3. Kaspersky Security Bulletin 2019. Статистика. Available online: https://securelist.ru/ kaspersky-security-bulletin-2019-statistics/95264/ (accessed on 24 March 2020).
4. Hu, K.H., Jianguo, W., Tzeng, G.H. (2017). Risk factor assessment improvement for China's cloud computing auditing using a new hybrid MADM model. // International Journal of Information Technology & Decision Making.- V. 16(03).- Pp.737–777.
5. Artur Rot. IT Risk Assessment: Quantitative and Qualitative Approach// Lecture Notes in Engineering and Computer Science. – 2008.- V.2173. - Pp. 1-6.
6. Hoh Peter In, Young-Gab Kim, Taek Lee, Chang-Joo Moon, Yoonjung Jung, Injung Kim. A Security Risk Analysis Model for Information Systems // Systems modeling and Simulation: Theory and Applications: Third Asian Simulation Conference.- Pp. 1-4.- 2004
7. Turksis Z., Goranin N., Nurusheva A., Boranbayev S. Information Security Risk Assessment in Critical Infrastructure: A Hybrid MCDM Approach. // INFORMATICA.- 2019.- Vol. 30, No. 1.- Pp. 187-211.
8. Stroie E. R. Advantages and Disadvantages of Quantitative and Qualitative Information Risk Approaches. // Chinese Business Review.- Pp. 1-3. -2012. –Vol. 10, No. 12, 1106-1110

9. Todd D. Jick Mixing Qualitative and Quantitative Methods: Triangulation in Action // Administrative Science Quarterly, Vol. 24, No. 4, Qualitative Methodology (Dec., 1979), Pp. 602-611.- 2011
10. Kaspersky Lab. Top 7 Mobile Security Threats in 2020. Available online: https://usa.kaspersky.com/resource-center/threats/top-seven-mobile-security-threats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store (accessed on 24 March 2020)
11. Kaspersky Lab Mobile Malware Continues to Grow and Online Bank Accounts are Targeted More Than 5 Million Times, Kaspersky Lab Q3 Report Shows. Available online: https://www.kaspersky.com/about/press-releases/2015_mobile-malware-continues-to-grow-and-online-bank-accounts-are-targeted-more-than-5-million-times-kaspersky-lab-q3-report-shows (accessed on 24 March 2020)

УДК 004

ОБНАРУЖЕНИЕ SINKHOLE - АТАК В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ

Марденов Ерік Маратұлы
uvideooperator@mail.ru
Докторант ФИТ ЕНУ им. Л.Н.Гумилева, Нур-Султан, Казахстан
Научный руководитель – Т.К.Жукабаева

Аннотация. Беспроводные сенсорные сети (БСС) подвержен многочисленным типам угроз и атак. Эта статья посвящена одной из сложных атак маршрутизаций – Sinkhole атака, которая является одной из самых строгих атак маршрутизации, поскольку она привлекает окружающие узлы вводящей в заблуждение информацией о маршруте и выполняет подделку данных или выборочную пересылку данных, проходящих через него.

Ключевые слова: Беспроводная сенсорная сеть, Sinkhole атака, Защитные атаки, Специальная сеть, Обнаружение вторжений.

Введение

С развитием технологий растет интерес к использованию БСС. Это область, где активные исследования могут проводиться с использованием различных алгоритмов, моделей, факторов безопасности и социальных факторов[1]. БСС представляют собой комбинацию чувствительных узлов и отвечают за восприятие, а также за первые этапы иерархии обработки[2].

Безопасность - жизненно важная проблема в БСС. Многие исследования сосредоточены на предоставлении решений безопасности для этих сетей

В реальном мире БСС сталкиваются с различными угрозами безопасности. В ответ на угрозы безопасности БСС в последние годы было предложено множество методов безопасности.[3,4]

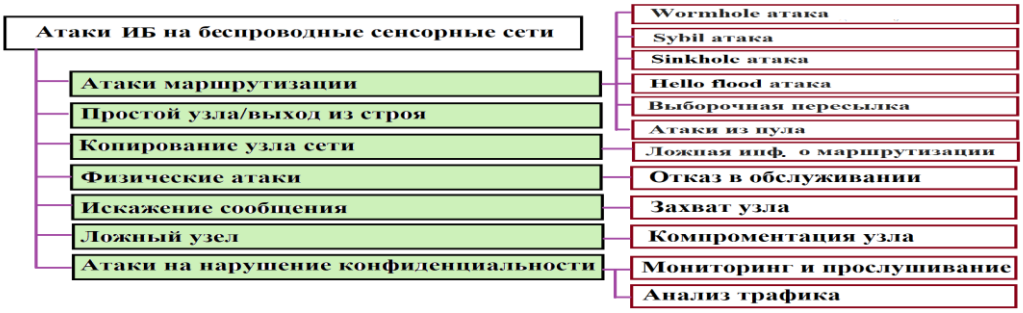


Рисунок-1. Классификация атак на БСС

Атака Sinkhole является одной из самых строгих атак маршрутизации, поскольку она привлекает окружающие узлы вводящей в заблуждение информацией о маршруте и выполняет подделку данных или выборочную пересылку данных, проходящих через него. Это может вызвать утечку энергии на окружающих узлах, что приведет к энергетическим дырам в БСС, и это может вызвать неправильные и потенциально опасные реакции, основанные на ложных измерениях [5]. Атаки Sinkhole выполняются либо путем взлома узла в сети, либо путем введения в сеть сфабрикованного узла. Вредоносный узел рекламирует себя как кратчайший путь к базовой станции и пытается направлять трафик от других узлов к себе. Это не только завлекает все узлы вблизи атаки, но также каждый узел ближе к базовой станции, чем атака. Узел злоумышленника или атака может легко изменить данные, ставящие под угрозу безопасность сети. Атака Sinkhole может быть инициирована как внутри сети, так и снаружи. В первом сценарии злоумышленник может использовать прослушиваемый узел, чтобы начать вторжение, а во втором случае захватчик может сформировать прямой путь к базовой станции через него, побуждая другие узлы отправлять свой трафик через него.

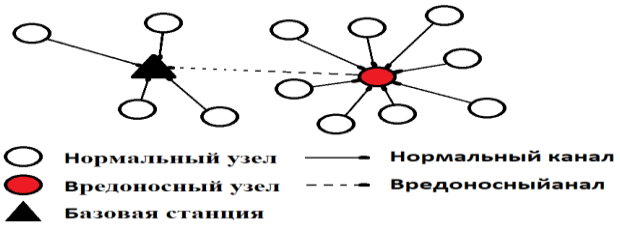


Рисунок-2. Sinkhole атака

Проблемы при обнаружении sinkhole атаки БСС

А. *Шаблон связи в* БСС*;* Все сообщения от сенсорных узлов в БСС направляются на базовую станцию. Sinkhole атаки обычно происходят, когда скомпрометированный узел отправляет ложную информацию о маршрутизации другим узлам в сети с целью привлечения максимально возможного трафика. Основываясь на этом шаблоне связи, злоумышленник скомпрометирует только узлы, которые находятся близко к базовой станции, вместо того, чтобы нацеливаться на все узлы в сети.

В. *Аварийная атака непредсказуема;* В БСС пакет передается на основе метрики маршрутизации, используемой различными протоколами маршрутизации [6]. Скомпрометированный узел использует свою метрику маршрутизации, которая использовалась протоколом маршрутизации, чтобы обмануть его соседние узлы, чтобы начать атаку провала. Тогда все данные от его соседей до базовой станции будут проходить через скомпрометированный узел.

C. *Инсайдерская атака.* Внутренняя атака и внешняя атака - это две категории атак в БСС. Внешняя атака - это когда злоумышленник не является частью сети. При внутренней атаке злоумышленник подвергает риску один из легитимных узлов путем закаливания узлов или из-за слабости системного программного обеспечения, после чего взломанный узел вводит ложную информацию в сеть после прослушивания секретной информации. [7].

D. *Физическая атака;* БСС обычно развертывается в агрессивной среде и остается без присмотра. Это дает злоумышленнику возможность физически атаковать узел и получить доступ ко всей необходимой информации

E. *Ресурсные ограничения*; Ограниченный источник питания, низкий диапазон связи, низкий объем памяти и низкая вычислительная мощность являются основными ограничениями в БСС, которые препятствуют внедрению надежного механизма безопасности. [8].

Подходы обнаружения атаки sinkhole

Основные подходы, которые использовались различными исследователями для обнаружения и идентификации атаки провалов в БСС.

A. *На основе правил.* Правила разработаны на основе поведения или техники, используемой для запуска атаки провала в грунте. Затем эти правила внедряются в систему обнаружения вторжений, которая работает на каждом узле датчика. Затем эти правила были применены к пакету, передаваемому через узлы сети. Если какой-либо узел нарушает правила, он считается противником и изолирован от сети.

В работе [9] использовали основанный на правилах подход, чтобы обнаружить атаку провала. Они создают два правила и внедряются в систему обнаружения вторжений (IDS). Когда одно из узлов нарушает одно из правил, система обнаружения вторжений выдает сигнал тревоги, но не предоставляет идентификатор узла скомпрометированного узла.

B. *Обнаружение аномалий*. При обнаружении на основе аномалий определяется нормальное поведение пользователя, а при обнаружении вторжения происходит поиск всего, что является аномальным в сети. В этом методе вторжение рассматривается как аномальная активность, потому что оно выглядит ненормальным по сравнению с нормальным поведением.

В работе [10] предложили систему, которая использовала значение RSSI (Индикатор силы принимаемого сигнала) с помощью узлов EM (Extra Monitor) для обнаружения атаки провала. EM имел большой диапазон связи, и одной из его функций является вычисление RSSI узла и отправка на базовую станцию с идентификатором источника и следующего перехода. Этот процесс происходит мгновенно при развертывании узла. Скомпрометированный узел идентифицируется и изолируется от сети базовой станцией с использованием значения VGM.

В работе [11], предложенная модель направлена на определение маршрутов для передачи этой информации, чтобы результирующая сеть могла гарантировать требуемое время жизни сети и обеспечивать радиосвязь между SN, чтобы сеть могла гарантировать доставку пакетов от SN к базовой станции.

C. *Статистический метод*. В статистических подходах данные, связанные с определенной деятельностью узлов в сети, изучаются и регистрируются исследователями.

В работе [12], «Исследование схем маршрутизации на основе динамической и статической кластеризации для БСС» представляет всесторонний обзор методов маршрутизации на основе динамической и статической кластеризации в БСС. Их общая цель - попытаться продлить срок службы сенсорной сети, не ставя под угрозу доставку данных.

В работе [13], каждый узел рассчитывает доверие своего соседнего узла на основе опыта взаимодействия; Рекомендации и знания затем отправляются на базовую станцию. Базовая станция решила, какой узел является провалом после получения нескольких значений доверия от других узлов. Поэтому значение доверия узла, которое выходит за пределы нормального значения 0,5, рассматривается как атака провала скважины.

D. *Обнаружение вторжения на основе гибридов.* В этом подходе используется комбинация как аномалий, так и сигнатур или неправильного использования. Частота

ложноположительных результатов, вызванных аномалиями, снижается в этом подходе благодаря использованию обоих методов. Также преимущество этого подхода состоит в том, чтобы иметь возможность ловить любые подозрительные узлы, чья подпись не включена в базу данных обнаружения.

В работе [14] предложили гибридную систему обнаружения вторжений для обнаружения провалов и других атак. Обнаружение гибридного вторжения было присоединено к узлу датчика и совместно использовало ресурс этого узла. Подозрительные узлы были добавлены в черный список на основе аномального поведения после анализа собранных данных от соседей. Затем этот список отправляется центральному агенту для принятия окончательного решения на основе характеристики схемы атаки (на основе неправильного использования). Подобно решению, предложенному работы [15], оно было разработано для статической БСС.

Е. *Управление ключами*. В подходе к управлению ключами целостность и аутентичность перемещений пакетов внутри сети защищена с помощью ключа шифрования и дешифрования. Любой пакет, передаваемый в сети, добавляется с другим сообщением таким образом, что для доступа к этому сообщению требуется ключ, и любая небольшая модификация сообщения может быть легко обнаружена. Эти ключи также помогают узлам проверять, поступило ли сообщение от базовой станции, и проверять подлинность сообщения.

В работе [16] предложили криптографический подход в протоколе маршрутизации для решения проблемы атаки провалов. Каждый узел получил открытый ключ, который использовался для проверки, приходит ли сообщение от базовой станции. Они также использовали пару открытых и закрытых ключей для аутентификации и подписывания сообщения данных. Все ключи были загружены в автономном режиме до развертывания сети. Их методы не позволили любому узлу скрыть свой идентификатор и подделку пакетов между узлами в сети. Этот протокол ориентирован на сопротивление атаке провалов, а не на обнаружение и устранение. В работе [17], «Энергоэффективный и основанный на кластерах протокол маршрутизации для БСС», предлагают протокол LEACH для экономии энергии узла, который разделен на два аспекта: выбор главы кластера и передача данных.

Моделирование sinkhole атаки с использование DSR

Атака sinkhole является одной из серьезных атак в БСС. В ней скомпрометированный узел или вредоносный узел объявляет неверную информацию о маршрутизации, чтобы выдать себя за определенный узел и получить весь сетевой трафик. После получения всего сетевого трафика он может либо изменить информацию о пакете, либо отбросить их, чтобы усложнить работу сети. Sinkhole атаки влияют на производительность специальных сетевых протоколов, таких как протокол DSR. Используемое программное обеспечение: NetSim Standard v10, Visual Studio 2015

Реализация в DSR:

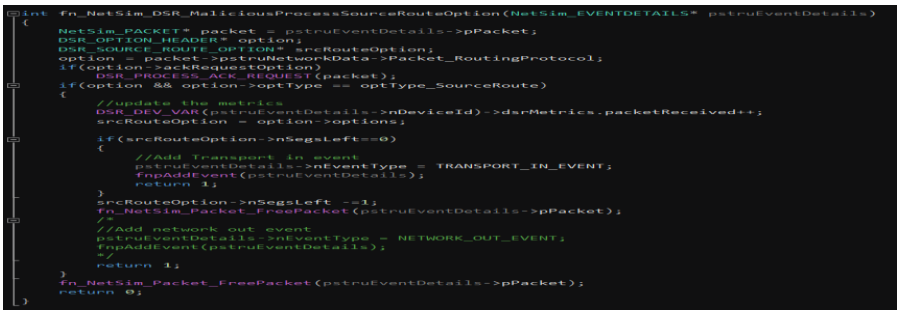
В DSR источник передает пакет RREQ во время обнаружения маршрута. Получатель пакета при получении пакета RREQ отвечает пакетом RREP, содержащим маршрут для достижения пункта назначения. Но промежуточные узлы также могут отправлять пакеты RREP источнику, если у них есть маршрут к месту назначения в их кэше маршрутов. Используя это в качестве преимущества, злонамеренный узел добавляет поддельную запись маршрута в свой кэш маршрутов с целевым узлом в качестве следующего перехода. При получении пакета RREQ от источника вредоносный узел отправляет поддельный пакет RREP с поддельным маршрутом. Исходный узел при получении этого пакета рассматривает это как лучший маршрут к месту назначения. Весь сетевой трафик идет к Sinkhole, и он может либо изменить информацию пакета, либо просто отбросить пакет.

Проект DSR содержит следующие функции:

• fn_NetSim_DSR_MaliciousNode()-Эта функция используется для определения, является ли текущее устройство вредоносным или не для того, чтобы установить вредоносное поведение.

• fn_NetSim_DSR_MaliciousRouteAddToCache () - Эта функция используется для добавления поддельной записи маршрута в кэш маршрута вредоносного устройства с его следующим переходом в качестве пункта назначения.

• fn_NetSim_DSR_MaliciousProcessSourceRouteOption () -Эта функция используется для отбрасывания полученных пакетов, если устройство является вредоносным, вместо пересылки пакета на следующий переход.



```
int fn_NetSim_DSR_MaliciousProcessSourceRouteOption(NetSim_EVENTDETAILS* pstruEventDetails)
{
    NetSim_PACKET* packet = pstruEventDetails->pPacket;
    DSR_OPTION_HEADER* option;
    DSR_SOURCE_ROUTE_OPTION* srcRouteOption;
    option = packet->pstruNetworkData->Packet_RoutingProtocol;
    if(option->ackRequestOption)
        DSR_PROCESS_ACK_REQUEST(packet);
    if(option && option->optType == optType_SourceRoute)
    {
        //update the metrics
        DSR_DEV_VAR(pstruEventDetails->nDeviceId)->dsrMetrics.packetReceived++;
        srcRouteOption = option->options;

        if(srcRouteOption->nSegsLeft==0)
        {
            //Add Transport in event
            pstruEventDetails->nEventType = TRANSPORT_IN_EVENT;
            fnpAddEvent(pstruEventDetails);
            return 1;
        }
        srcRouteOption->nSegsLeft --1;
        fn_NetSim_Packet_FreePacket(pstruEventDetails->pPacket);
        /*
        //Add network out event
        pstruEventDetails->nEventType = NETWORK_OUT_EVENT;
        fnpAddEvent(pstruEventDetails);
        */
        return 1;
    }
    fn_NetSim_Packet_FreePacket(pstruEventDetails->pPacket);
    return 0;
}
```

Рисунок-5. Функция fn_NetSim_DSR_MaliciousProcessSourceRouteOption ()

Поток кода - если узел является вредоносным узлом, то при получении запроса маршрута функция добавляет маршрут от себя к цели в кэше маршрутов и отправляет ложный ответ о маршруте. Когда вредоносный узел получает пакет данных, он дает подтверждение ответа и освобождает пакет.

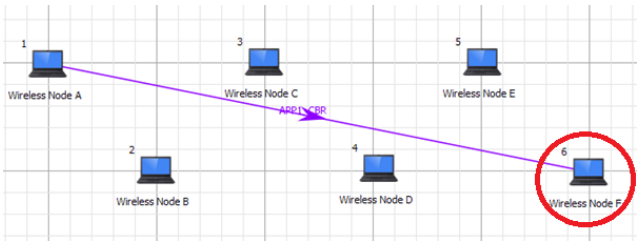


Рисунок-5. Вид в программе NetSim

Источник - идентификатор устройства 1, Назначение - идентификатор устройства 6, Sinkhole (вредоносный узел) - идентификатор устройства 6. Мы обнаружили, что злонамеренный узел (идентификатор устройства 6) дает Route Reply при получении Route Request и привлекает пакеты к себе. Мы также увидели, что злонамеренный узел не пересылает полученные пакеты.

Заключение

Основываясь на существующих работах, большинство исследователей пытаются найти ИКТ-решения для обнаружения, идентификации и обеспечения устойчивости к провалам в БСС. Исследователи использовали схему обнаружения вторжений, основанную на методе аномалий, другие использовали правила, основанные на правилах и управлении ключами, для обнаружения и идентификации узлов провалов. Очень немногим исследователям удалось проверить свою систему безопасности, используя настоящую БСС. Также некоторые результаты показали низкую частоту обнаружения, высокую нагрузку на сеть и высокую стоимость связи. Будущее решение должно быть проверена в реальной сенсорной сети. Благодаря такой проверке будет легко проверить, соответствуют ли их решения доступным ресурсам БСС.

Список использованных источников

1. Al-Sakib Khan Pathan ,Hyung-Woo Lee, ChoongSeon Hong, “Security in Wireless Sensor Networks: Issues and Challenges”, Proc. ICACT 2006, Volume 1, 20-22 Feb, 2006, pp. 1043-1048.

2. Kalpana Sharma, M K Ghose, “Wireless Sensor Networks: An Overview on its Security Threats”, IJCA Special Issue on “Mobile Ad-hoc Networks” MANETs, 2010
3. Zhou WX, Lin S. Malicious Node Recognition Algorithm in Wireless Sensor Networks. Computer Systems and Applications, 2020, 29(2): 175-180(in Chinese).
4. A. Perrig, J. Stankovic, D. Wagner Security in WSN Communications of the ACM, 47(6) (2004), pp. 53-57
5. Rehman, A., Rehman, S.U. & Raheem, H. Sinkhole Attacks in Wireless Sensor Networks: A Survey. Wireless Pers Commun 106, 2291–2313 (2019).
6. S. Deb Roy, S.Singh, S.Choudhury, N. C. Debnath. (2008). Countering Sinkhole and Black hole Attacks on Sensor Networks using Dynamic Trust Management”, ISCC 2008. IEEE Symposium on (pp.537-542). IEEE.
7. Pathan, K., AI-S. (2011) Security of SelfOrganizing Networks-MANET, WSN, VANET, WMN. ISB N-13:978-1-4398-1920-3. Taylor and Francis Group
8. Jaydip Sen. (2009). A Survey on Wireless Sensor Network Security, International Journal of Communication Networks & Information Security, 1(2).
9. Krontiris,I., Dimitriou,T., Giannetsos,T. and Mpasoukos, M. (2008). Intrusion Detection Sinkhole Attacks in Wireless Sensor Network. In Networking and Communications. WIMOB’08. IEEE Interational Conference on Wireless and Mobile Computing, (pp. 526-531). IEEE.
10. Tumrongwittaya and Varakulsiripunth. (2009). Detection of Sinkhole attack in Wireless Sensor Networks, In ICCAS-SICE, 2009 (pp. 1966-1971). IEEE..
11. Chutima, P. and Sujitra, M. “Optimal WSN Design for Efficient Energy Utilization”, Advanced Information Networking and Applications, IEEE Workshops of International Conference, pp. 814-819, Singapore, 2011.
12. Prashant krishan , “A Study on Dynamic and Static Clustering Based Routing Schemes for Wireless Sensor Networks”, International Journal of Modern Engineering Research (IJMER), pp-1100-1104, 2013.
13. Roy, D.S., Singh, A.S. and Choudhury, S. (2008). Countering Sinkhole and Blackhole Attacks on Sensor Networks using Dynamic Trust Management. In Computers and Communications, 2008. ISCC 2008. IEE Symposium on (pp. 537-542). IEEE.
14. Coppolino, L., D’Antonio, S., Romano, L., and Spagnuolo, G.(2010). An intrusion detection system for critical information infrastructures using WSN technologies. In Critical Infrastructure (CRIS), 2010 5th International Conference on (pp. 1-8). IEEE
15. Tumrongwittaya and Varakulsiripunth. (2009). Detection of Sinkhole attack in Wireless Sensor Networks, In ICCAS-SICE, 2009 (pp. 1966-1971). IEEE..
16. Papadimitriou, A., Fessant, L. F. and Sengul, C. (2009). Cryptographic protocols to fight sinkhole attacks on tree based routing in WSN. In Secure Network Protocols, NPSec 2009. 5th IEEE Workshop on (pp.43-48).
17. Hairong Zhao, Wuneng Zhou, Yan Gao, “Energy Efficient and Cluster Based Routing Protocol for WSN” Eighth International Conference on Computational Intelligence and Security, 2012.

УДК 681 5 9 7558

СИНТЕЗ РОБАСТНОГО УПРАВЛЕНИЯ САМОЛЕТОМ В УСЛОВИЯХ ВОЗМУЩЕНИЙ

Маштаева Аида Асильхановна
mashtayeva@mail.ru
Докторант 1-го курса специальности «Автоматизация и управление»
Евразийского национального университета им. Л.Н. Гумилева, Нур-Султан, Казахстан
Научный руководитель – Д.К. Сатыбалдина

Повышенное внимание в авиационной сфере уделяется вопросам обеспечения безопасных условий полета, в особенности в случае неблагоприятной метеорологической