ЎЗБЕКИСТОН РЕСПУБЛИКАСИ АХБОРОТ ТЕХНОЛОГИЯЛАРИ ВА КОММУНИКАЦИЯЛАРИНИ РИВОЖЛАНТИРИШ ВАЗИРЛИГИ

МУҲАММАД АЛ-ХОРАЗМИЙ НОМИДАГИ ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ УРГАНЧ ФИЛИАЛИ

МУҲАММАД АЛ-ХОРАЗМИЙ ИЗДОШЛАРИ

мавзусидаги

Республика илмий-техникавий анжумани

МАТЕРИАЛЛАРИ

2018 йил 27-28 апрель

Урганч - 2018

АТАКИ НА БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ И КОНТРМЕРЫ

Т.М. Бабажанова, Е.Н. Рейпназаров, А.П. Лазарев

Различные типы атак на беспроводные сенсорные сети описаны в этой статье. Чтобы справиться с этими атаками, были предложены основные доступные контрмеры.

Различные формы атак. Большое количество атак может быть выполнено над беспроводные сенсорные сети (Wireless Sensor Networks, WSN) с различными целями [1]. Например, одна из атак может нацеливаться на целостность сообщений, проходящих через четь, в то время как другие стремится уменьшить доступность сети или ее компонентов. Атаки часто возникают путем ввода некоторых интрузивных элементов в сеть [2], [3]. Другие атаки, воздействующие на внешнюю среду, могут косвенно вызвать ухудшение или вмешательство в передаваемые сигналы.

Наиболее известными атаками на WSN являются следующие [4], [5]:

– Помехи: злоумышленник наводняет радиочастоты, используемые сетью, с шумом и может предотвратить обмен сообщениями. Работа сети может быть сильно нарушена, если радио покрытие злоумышленника велико. Последствием этой атаки является отказ в обслуживании (DoS) [6].

– Прослушивание: контроль доступа к сети невозможен, поскольку связь передается по радиоволнам, и, кроме того, сеть может быть развернута в открытой среде, доступной для всех [7]. Таким образом, очень легко перехватить данные, обмениваемые по сенсорной сети и получить доступ к их контенту, если служба конфиденциальности не предоставляется.

– Физическое нарушение (фальсификация): WSN часто развертываются в незащищенных областях, в последствия, злоумышленник может иметь физический доступ к узлам и может нарушать аппаратное обеспечение узлов [8]. Целью может быть извлечение секретной информации такие как криптографические ключи, или для добровольного нарушения работы сети и приложения, что приводит к не стандартному поведению узла.

– Пренебрежение и жадность: злоумышленник полностью или частично удаляет данные сообщения, генерируемые узлом, подверженным атаке [8], [9].

– Выборочная переадресация: узел злоумышленника не направляет сообщение, если требуется [10]. Выбор удаленных сообщений выполняется в соответствии с определенными критериями или случайным образом.

– Воспроизведение, задержка и повреждение данных: злоумышленник повторяет, задерживает или изменяет содержимое сообщений в пути. Сообщения могут содержать собранные данные и данные конфигурации или маршрутизации [11]. Цель состоит в том, чтобы создавать циклы, привлекать или отражать трафик, увеличивать или уменьшать количество маршрутов, генерировать ложные ошибки, разбивать сеть и увеличивать задержку для распределения данных.

– Исчерпание батареи: эта DoS атака имеет решающее значение, так как истощение батареи узлов, составляющих сеть, сильно влияет на срок службы сети. Утечка батареи может быть проведена путем ввода многих сообщений в сеть, чтобы узлы теряли энергию в ненужных повторных передачах [12].

Профилактические механизмы. Предотвращение должно оставаться главной задачей любого сетевого администратора, стремящегося защитить систему. WSN следует защищать от опрокидывания и против вторжения некоторых узлов, которые могли бы подменять личность законного датчика, нарушить маршрутизацию или сильно побудить датчики перераспределить их энергию и сократить срок их службы и т. д [13].

В превентивных механизмах используются криптографические примитивы, чтобы гарантировать конфиденциальность, достоверность, целостность и свежесть информации при транзите по сети. Они защищают все обмены между узлами и базовыми станциями, которые отвечают за сбор данных от датчиков или между двумя соседними узлами. В

последнем случае сообщения защищены перехватом между любыми парами узлов [14], и злоумышленникам очень сложно вмешиваться в сеть, используя свое собственное оборудование. Однако, независимо от надежности этих криптографических примитивов, злоумышленник все равно сможет физически контролировать законный узел, вставить в него вредоносный код и тем самым изменить этот узел на злоумышленника. Физическая безопасность узлов может быть усилена, но до сих пор не известно ни эффективного, ни недорогого метода.

Поскольку превентивные механизмы недостаточны для обеспечения безопасности WSN, необходимо внедрить механизмы допуска к вторжению и развернуть новые инструменты для обнаружения и аннулирования злоумышленников. Это позволит повысить безопасность сети.

Обнаружение злоумышленника. Обнаружение злоумышленника – очень активная тема исследований, даже в традиционных сетях. Основная мотивация разработки систем обнаружения вторжений основана на том, что невозможно создать абсолютно безошибочный защитный механизм [15]. После обнаружения вторжения можно проверить, был ли защитный механизм нарушен, а затем запустить автоматическую реакцию и позволить сетевому администратору принять решение. Кроме того, информация, предоставляемая системой обнаружения вторжений, может использоваться для улучшения защитных механизмов сети.

В системе обнаружения вторжений контролируется и анализируется поведение целевой защиты. Анализ его предполагает, что поведение злоумышленников, нормальное поведение системы или поведение, ожидаемое от системы, известны. Согласно классу рассматриваемых моделей поведения существует две стратегии обнаружения [16], [17]:

– Обнаружение аномалий: наблюдаемое поведение целевой системы сравнивается с нормальным и ожидаемым поведением. Если поведение системы существенно отличается от нормального или ожидаемого поведения, система сталкивается с аномалиями и становится жертвой вторжения.

– Обнаружение злоупотреблений: действия, предпринятые в целевой системе, сравниваются с действиями, которые обычно выполняются злоумышленниками и перечисляются в виде подписей. Интрузия обнаруживается, когда нам удается идентифицировать подпись из анализируемых действий.

Обнаружение злоумышленников в WSN требует совсем другого подхода к сравнению с обычными сетями, поскольку модели, атаки и ресурсы различны. В обычных сетях роль пользователя обычно существует; пользователь – тот, кто использует сеть, и кто генерирует свой профиль трафика [18]. В сенсорной сети события контролируются узлами датчиков, которые генерируют данные и отправляют их в место, где пользователь или наблюдатель могут приступить к их анализу. Поведение пользователя в контексте обнаружения злоумышленника неинтересно, потому что пользователь не влияет на поведение сети, за исключением некоторых редких ситуаций, когда пользователь взаимодействует с сетью для выполнения конфигурации или стимуляции ее [19].

Традиционно возможны две альтернативы для обнаружения вторжений. В централизованном подходе базовая станция извлекает из сети информацию, создаваемую узлами, и отвечает за обнаружение злоумышленников. В децентрализованном подходе все узлы сети или их подмножества наблюдают за своими соседями и выполняют простые операции обнаружения вторжений.

Допуск на вторжение. Допуск вторжения является третьим подходом к обеспечению безопасности. В этом подходе идея состоит в том, чтобы сделать критические функции системы максимально устойчивыми к любым компрометирующим атакам злоумышленника [20].

В контексте WSN маршрутизация лежит в основе большинства работ по толерантности к вторжению. Несколько работ определяют несколько маршрутов для одновременного или альтернативного использования, чтобы гарантировать полную или

частичную доставку сообщений. Некоторые другие работы пытаются установить новые маршруты после обнаружения проблем связи [21]

Некоторые методы допуска к помехам изменяют маршрутизацию сетей путем определения дополнительных маршрутов для каждой пары источника-получателя любых сообщений. Проектирование маршрутизации с несколькими маршрутами обеспечивает полную или частичную непрерывность работы в сети даже в присутствии злоумышленников, действующих на маршрутизацию.

WSN – многообещающая новая технология, из которой могут появиться мощные инструменты для удаленного мониторинга. Для принятия такой технологии, особенно в контексте крайне уязвимых приложений, вопрос безопасности должен быть приоритетом. В этой статье мы представили основные типы атак, вызванных WSN, и три подхода к безопасности.

Литература

1. Турумбетов, Б.К., Джолдасбаева, А.Б., & Рейпназаров, Е.Н. (2014). Ўзбекистонда интернетнинг янги имкониятлари ва LTE технологиясининг ривожланиши. In “XXI аср-интеллектуал авлод асри” шиори остидаги ёш олимлар ва талабаларнинг ҳудудий илмий-амалий конференцияси материаллари, 17-18 июнь (pp.200-202).

2. Файзуллаев, Б.А., Джолдасбаева, А.Б., & Рейпназаров, Е.Н. (2015). Информациялық есаплаў тармақларында мағлыўмат узатыў процесиниң иммитациялық моделин жаратыў. In “Фан, таълим ва ишлаб чиқариш интеграциясида ахборот-коммуникация технологияларини қўллашнинг ҳозирги замон масалалари” Республика илмий-техник анжуманининг маърузалар тўплами, 17-18 июнь (pp.157-161).

3. Turumbetov, B.K., & Reypnazarov, E.N. (2015). GSM tarmog‘ining kommutatsiya va tayanch stantsiyalar tizimining tarkibi. In “Axborot va telekommunikatsiya texnologiyalari muammolari” Respublika ilmiy-texnik konferensiyasining ma’ruzalar to‘plami, 12-13 mart (pp.257-259).

4. Kaipbergenov, B.T., Turumbetov, B.K., Atamuratov, A.T., & Reypnazarov, E.N. (2015). Designing subscriber network according to PON technology. “European Applied Sciences” International scientific journal. Stuttgart, Germany, 9, 45-48.

5. Файзуллаев, Б.А., Турумбетов, Б.К., & Рейпназаров, Е.Н. (2015). Телекоммуникация тармоқларини оммавий хизмат кўрсатиш тизими сифатида тадқиқ этишда ахборот коммуникация технологияларидан фойдаланиш. In “Замонавий фан ва техника ривожида ахборот ва телекоммуникация технологияларининг ўрни” Республика илмий-техник конференциясининг материаллари тўплами, 11-12 сентябрь (pp.203-205).

6. Турумбетов, Б.К., & Рейпназаров, Е.Н. (2016). Мультисервис тармоқларини таҳдидлардан ҳимоялашда Fraud Management ва CRM-тизимлари ҳамкорлиги. In “Ахборот ва телекоммуникация технологиялари муаммолари” Республика илмий-техник конференциясининг маърузалар тўплами, 10-11 март (pp.128-130).

7. Babajanova, T.M., & Reypnazarov, E.N. (2016). The main features of digital radio relay links. In “Фан ва таълим-тарбиянинг долзарб масалалари” Республика илмий-назарий ва амалий анжуман материаллари, 26-27 май (pp.104-106).

8. Каипбергенов, Б.Т., Файзуллаев, Б.А., Смамутов, А.А., & Рейпназаров, Е.Н. (2016). Математическое моделирование абсорбционного процесса на примере производства кальцинированной соды с использованием пакета MATLAB-SIMULINK. Тошкент давлат техника университети хабарномаси. Ташкент, 95(2), 36-41.

9. Турумбетов, Б.К., & Рейпназаров, Е.Н. (2017). Телекоммуникация технологиялари йўналиши талабаларига ихтисослик фанларини ўқитишда виртуал лабораториялардан фойдаланиш. In “Кадрлар тайёрлаш сифатини оширишда ахборот технологияларининг ўрни” Республика илмий услубий конференцияси маърузалар тўплами, 5-6 январь (pp.156-158).

10. Бабажанова, Т.М., Рейпназаров, Е.Н., & Сапарова, Б.М. (2017). Талабаларга IP-тармоқ бўйича реал вақт овозли хабарларини узатиш тамойилларини ўргатишнинг ўзига хосликлари. In “Кадрлар тайёрлаш сифатини оширишда ахборот технологияларининг ўрни” Республика илмий услубий конференцияси маърузалар тўплами, 5-6 январь (pp.173-174).

11. Сиддиков, И.Х., Хужаматов, Х.Э., & Рахмонова, Г.С. (2017). Управляемые гибридные источники электроснабжения для объектов телекоммуникаций. In Материалы конференции “Потенциал интеллектуально одаренной молодежи-развитию науки и образовани”, (pp.121-123).

12. Сиддиков, И.Х., Хужаматов, Х.Э., & Шержанова, Д.С. (2017). Тармоқланган телекоммуникация объектларининг энергия таъминотида гибрид манбаларни ишлатиш ва бошқариш жараёнлари таҳлили. “Muhammad al-Xorazmiy avlodlari” ilmiy-amaliy va axborot-tahliliy jurnal. 2, 35-41.

13. Рахимов, Т.Г., & Рейпназаров, Е.Н. (2017). Рақамли телевидение тизимларида халақитлар ва шовқинлар, уларни бартараф этиш чоралари. In “Иқтисодиётнинг реал тармоқларини инновацион ривожланишида ахборот-коммуникация технологияларининг аҳамияти” Республика илмий-техник анжуманининг маърузалар тўплами, 6 апрель (pp.196-197).

14. Турумбетов, Б.К., & Рейпназаров, Е.Н. (2017). Юқори сифатли маълумотларни реал вақтда узатишда SCTP транспорт протоколини қўллаш. In “Иқтисодиётнинг реал тармоқларини инновацион ривожланишида ахборот-коммуникация технологияларининг аҳамияти” Республика илмий-техник анжуманининг маърузалар тўплами, 6 апрель (pp.244-245).

15. Rakhimov, T.G., & Reypnazarov, E.N. (2017). Integration of terrestrial television broadcasting with mobile communication networks. In “Таълим ва илмий тадқиқотлар самарадорлигини оширишда замонавий ахборот-коммуникация технология-ларининг ўрни” Республика илмий-амалий анжумани материаллари тўплами, 6 май (pp.25-27).

16. Turumbetov, B., Reypnazarov, E., & Seytmambetova, D. (2017). WiMAX texnologiyasi xususiyatlari va imkoniyatlari. In “Таълим ва илмий тадқиқотлар самарадорлигини оширишда замонавий ахборот-коммуникация технология-ларининг ўрни” Республика илмий-амалий анжумани материаллари тўплами, 6 май (pp.307-308).

17. Саттаров, Х.А., & Хужаматов, Х.Э. (2015). Методика развития конструкций датчиков угловых ускорений. Молодежь в науке: Новые аргументы. 204-207.

18. Khujamatov, Kh.E. (2016). The quality of electrical energy in the three-phase electric networks. Проблемы и достижения современной науки. 1, 154-156.

19. Сиддиков, И.Х., & Хужаматов, Х.Э. (2016). Қайта тикланувчи энергия манбаларини ўз ичига олган гибрид энергия таъминоти тизимларининг бошқарувини моделлаштириш ва тадқиқ этиш. “TATU xabarlari” ilmiy-texnika va axborot-tahliliy jurnali. 3, 60-66.

20. Хужаматов, Х.Э. (2016). Телекоммуникация объектларини барқарор электр энергияси билан таъминлашда автоном қуёш электр станциясини қўллаш. “TATU xabarlari” ilmiy-texnika va axborot-tahliliy jurnali. 4, 22-31.

21. Сиддиков, И.Х., Хужаматов, Х.Э., & Хонтураев, И.М. (2017). Современные элементы и устройства контроля одно-и трехфазного электрического тока. Потенциал интеллектуально одаренной молодежи-развитию науки и образования. 2, 119-121.