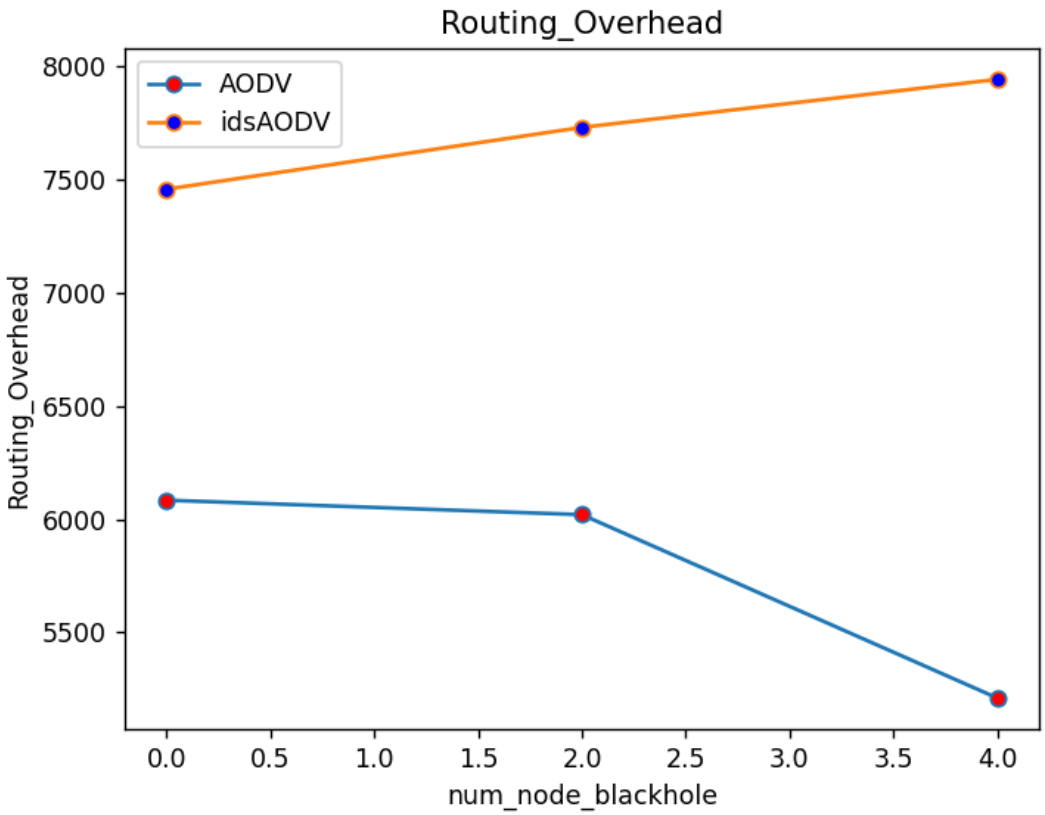

Рисунок 4 – Расходы на маршрутизацию, когда узлы перемещаются со скоростью 15 м/с

Когда в сети нет атакующих чёрных узлов. Коэффициент успешной доставки пакетов протокола AODV выше, чем у протокола IDSAODV. В случае узлов, движущихся со скоростью 15 м/с, вероятность успешной доставки пакетов для всех протоколов снижается, для протокола AODV — 74,19 %, для протокола IDSAODV — 67,53 %.

Когда в сети есть атакующие чёрные узлы. Коэффициент успешной доставки пакетов двух протоколов маршрутизации значительно снижается. Протокол IDSAODV имеет лучшую коэффициент успешной доставки пакетов, чем протокол AODV, поскольку количество узлов атаки чёрной дыры в сети увеличивается. По мере увеличения количества узлов атаки чёрной дыры, расходы на маршрутизацию протокола IDSAODV также увеличивается.

Заключение. Атаки чёрной дыры оказывают большое влияние на коэффициент успешной доставки пакетов. При атаке чёрной дырой протокол IDSAODV имеет лучший коэффициент успешной доставки пакетов, чем протокол AODV, но ненамного. Скорость движения узлов также существенно влияет на коэффициент успешной доставки пакетов в сети. Ограничение протокола IDSAODV заключается в том, что в некоторых случаях не всегда бывает так, что первый пакет RREP с наибольшим полученным значением SN также поступает из узла чёрной дыры, то есть когда узел назначения или промежуточный узел отвечает на Пакет RREP с наибольшим SN расположен ближе к узлу назначения, чем к узлу чёрной дыры.

Список использованных источников:

1. Routing Security in Wireless Ad Hoc Networks / H. Deng, W. Li and D. P. Agrawal // IEEE Communication Magazine, October 2002

2. Ad hoc wireless networks: Architecture and Protocols / C. Siva Ram Murthy, B. S. Manoj // Prentice Hall Publishers, May 2004.

UDC 621.391

SIMULATION OF ROUTING PROTOCOLS DURING A BLACK HOLE ATTACK IN MOBILE AD-HOC NETWORKS

Nguyen T.T

Belarusian State University of Informatics and Radioelectronics[1], Minsk, Republic of Belarus

Tsvetkov V.Y. – Doctor of Technical Sciences

Annotation. The article presents the modeling of routing protocols: AODV, IDSAODV in mobile ad-hoc networks during a black hole attack.

Keywords. IDSAODV, AODV, black hole attack.