АНАЛИЗ УЯЗВИМОСТЕЙ АЗН-В НА БАЗЕ 1090 EXTENDED SQUITTER

© 2016 г. И.Д. ГРИГОРЬЕВ, В.Г. ОРЛОВ

Московский технический университет связи и информатики

Автоматическое зависимое наблюдение вещательного типа (АЗН-В, от англ. *Automatic Dependent Surveillane – Broadcast, ADS-B*) – это приложение, функционирующее в рамках концепции организации системы управления воздушным трафиком *CNS/ATM (Communication, Navigation, Surveillance – Air Traffic Management)*. Функционал приложения является резидентной частью данных систем и состоит в периодическом вещании летательными аппаратами (ЛА) сообщений, содержащих в себе идентификационные данные о ЛА и актуальную информацию об их текущем местоположении. ЛА получают информацию о скорости полета и своем положении в географической системе координат с помощью *GPS*-приемника, расположенного на борту. Полученные данные преобразуются в формат сообщения и передаются широковещательным способом с помощью подсистемы передачи *ADS-B Out*. Сообщения принимаются и обрабатываются наземными станциями и ЛА, находящихся в зоне радиовидимости источника сообщений и оборудованных подсистемой приема *ADS-B In*. Архитектура системы представлена на рис. 1.

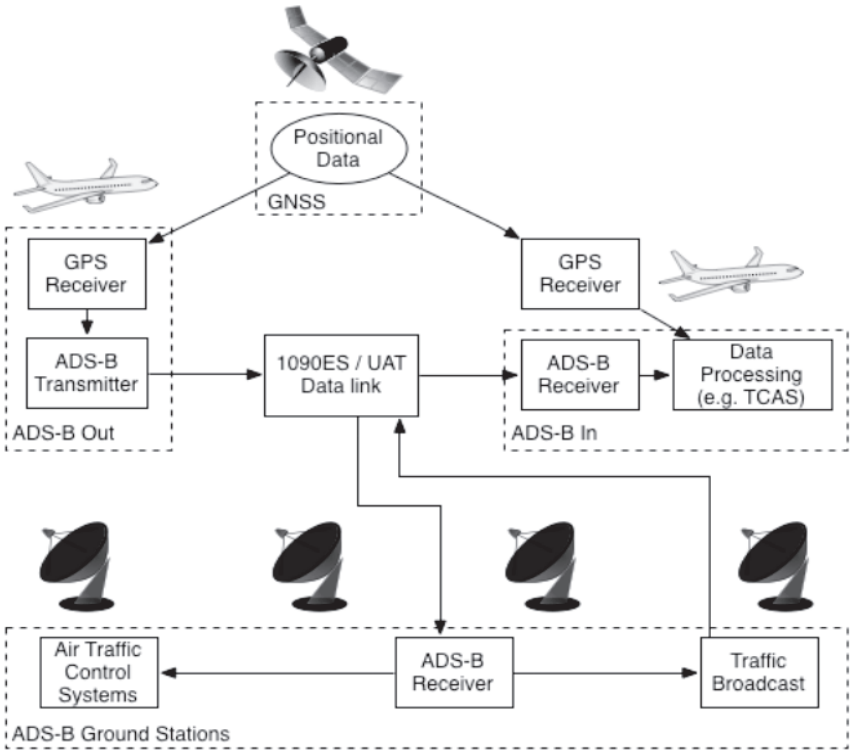

Рис. 1. Архитектура системы АЗН-В.

Одной из систем, занимающихся передачей АЗН-В данных, является 1090 *Extended Squitter*, расширенный сквиттер передатчика режима *S*. Передача происходит на частоте 1090 МГц, используемой для отправки данных от ЛА к другим ЛА и назем-

ным станциям. На рис. 2 представлено графическое отображение процесса передачи одного сообщения, которое начинается с преамбулы, состоящей из двух синхронизирующих импульса. Блок данных передается с использованием *PPM (Pulse-Position Modulation)*. В пределах слота, размером в 1 микросекунду, передается импульс в 0,5 микросекунды. Импульс в первой половине слота является битом, содержащим 1, а во второй половине слота – 0 [1].

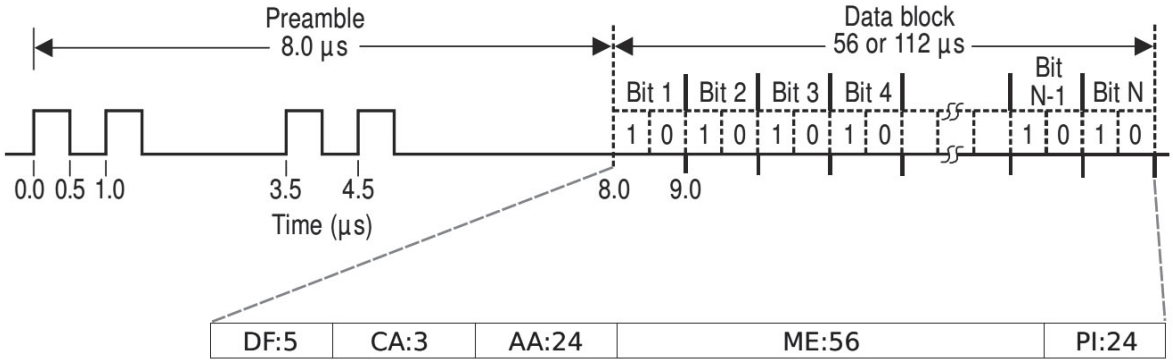

Рис. 2. Формат сообщения 1090 ES.

В стандарте системы режима *S* содержатся данные о сообщениях двух разных размеров: 56 бит и 112 бит [2]. Для передачи АЗН-В данных используется 112-битовый формат сообщения. Поле *DF* содержит тип сообщения, для расширенного сквиттера его значение равно 17. В 56 битах поля *ME* передается полезная нагрузка. В поле *CA* хранится информация о транспондере, а в *AA* – уникальный ИКАО – адрес ЛА, используемый для идентификации. Поле *PI* содержит 24-битовый *CRC* код для обнаружения и коррекции возможных ошибок передачи, с помощью него можно скорректировать до 5 битовых ошибок в сообщении *1090ES*, используя фиксированный порождающий многочлен 24 степени.

Метод множественного доступа, используемый системой – *Random Time Multiple Access*. Правила для отправки и приема АЗН-В сообщений основаны на псевдо - случайном распределении времени передачи и приема сообщений. В стандартной конфигурации работы системы на ЛА, отправка сообщений происходит каждые 500 мсек с отклонением на время, равномерно распределенное на интервале между -100 и 100 мсек.

Простейшей уязвимостью, которой подвержена технология АЗН-В, является возможность подслушивания канала, перехвата и расшифровки незащищенных сообщений. Данная пассивная атака также называется воздушной разведкой [3]. Возможность перехвата сообщений в канале системы была известна еще на ранних стадиях разработки. Данная уязвимость эксплуатируется интернет-сервисами, предоставляющими данные об актуальных рейсах гражданской авиации (ГА), в том числе, визуализируя их. Подслушивания возможно избежать с использованием полного шифрования сообщений, при этом обнаружение самого факта подслушивания в системе практически невозможно. В небольшом перечне стран, например, в Великобритании, имеется законодательная практика преследования злоумышленников, занимающихся прослушиванием незашифрованного широковещательного трафика, не предназначающегося для получателя.

Уязвимостью того же уровня сложности является возможность глушения сигнала, в результате которого один или множество узлов лишаются возможности отправлять и принимать сообщения путём создания сигнала большей мощности на частоте 1090 МГц. Данная уязвимость является типичной для любых систем беспроводной связи, но ее эксплуатация в авиации имеет наиболее опасный характер благодаря возможности создания зон, внутри которых невозможно передать критично важную информацию. Также возможна нацеленная атака на базовую станцию. Глушение традиционных первичных радаров, в отличие от АЗН-В базовых станций, затруднено благодаря вращающимся антеннами более высокой мощности передачи сигнала.

Благодаря отсутствию аутентификации и шифрования в *1090ES*, система уязвима для атак, непосредственно влияющих на целостность передающейся информации. Злоумышленник способен посылать ложные сообщения, от имени действующих ЛА, вводя в заблуждение участников воздушного движения. Противоположной потенциально возможной атакой является «удаление» передающегося сообщения из канала путём использования явления интерференции [4]. Возможно добиться как полного отсутствия сообщения на приемной стороне, так и некоторого количества битовых ошибок в принимаемом сообщении. *CRC* контрольная сумма, содержащаяся в каждом сообщении позволяет исправить на приемной стороне до 5 битовых ошибок на сообщение. Если оно имеет внутри себя более 5 битовых ошибок, то сообщение отбрасывается приемником как поврежденное.

Исходя из наличия вышеописанных уязвимостей определен тип атаки, при котором один или несколько узлов – злоумышленников посылают сообщения *1090ES* с высокой частотой отправки по времени. С целью определить последствия такой атаки и возможные конфигурации, была разработана имитационная модель системы. В качестве среды моделирования использовался симулятор дискретных событий *OMNeT++* с фреймворком *MiXiM*, разработанным для моделирования беспроводных систем связи. Исходные данные указаны в табл. 1.

Таблица 1

Исходные статические параметры модели

Частота передачи	1090 МГц
Мощность передатчика	57 дБм
Чувствительность передатчика	<= -84дБм
Скорость передачи данных	1 Мбит/сек
Длина сообщения	112 бит
Частота отправки сообщения для ЛА	0.24 раз в 1 сек
Размеры площадки	100x100x10 км
Продолжительность моделирования	5 мин

Моделирование производилось при различных изменяемых параметрах в системе. Были получены результаты при нормальной работе системы для различного количества узлов, при работе одного узла-злоумышленника и с работой двух узлов-злоумышленников.

Таблица 2

Процент корректно доставленных сообщений для различных конфигураций

Количество узлов	Частота отправки вредоносных сообщений, мкс.				
	0	1000	100	10	2 x 10
25	93,5%	70,71%	45,28%	41,20%	22,31%
50	93,25%	69,05%	45,25%	41,13%	22,1%

В табл. 2 содержится соотношение количества сообщений, полученных всеми узлами, к количеству отправленных сообщений для зоны с 25 и 50 ЛА. Данное количество узлов выбрано согласно следующим условиям: обеспечение репрезентативности собранной статистики и соответствие реальному среднему количеству ЛА гражданской авиации в зонах активного авиасообщения площадью 10000 кв.км.

В обычном режиме работы при отсутствии злоумышленников с частотой отправки АЗН-В отчетов раз в 500 мс потери сообщений составляют около 7%. Это объясняется способом реализации случайного метода доступа к среде и является нормой. При внедрении одного вредоносного узла, вещающего сообщения раз в 1 мс потери составляют 30%, а с уменьшением интервала ожидания между отправкой сообщений до 10 мкс до получателей не доходит около 59% АЗН-В сообщений. В конфигурациях с двумя атакующими узлами, с частотой отправки отчетов раз в 10 мкс, процент потерь приближается к 80.

На рис. 3 изображены гистограммы, наглядно показывающие количество приня-

тых и отправленных сообщений для каждого узла. Верхняя гистограмма построена для сценария работы системы в нормальном режиме, а нижняя для сценария атаки одним узлом-злоумышленником с частотой отправки сообщений в 10 мкс. Видно, что, благодаря методу случайного доступа к среде, при высокой загруженности канала количество полученных сообщений каждым узлом может значительно разниться при равных условиях. При сценарии атаки узел 3 получил примерно на 100 сообщений больше, чем узел 1, что также является нарушением стабильности работы системы.

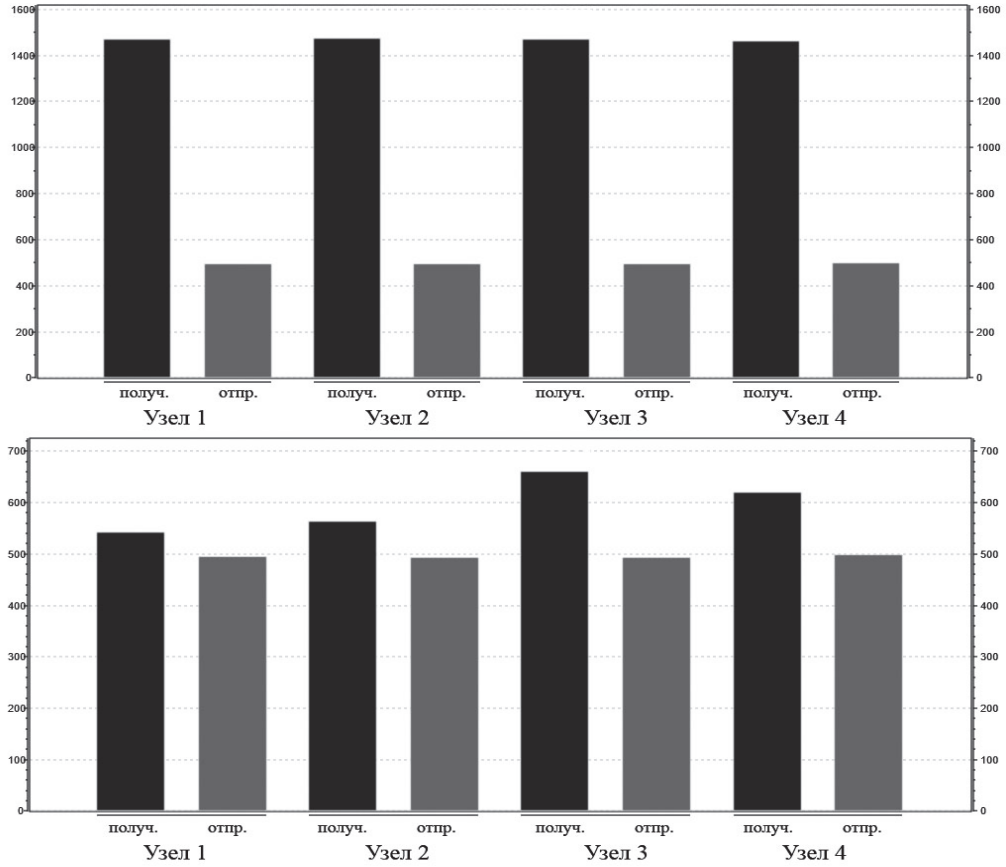

Рис. 3. Статистика сообщений для каждого узла-ЛА.

Таким образом, последствием при реализации атаки данного типа является нарушение ситуационной осведомленности участников воздушного движения, которой подвержены находящиеся в зоне атаки ЛА и базовые станции. При проведении более масштабной атаки на узлы с передатчиками системы 1090 *Extended Squitter* возможны как информационная изоляция ЛА, не позволяющая пилоту получить актуальные навигационные данные о соседних участниках движения, так и внедрение ложной информации о местоположении ЛА диспетчеру с блокировкой корректных АЗН-В сообщений.

СПИСОК ЛИТЕРАТУРЫ

1. RTCA Inc., “Minimum Aviation System Performance Standards for Automatic Dependent Surveillance Broadcast (ADS-B),” DO-242A (including Change 1), Dec. 2006.
2. *Schäfer M., Lenders V., and Martinovic I.* “Experimental Analysis of Attacks on Next Generation Air Traffic Communication,” in Applied Cryptography and Network Security. Springer, 2013, pp. 253–271.
3. *McCallie D., Butts J., and Mills R.* “Security analysis of the ADSB implementation in the next generation air transportation system,” International Journal of Critical Infrastructure Protection, vol. 4, no. 2, pp. 78–87, Aug. 2011.
4. *Wilhelm M., Schmitt J.B., and Lenders V.* “Practical message manipulation attacks in IEEE 802.15.4 wireless networks,” in MMB & DFT 2012 Workshop Proceedings, 2012.