Применение метода вырожденного последовательного анализа для контроля целостности навигационного поля ГНСС ГЛОНАСС

Г. Д. Парамонов[1], В. А. Авдеев[2]

Санкт-Петербургский государственный университет аэрокосмического приборостроения

[1]runken@mail.ru, [2]apex7781@mail.ru

***Аннотация*. Проведен анализ методов контроля навигационного поля глобальных навигационных спутниковых систем. Определены возможные источники имитационных помех. Исследована возможность применения метода вырожденного последовательного анализа для выявления проведенной спуфинг-атаки.**

Ключевые слова: ГЛОНАСС, контроль навигационного поля, автономные алгоритмы контроля целостности, последовательный критерий, имитационная помеха

I. Введение

Технология Глобальной навигационной спутниковой системы (ГНСС) широко используется в обществе с момента ее разработки. В настоящее время широко распространены продукты, основанные на ГНСС. Автомобильные и персональные навигационные устройства, системы навигации и посадки воздушных судов, слежение за дикой природой – вот лишь некоторые из приложений ГНСС. Как следствие, неудивительно, что в последние годы безопасность навигационных данных стала предметом серьезной озабоченности. Сигналы ГНСС чувствительны к помехам, поскольку мощность принимаемого сигнала на земле достаточно мала из-за потерь энергии, происходящих при его распространении. Помимо этого, открытая структура навигационных сигналов делает их уязвимыми к намеренным искажениям [1]. Сигналы постановщика помех приводят к тому, что приемник начинает работать на основе поддельной информации без какого-либо осознания этого со стороны потребителя. Таким образом, подмена, как еще один метод атаки, считается более опасным, чем создание помех и является одой из главных причин нарушения целостности навигационного поля.

II. Спуфинг и возможности противодействия

Как показали последние исследования в предметной области, манипуляции с передаваемой информацией могут выводить из строя современные приемники навигационной информации [2]. Данный факт приводит к снижению эффективности работы транспортной инфраструктуры, логистических систем и многих других приложений [3]. Помимо этого, целостность навигационного поля ГНСС является ключевым фактором в отрасли сельского хозяйства и геоматики, в которых текущие меры по обеспечению безопасности крайне ограничены или же отсутствуют вовсе, поэтому такая угроза как спуфинг-атака является критической.

Принцип данного воздействия можно описать следующим образом. В процессе атаки злоумышленником транслируется поддельный навигационный сигнал [4]. Его характеристики схожи с истинным, однако уровень более высокий. Перехват управления над приемником навигационного сигнала и устройством, в котором он установлен, происходит за счет того, что приемник отдает приоритет сигналам с лучшим качеством приема. Иным способом является трансляция сигнала, согласованного по задержке и доплеровскому сдвигу частоты в точке расположения антенны подавляемого приемника. Начальная энергия ложного сигнала устанавливается низкой и постепенно наращивается до значения, при котором сработает перехват колец слежения. Постепенное нарастание требуется во избежание включения режима блокировки – в нем, как известно, прием данных полностью прекращается, благодаря чему не представляется сложным сделать вывод о ненадежности результатов. Однако при спуфинге такого не происходит, а выходные данные принимаются за качественные. После этого фазово-кодовые соотношения могут быть изменены постановщиком имитационной помехи.

Существует много способов обнаружить подмену, как до, так и после предварительной обработки сигналов. Во втором случае есть метод, основанный на анализе отношения C/N_0 (несущей к шуму), поскольку верхний предел значения C/N_0 может свидетельствовать о подмене. В других исследованиях используют мониторинг качества сигнала (SQM) как метод обнаружения спуфинга в ГНСС. В частности, поскольку взаимодействие между истинными сигналами и сигналами подмены вызывает искажение корреляционной функции, любые аномально повышенные пики корреляции являются признаком наличия подмены. Использование несколько антенн или фазированных антенных решёток позволяет определять направления прихода сигналов ГНСС. Обычно направление прихода истинных сигналов равномерно распределено по небосводу, в то время как ложные

сигналы поступают с одного направления. Однако этот метод может быть применим не для всех потребителей. В данной же работе рассматривается метод, который можно реализовать на программном уровне.

III. Применение метода вырожденного последовательного анализа

Первым шагом является нахождение решения навигационной задачи по данным, полученным из RINEX-файла. Формируется система уравнений на основе эфемерид и измеренных псевдодальностей, производится их линеаризация и решение на основе метода наименьших квадратов и итерационного алгоритма Ньютона. Для дальнейшего исследования берутся невязки измерений, их средние значения и дисперсии, полученные из предыдущих статистических измерений.

Применение метода последовательного анализа заключается в приведении задачи к проверке того, что среднее квадратическое отклонение нормально распределенной случайной величины не превышает заданного значения.

Пусть x – нормально распределенная величина невязок измерений [5]. Предположим, что что качество измерений навигационной системы считается тем более качественным, чем меньше среднее квадратическое отклонение σ. При этом найдется такая величина σ′, что измерение будет считаться аномальным, если σ > σ′, или нормальным, если σ < σ′. Если же σ = σ′, то безразлично, как будет классифицировано измерение. Однако если σ значительно меньше σ′, то классификация измерения как аномального будет обычно рассматриваться, как существенная ошибка. Аналогично, если σ значительно больше σ′. Таким образом, можно задать такие две величины σ_0 и σ_1, что признание измерения аномальным будет серьезной ошибкой если только $\sigma \le \sigma_0$, а для значения σ между σ_0 и σ_1 не имеет особой разницы то, какое решение будет принято.

Величина допустимого риска определяется так: вероятность классифицировать измерение как аномальное не должна превышать заданной малой величины α, когда $\sigma \le \sigma_0$, и вероятность признать измерение нормальным не должна превышать заданной величины β, когда $\sigma \ge \sigma_0$. Плотность вероятности выборки измерений $(x_1, x_2, \dots, x_m)$

$$p_m = \frac{1}{(2\pi)^{\frac{m}{2}}\sigma^m} e^{-\frac{1}{2\sigma^2}\sum_{i=0}^{m}(x_i-\theta)^2},$$

где среднее значение θ предполагается известным.

Последовательный критерий отношений вероятностей производится следующим образом. На каждом этапе проверки вычисляется отношение p_{1m}/p_{0m}. Наблюдения производятся до тех пор, пока

$$\frac{\beta}{1-\alpha} < \frac{p_{1m}}{p_{0m}} = \frac{\frac{1}{\sigma_1^m} e^{-\frac{1}{2\sigma_1^2}\sum_{i=1}^{m}(x_i-\theta)^2}}{\frac{1}{\sigma_0^m} e^{-\frac{1}{2\sigma_0^2}\sum_{i=1}^{m}(x_i-\theta)^2}} < \frac{1-\beta}{\alpha}. \quad (1)$$

После логарифмирования, деления на $\frac{1}{2\sigma_0^2}-\frac{1}{2\sigma_1^2}$ и упрощения неравенство (1) будет иметь вид

$$\frac{2\ln\frac{\beta}{1-\alpha}+m\ln\frac{\sigma_1^2}{\sigma_0^2}}{\frac{1}{\sigma_0^2}-\frac{1}{\sigma_1^2}} < \sum_{i=1}^{m}(x_i-\theta)^2 < \frac{2\ln\frac{1-\beta}{\alpha}+m\ln\frac{\sigma_1^2}{\sigma_0^2}}{\frac{1}{\sigma_0^2}-\frac{1}{\sigma_1^2}}$$

Измерение считается нормальным, если

$$\sum_{i=1}^{m}(x_i-\theta)^2 \le \frac{2\ln\frac{\beta}{1-\alpha}+m\ln\frac{\sigma_1^2}{\sigma_0^2}}{\frac{1}{\sigma_0^2}-\frac{1}{\sigma_1^2}} \quad (2)$$

Измерение считается аномальным, если

$$\sum_{i=1}^{m}(x_i-\theta)^2 \ge \frac{2\ln\frac{1-\beta}{\alpha}+m\ln\frac{\sigma_1^2}{\sigma_0^2}}{\frac{1}{\sigma_0^2}-\frac{1}{\sigma_1^2}} \quad (3)$$

На основе неравенств (2) и (3) для каждого целого значения m вычисляются числа принятия и ошибки

$$a_m = \frac{2\ln\frac{\beta}{1-\alpha}}{\frac{1}{\sigma_0^2}-\frac{1}{\sigma_1^2}} + m\frac{\ln\frac{\sigma_1^2}{\sigma_0^2}}{\frac{1}{\sigma_0^2}-\frac{1}{\sigma_1^2}}$$

$$r_m = \frac{2\ln\frac{1-\beta}{\alpha}}{\frac{1}{\sigma_0^2}-\frac{1}{\sigma_1^2}} + m\frac{\ln\frac{\sigma_1^2}{\sigma_0^2}}{\frac{1}{\sigma_0^2}-\frac{1}{\sigma_1^2}}$$

Эти числа не зависят от исхода испытания и поэтому могут быть вычислены перед началом проверки.

IV. Заключение

Была определена основная постановка метода вырожденного последовательного анализа, примененного к задаче программного обнаружения спуфинга. Дальнейшим направлением исследования

является уточнение оперативной характеристики и среднего значения наблюдений критерия, а затем моделирование предложенного метода в системе MATLAB с использованием реальных данных.

Список литературы

[1] Runzhou Fan GNSS spoofing discovery by type-based and sequential type-based detectors, Department of Electrical & Computer Engineering McGill University Montreal, Canada, 2020.

[2] Мухортов В., Королев И., Шкуринский С. Защита систем спутниковой навигации от внешних программно-аппаратных воздействий // Инновации в науке. 2016. №3-2 (52).

[3] Толстиков А.С., Ушаков А.Е. Противодействие спуфингу и повышение помехоустойчивости аппаратуры потребителя глобальных навигационных спутниковых систем // Интерэкспо Гео-Сибирь. 2018. №9.

[4] Торгашев Б.В., Елагина К.Н. Растущая потребность в кибербезопасности в глобальных навигационных спутниковых системах // Экономика и качество систем связи. 2022. №3 (25).

[5] Вальд А. Последовательный анализ. Государственное изд-во физ.-мат. лит-ры, 1960, 328 с.