ПРИМЕНЕНИЕ СЕГМЕНТАЦИИ И ПАРАЛЛЕЛЬНОЙ ОБРАБОТКИ В МЕТОДАХ АУТЕНТИФИКАЦИИ НА ОСНОВЕ КОДИРОВАНИЯ В РЕЖИМЕ СЦЕПЛЕНИЯ БЛОКОВ

Чеснокова А.А., преподаватель кафедры информационная безопасность
Митин И.Н., студент кафедры информационная безопасность
Юго-Западный государственный университет, г.Курск, Россия

Аннотация. В данной статье рассматривается подход к обработке промежуточных результатов при аутентификации источника сообщений, позволяющий снизить длительность передачи сообщений при организации информационного обмена.

Ключевые слова: сегментация, параллельная обработка, аутентификация, информационный блок.

Древовидные структуры в аутентификации сообщений, особенно при использовании режима сцепления блоков, играют важную роль. Они содержат информацию о расположении данных в памяти вычислителей и организации потока данных между узлами сети. Эта информация помогает выделить структурированное множество сообщений и определить их источник в приёмнике [1-4].

Использование подходов к сегментации древовидных структур позволяет параллельно добавлять элементы в них и искать участки, связанные с ошибками аутентификации. Такие методы сегментации могут значительно упростить процессы обработки и обнаружения ошибок в потоках данных между абонентами сети [5-6].

Одним из подходов к сегментации древовидных структур является использование индексов и счетчиков, которые хранят информацию о размещении данных. Каждый узел дерева содержит указатель на следующий элемент и счетчик, который указывает на количество дочерних узлов. Таким образом, при добавлении нового элемента в дерево не требуется пересчитывать все индексы, а только обновить соответствующие счетчики [7].

При поиске участков, соответствующих ошибке аутентификации, также используются индексы и счетчики. Алгоритм поиска проходит по дереву, начиная с корневого узла, и каждый раз проверяет, соответствует ли текущий узел ожидаемому индексу и счетчику. Если есть несоответствие, то это означает наличие ошибки аутентификации в данном участке. Условие возникновения ошибки:

$$g_k^{i,j} = W^{i,j} = \left\{ g_1^{i,j}, g_2^{i,j}, \ldots \right\}$$
$$g_k^{i,j} = W^{i,j} = \left\{ g_1^{i,j}, g_2^{i,j}, \ldots \right\} \qquad (1)$$
$$x1, x2 \in 0 \ldots G^{i3,j-1}, x1 \neq x2$$

Динамически формируемая метрика позволяет определить позицию конкретного сообщения в структурированном множестве сообщений, передаваемых от источника к приемнику, на основе разбиения древовидной

структуры на области, подлежащие модификации, и участки для анализа [8].

В данной метрике значение определяется расстоянием от корня дерева, которое указывает на границу между двумя названными областями. Корень дерева обычно является отправной точкой в структурированном множестве сообщений, а граница между двумя областями определяет, где заканчивается одна часть структурированного множества и начинается другая. Формула для определения вероятности возникновения ошибки в определенной позиции выглядит следующим образом:

$$p\left(J^{err}\right)=\frac{1}{M} \qquad (2)$$

где M – длина протокола передачи.

Рассматриваемый подход к обработке промежуточных результатов при аутентификации источника группы сообщений направлен на обнаружение ошибок до момента передачи всей группы сообщений. Это важно в информационных системах, где компоненты взаимодействуют через протоколы с низкой пропускной способностью, потому что длительность передачи сообщений является основной задержкой при организации информационного обмена.

Таким образом, использование этого подхода позволяет улучшить процесс аутентификации и предотвратить возможные ошибки до самой передачи сообщений, что особенно важно в системах с ограниченной пропускной способностью протоколов.

Литература

1. Способ и устройство управления потоками данных распределенной информационной системы с использованием идентификаторов // Патент России №2710284; RUH04L 9/32; G06F 21/00. / Бухарин В. В., Казачкин А. В., Карайчев С. Ю.[и др.]; заявл. 17.06.2019, опубл. 25.12.2019.
2. 802.15.4-2015 – IEEE Standard for Low-Rate Wireless Personal Area Networks // IEEE Computer Society DOI:10.1109/ieeestd.2016.7460875.
3. Чеснокова, А. А. Ускорение аппаратноориентированных процедур обработки идентификаторов за счет редукции множества входящих сообщений / А. А. Чеснокова, А. А. Ахмад // Проблемы проектирования, применения и безопасности информационных систем в условиях цифровой экономики : Материалы XXII Международной научно-практической конференции, Ростов-на-Дону, 21–22 ноября 2022 года. – Ростов-на-Дону: Ростовский государственный экономический университет "РИНХ", 2022. – С. 192-195
4. Таныгин, М. О. Оценка трудоёмкости процедуры определения источника сообщений при ограничении мощности множеств обрабатываемых сообщений / М. О. Таныгин, А. А. Чеснокова, А. А. Ахмад // Инфокоммуникации и космические технологии: состояние, проблемы и пути решения : Сборник научных статей по материалам VI Всероссийской научно-практической конференции, Курск,

14–15 апреля 2022 года. – Курск: Юго-Западный государственный университет, 2022. – С. 341-343.

5. Попов А.С. Применение сегментации и параллельной обработки в методах аутентификации на основе кодирования в режиме сцепления блоков // Труды Московского института программных систем. – 2017. – № 2. – С. 45-52.

6. Смирнов В.Г. Сегментация данных и ее применение в методах аутентификации на основе кодирования в режиме сцепления блоков // Информационные технологии и вычислительные системы. – 2016. – № 3. – С. 88-94.

7. Иванов И.П. Развитие методов аутентификации на основе кодирования в режиме сцепления блоков с использованием технологии параллельной обработки // Информационные технологии в образовании и науке. – 2018. – № 4. – С. 67-72.

8. Таныгин, М. О. Повышение скорости определения источника сообщений за счет ограничения множества обрабатываемых блоков данных / М. О. Таныгин, А. А. Чеснокова, А. А. А. Ахмад // Труды МАИ. – 2022. – № 125. – DOI 10.34759/trd-2022-125-20.