УДК 621.391

АТАКА ЧЕРВОТОЧИНЫ 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. Данная статья представляет обзор атаки червоточины на мобильные ad-hoc сети. В статье описываются основные характеристики и последствия этой атаки и методы, которые злоумышленники используются для выполнения такой атаки.

Ключевые слова. MANET, атака червоточины, ad-hoc.

Введение. В настоящее время беспроводные сети широко используются в различных областях, в том числе и в мобильных ad-hoc сетях (MANET). Однако, в связи с их открытой структурой и динамичностью, они становятся более уязвимыми для атак и угроз безопасности. Одной из серьезных угроз безопасности MANET является атака червоточины. Атака червоточины MANET представляет собой атаку на протоколы маршрутизации в MANET, которая осуществляется с помощью внедрения злонамеренных узлов в сеть. В этой атаке злоумышленник использует уязвимость в протоколе маршрутизации, чтобы внедрить свой злонамеренный узел в сеть. Этот узел затем может захватывать информацию, перехватывать пакеты данных или нарушать работу сети. Цель данной статьи является представлением обзор атаки червоточины MANET на мобильные ad-hoc сети. В статье будут описаны основные характеристики и последствия этой атаки, а также приведены методы для выполнения этой атаки.

Основная часть. Атака червоточины направлена на подслушивание информации, иногда хакеры устраивают атаки, чтобы нарушить производительность сети. Для атаки хакеры используют два вредоносных узла, которые соединяются друг с другом через частную ссылку, называемую туннелированием или с использованием механизмов инкапсуляции. Атаки через червоточины могут выполняться в двух режимах: скрытом режиме и режиме присоединения [1].

Использование частной ссылки: для атаки хакеры используют 2 вредоносных узла (M_1, M_2), которые соединяются друг с другом через частный путь, называемый туннелем [2, 3]. Получив запрос маршрутизации RREQ, злонамеренный узел M_1 пересылает пакет RREQ к M_2 через туннель, M_2 продолжает пересылать RREQ к месту назначения. Получив пакет RREQ, узел назначения отправляет пакет RREP через туннель к источнику. В результате исходный узел устанавливает маршрут через туннель, поскольку этот маршрут стоит меньше, чем фактический маршрут. На рисунке 1 описана атака червоточины с использованием частной ссылки.

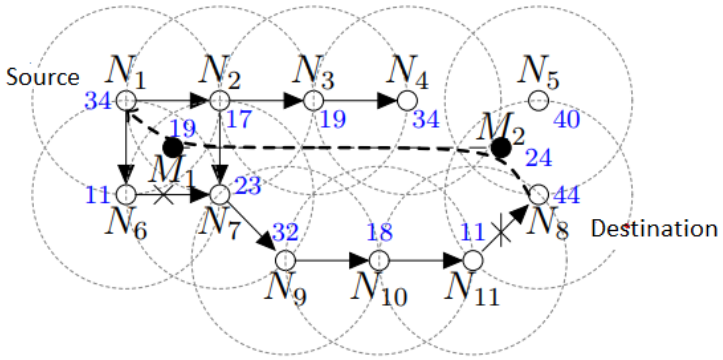

Рисунок 1 – атака червоточины с исползованием частной ссылки

Описание процесса, посредством которого исходный узел N_1 обнаруживает маршрут к месту назначения N_8 в топологии сети с двумя вредоносными узлами (M_1, M_2), соединяющимися через туннель. Исходный узел N_1 широковещательно передает пакет RREQ для обнаружения маршрута к целевому узлу N_8. Первый пакет RREQ к месту назначения на туннельном маршруте: $\{N_1 x\, M_1 x\, M_2 x N_8\}$. Когда пакет получает пакет RREQ, злонамеренный узел M_1 добавляет новую

запись в таблицу маршрутизации, чтобы представить маршрут к источнику N_1, информация о записи: Node= N_1, NH = N_1, HC = RREQ.HC+1=1, SN=35. Точно так же злонамеренный узел M_2 добавляет новую запись в таблицу маршрутизации, чтобы представить маршрут к источнику N_1, через следующий переход M_1, информация записи: Node =N_1, NH=M_1, HC=RREQ.HC+1=2, SN=35. Наконец, после получения пакета RREQ узел назначения N_8 добавляет новую запись в таблицу маршрутизации, чтобы представить маршрут обратно к N_1 через следующий переход M_2, информация записи: Node= N_1, NH= M_2, HC=RREQ. .HC+1=3, SN=35, и узел назначения N_8 отвечает на маршрут, посылая пакет RREP в направлении $\{N_8 x\ M_2 x\ M_1 x\ N_1\}$. Кроме того, второй пакет RREQ также достигает пункта назначения по маршруту $\{N_1 \rightarrow N_2 \rightarrow N_7 \rightarrow N_9 \rightarrow N_{10} \rightarrow N_{11} \rightarrow N_8\}$. Но узел назначения N_8 отбрасывает второй полученный пакет RREQ, поскольку он уже обработан. Детали управляющего пакета и таблицы маршрутизации перечислены в таблице 1.

Таблица 1 – Результат обнаружения маршрута при атаке червоточины

Пакет	Узел	Информация о пакете [LH] [IP_{src}, IP_{dst}, HC, SN]	Таблица маршрутизации			
			Node	NH	HC	SN
RREQ	N_1	$[N_1]$ $[N_1, N_8, 0, 35]$	NULL			
	N_2	$[N_2]$ $[N_1, N_8, 1, 35]$	N_1	N_2	1	35
	N_3	$[N_3]$ $[N_1, N_8, 2, 35]$	N_1	N_2	2	35
	N_4	$[N_4]$ $[N_1, N_8, 3, 35]$	N_1	N_3	3	35
	N_5	Пакет RREQ не получен				
	N_6	$[N_6]$ $[N_1, N_8, 1, 35]$	N_1	N_1	1	35
	N_7	$[N_7]$ $[N_1, N_8, 2, 35]$	N_1	N_1	2	35
	N_8	$[N_8]$ $[N_1, N_8, 3, 35]$	N_1	M_2	3	35
	N_9	$[N_9]$ $[N_1, N_8, 3, 35]$	N_1	N_7	3	35
	N_{10}	$[N_{10}]$ $[N_1, N_8, 4, 35]$	N_1	N_9	4	35
	N_{11}	$[N_{11}]$ $[N_1, N_8, 5, 35]$	N_1	N_{10}	5	35
	M_1	$[M_1]$ $[N_1, N_8, 1, 35]$	N_1	N_1	1	35
	M_2	$[M_2]$ $[N_1, N_8, 2, 35]$	N_1	M_1	2	35
RREP	N_8	Инициализация пакета RREP $[N_8]$ $[N_8, N_1, 0, 45]$				
	M_2	$[M_2]$ $[N_8, N_1, 1, 45]$	N_8	N_8	1	45
	M_1	$[M_1]$ $[N_8, N_1, 2, 45]$	N_8	M_2	2	45
	N_1	$[N_1]$ $[N_8, N_1, 3, 45]$	N_8	M_1	3	45

Использование инкапсуляции: этот метод использует 2 вредоносных узла, которые отображаются в сети как обычные узлы. Получив пакет RREQ, злонамеренный узел инкапсулирует его перед передачей пакета RREQ получателю через другие промежуточные узлы. Инкапсуляция выполняется таким же образом при получении пакета RREP. Цель состоит в том, чтобы снизить стоимость пакета управления путем, установив значение поля HC равным 0. Кроме того, злонамеренный узел увеличивает значение поля ID_broadcast пакета RREQ, чтобы сосед согласился обработать пакет, если он уже получил его тот же пакет от другого соседа. Цель состоит в том, чтобы исходный узел установил путь по маршруту, содержащему вредоносный узел, потому что стоимость ниже, чем фактический маршрут. В зависимости от местоположения маршрут

содержит один или два вредоносных узла [2, 3]. Атака с использованием метода инкапсуляции описана на рисунке 2.

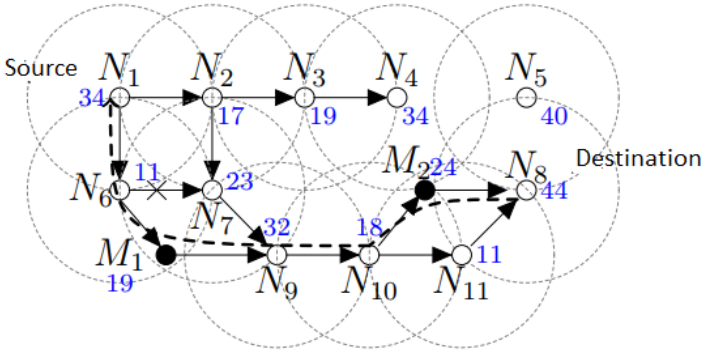

Рисунок 2 – Атака червоточины с использованием инкапсуляции

На рисунке 2. показаны два вредоносных узла M_1 и M_2, использующие инкапсуляцию для атаки на сеть. Узел N_9 получает оба пакета RREQ от источника N_1 по маршруту $\{N_1 \rightarrow N_2 x\ N_7\}$ и $\{N_1 \rightarrow N_6 x\ M_1\}$. Узел N_9 обнаруживает, что расход поиска через следующий переход M_1 составляет 1 переход, потому что значение HC пакета RREQ повторно инициализируется при пересылке через M_1 . Таким образом, N_9 устанавливает обратный маршрут к источнику через следующий переход M_1, добавляя новую запись в таблицу маршрутизации, информация о записи: NODE=N_1, NH=M_1, HC=RREQ.HC+1=1, SN=35. Пакеты RREQ, поступающие от N_7, не принимаются из-за более высокой стоимости. Узел назначения N_8 получает 2 пакета RREQ, приходящих от узлов N_{11} и M_2, пакет, приходящий от N_{11} имеет стоимость 3 переходов, поскольку он должен пересылаться через 3 промежуточных узла, включая $\{N_9, N_{10}, N_{11}\}$, в то время как пакет RREQ поступает от M_2 стоит 1 переход. Следовательно, узел назначения устанавливает маршрут к источнику через следующий переход M_2 , добавляя новую запись в таблицу маршрутизации, информация о записи: NODE=N_1, NH=M_2, HC=RREQ.HC+1=1, SN=35. Пакет RREQ, поступающие от N_{11}, не принимаются из-за больших накладных расходов. Узел назначения N_8 отвечает на исходный маршрут, посылая пакет RREP в направлении $\{N_8 \rightarrow M_2 \rightarrow N_{10} \rightarrow N_9 \rightarrow M_1 \rightarrow N_6 \rightarrow N_1\}$. Все промежуточные узлы сохраняют маршрут к месту назначения N_8 каждый раз, когда они получают пакет RREP, и пересылают пакет RREP обратно к источнику, используя запись в таблице маршрутизации. В результате исходный узел N_1 устанавливает маршрут к месту назначения через следующий переход N_1 со стоимостью назначения 2 перехода, этот маршрут содержит два злонамеренных узла M_1 и M_2, как подробно описано в таблице 2.

Таблица 2 – Результат обнаружения маршрута при атаке червоточины

Пакет	Узел	Информация о пакете [LH] [IP_{src}, IP_{dst}, HC, SN]	Таблица маршрутизации			
			Node	NH	HC	SN
RREQ	N_1	[N_1] [N_1, N_8 , 0, 35]	NULL			
	N_2	[N_2] [N_1, N_8 , 1, 35]	N_1	N_1	1	35
	N_3	[N_3] [N_1, N_8 , 2, 35]	N_1	N_2	2	35
	N_4	[N_4] [N_1, N_8 , 3, 35]	N_1	N_3	3	35
	N_5	с				
	N_6	[N_6] [N_1, N_8 , 1, 35]	N_1	N_1	1	35
	M_1	[M_1] [N_1, N_8 , 0, 35]	N_1	N_6	2	35
	N_7	[N_7] [N_1, N_8 , 2, 35]	N_1	N_2	2	35

Пакет	Узел	Информация о пакете [LH] [IP_{src}, IP_{dst}, HC, SN]	Таблица маршрутизации			
			Node	NH	HC	SN
	N_8	$[N_8]$ $[N_1, N_8, 6, 35]$	~~N_1~~ N_1	~~N_{11}~~ M_2	~~6~~ 1	~~35~~ 35
	N_9	$[N_9]$ $[N_1, N_8, 3, 35]$	~~N_1~~ N_1	~~N_7~~ M_1	~~3~~ 1	~~35~~ 35
	N_{10}	$[N_{10}]$ $[N_1, N_8, 4, 35]$	N_1	N_9	4	35
	N_{11}	$[N_{10}]$ $[N_1, N_8, 5, 35]$	N_1	N_{10}	5	35
	M_2	$[M_2]$ $[N_1, N_8, 0, 35]$	N_1	N_{10}	3	35
RREP	N_8	Инициализация пакета RREP $[N_8]$ $[N_8, N_1, 0, 45]$				
	M_2	$[M_2]$ $[N_8, N_1, 0, 45]$	N_8	N_8	1	45
	N_{10}	$[N_{10}]$ $[N_8, N_1, 1, 45]$	N_8	M_2	1	45
	N_9	$[N_9]$ $[N_8, N_1, 2, 45]$	N_8	N_{10}	2	45
	M_1	$[M_1]$ $[N_8, N_1, 0, 45]$	N_8	N_9	3	45
	N_6	$[N_6]$ $[N_8, N_1, 1, 45]$	N_8	M_1	1	45
	N_1	$[N_1]$ $[N_8, N_1, 2, 45]$	N_8	N_2	2	45

Заключение. В статье представлены два метода атаки червоточины, которые злоумышленники используют для атаки. В туннельном режиме управляющий пакет не изменяется при прохождении через вредоносный узел, поэтому решения по обеспечению безопасности, использующие проверку целостности пакетов, не будут работать. В механизме инкапсуляции злонамеренный узел изменил параметры пакета, поэтому может использовать механизм проверки целостности пакета, чтобы определить, была ли сеть атакована.

Список использованных источников:

1. Wormhole Attack Detection Technique in Mobile Ad Hoc Networks / Kaur P., Kaur D., Mahajan R // Vol. 97. P. 2939–2950.

2. Wormhole Attack in Wireless Ad Hoc Networks / Khabbazian M., Mercier H., Bhargava V.K // Vol. 8. P.736–745.

3. A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET / Jen S.M., Laih C.S., Kuo W.C// Vol. 9. P. 5022–5039

UDC 621.391

WORMHOLE 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. This article provides an overview of the MANET wormhole attack on mobile ad-hoc networks. The article describes the main characteristics and consequences of this attack and the methods used by attackers to carry out such an attack.

Keywords. MANET, wormhole attack, ad-hoc.