УДК 004.056

ОБНАРУЖЕНИЕ FALSE DATA INJECTION АТАК НА СИСТЕМЫ УПРАВЛЕНИЯ

Даненков И.С. (Университет ИТМО)
Научный руководитель – к.т.н, ассистент Юрьева Р.А.
(Университет ИТМО)

В работе рассмотрены подходы и методы защиты систем управления с использованием алгоритмов шифрования. Рассмотрена модель системы управления в общем виде и модель, состоящая из PID регулятора и электропривода. Проведён эксперимент, демонстрирующий эффективность метода и сделана оценка влияния длины ключа RSA на показатели качества управления.

За последние 10 лет произошла существенная интеграция промышленных установок и систем управления с современными информационными технологиями, что значительно повысило количество уязвимостей в системах такого рода. Атаки на такие системы могут нести за собой не только финансовый ущерб, но и ущерб жизням людей, поэтому такая проблема как защита систем управления особенно актуальна. Атака false data injection основана на внедрении вредоносных данных, которые не могут быть обнаружены в качестве ошибочных, из-за особенностей методов обнаружения таких данных.

В данной работе рассмотрен вариант защиты системы управления с использованием алгоритма шифрования RSA. Рассмотрена и проанализирована модель системы управления на основе электропривода и PID регулятора. Для симуляции работы защищённой системы управления использовался пакет Simulink, входящий в состав программного обеспечения Matlab. Атака производилась на обратную связь. Для демонстрации подхода использовались 16-битные ключи, которые сменялись каждые 0,5 секунд. В состав модели системы управления входил детектор ошибочных значений. Каждую секунду на систему управления совершалась атака, которая обнаруживалась только в системе с применением алгоритма шифрования. Атака false data injection, проведённая на незащищённую систему управления, приводит к выводу её из строя, в то время как защищённая система обнаруживает её и позволяет принять меры противодействия, например немедленная остановка процесса, происходящего в динамической системе или безопасная остановка процесса после завершения выполнения текущего задания.

Проведено сравнение графиков значений выходного управляемого сигнала для реализаций систем управления с шифрованием и без, показано незначительное различие, что означает несущественное влияние алгоритма шифрования с заданным интервалом дискретизации управляющего сигнала,. Для реализации в реальных системах предлагается следующее увеличить длину ключей и количество пар ключей.

Даненков И.С. (автор) Подпись

Юрьева Р.А. (научный руководитель) Подпись