ПРИМЕНЕНИЕ БЛОКЧЕЙН-ТЕХНОЛОГИИ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕЙ MANET

Самойлов Николай Юрьевич

студент, Омский государственный технический университет, РФ, г. Омск

Аверченко Артем Павлович

научный руководитель,

Аннотация. Технология MANET представляет собой беспроводные самоорганизующиеся сети, и в будущем она может сыграть главную роль в развитии интернета, однако на данный момент эта технология широко не используется в связи с наличием нерешенных проблем. Такими проблемами являются обеспечение безопасности, доверенности между узлами, энергоэффективности и маршрутизации. Одним из предложенных решений является внедрение технологии блокчейн, которая может обеспечить требуемую доверенность между узлами сети.

Ключевые слова: MANET, блокчейн, OLSR, AODV

I. Введение

Принцип построения мобильных ad hoc сетей появился более 20 лет назад, но до сих пор так и не нашел широкого применения, разве что на небольших локальных участках. Связано это с тем, что в текущих реалиях развития сетевых технологий у MANET остаются нерешенными такие проблемные стороны, как безопасный и доверенный обмен информацией между мобильными узлами, а также корректная и энергоэффективная маршрутизация между ними. Стандартные протоколы защиты не могут быть использованы в такой топологии по следующему ряду причин:

1. Децентрализованность означает отсутствие посредников (серверов) при обмене данными между двумя узлами, а значит такой метод информационной безопасности, как центр сертификации не применим в MANET;
2. Мобильность маршрутизаторов (узлов), их постоянное хаотичное перемещение приводит к частым соединениям и разъединением между узлами, что накладывает существенные трудности на процессы аутентификации и безопасной маршрутизации. Мобильные устройства должны самостоятельно правильно определять уровень доверия к соседям и передавать информацию об этом всем участникам сети;
3. Мобильные ad hoc сети – это транзитные сети, то есть узлы-отправители и узлы-получатели одновременно являются узлами-маршрутизаторами. Совмещение этих двух задач приводит не только к повышенной нагрузке на сеть и увеличенному энергопотреблению, но и создает благоприятный фон для проведения DDOS-атак (атак на вычислительные способности сети с целью довести ее до отказа с помощью большого количества ложных запросов);
4. Мобильные устройства никак не защищены физически. Злоумышленник может получить доступ к узлу с высокой репутацией, а затем объявить себя кратчайшим путем, благодаря чему будет способен пропускать через себя весь трафик. Такая

манипуляция позволит ему перехватывать чужие сообщения (атака «Черная дыра») и, а также уменьшить пропускную способность определенного участка сети (атака «Воронка») [1]. Также физическая незащищенность узлов позволяет криптоаналитику проводить различные виды атак по побочным каналам (Side-channel attack). Подробнее угрозы информационной безопасности MANET-сетей рассмотрены в статье [2].

В связи с наличием таких тяжелых условий работы мобильных ad hoc сетей необходимо прибегать к нестандартным методам защиты информации.

Одним из недавно предложенных решений имеющихся проблем было внедрение блокчейн в MANET. Отличительной особенностью данной технологии является ее способность обеспечить требуемую доверенность между узлами сети за счет возможности распределенного хранения неизменяемых данных об этих узлах. Идея записывать информацию в блоки была придумана еще в 90-х годах, но только в 2008 году смогли реализовать систему, где каждый из блоков содержит новую информацию и хеш (сжатый до определенного количества знаков произвольный массив данных) предыдущего блока [3]. При изменении информации в определенном блоке имеющейся цепочки меняется его хеш. В связи с этим преобразуется содержимое всех последующих блоков, что делает невозможным бесследную подмену информации. Автором данного исследования является анонимный программист под псевдонимом «Сатоши Накамото». Изначально применение блокчейн-технологии видели только в банковском деле (идея «Сатоши» была реализована в платежной системе «Биткоин»). Однако в блоки помимо денежных транзакций, можно записывать любую информацию, по этой причине блокчейн используют в различных сферах: в здравоохранении [4] в избирательном процессе [5].

В настоящей статье будет рассмотрен вопрос применения блокчейн для обеспечения необходимого уровня информационной безопасности в мобильных ad-hoc сетях.

II. Принцип работы «Blockchain» в MANET-сетях

При организации маршрутизации в MANET нужно учитывать возможное влияние злоумышленников, такое как перехват информации путем неверно адресованной пересылки пакетов. Согласно имеющейся задумке блокчейн будет записывать в себе информацию касательно поведения отдельных узлов, все «хорошие» и «плохие» действия.

MANET состоит из разных устройств – от слабых с малой вычислительной мощностью и объемом АКБ до сильных, у которых вычислительная мощность значительно выше, а заряд АКБ достаточен для длительной, тяжелой работы. Для реализации блокчейн в MANET узлы с высокой вычислительной мощностью и длительным временем работы должны заниматься майнингом, т.е. записью в блоки информации касательно «плохих» и «хороших» действий окружающих узлов и последующей широковещательной рассылкой нового блока. После рассылки все остальные майнеры и узлы смогут оценить уровень доверия к соседям и организовывать более безопасную маршрутизацию.

Не каждый узел сети MANET имеет техническую возможность хранить у себя копию блокчейн или решать задачи по поиску новых блоков с последующей записью информации в них, поэтому данную работу делают за него майнеры. У каждого майнера есть условная территория, путь к которому от узла будет наименьшим. Такие территории отмечены на рисунке 1. Узлам в пределах данной территории майнеры дают возможность подключаться к себе как к ноде (компьютеру децентрализованной сети, контактирующему посредством P2P-протоколов для обмена информацией о блоках и транзакциях). Узлы, являясь участниками сети MANET, постоянно синхронизируется с нодами (майнерами), сравнивая информацию о своих узлах досягаемости с той, что есть в блокчейн. В том случае, если появляется информация о злоумышленном узле или ином, на который по каким-либо причинам нельзя отправлять пакет, и он имеется в списке досягаемых, то узел запоминает эту информацию и руководствуется ею в случае дальнейшей пересылки пакетов. В примере организации MANET на рис. 2 имеется два майнера (М1 и М2). Устройство 1 (далее У) отправляет сообщение, предназначенное У8. Первоначально У1 анализирует своих соседей на вредоносность, сопоставляя их с имеющейся информацией в блокчейн. После подтверждения информации о том, что окружающие узлы не являются вредоносными, и на основе уровня сигнала У1

выбирает, например, У2. У2, получив пакет, повторяет те же самые действия, в процессе которых обнаруживает вредоносный узел У5, которому пересылать пакет нельзя. Поэтому он пересылает на У4. В процессе выбора следующего пункта назначения обнаруживается вредоносный узел У5, а У6, дойдя до критического уровня заряда АКБ, совершает широковещательную рассылку с целью уведомить окружающие узлы о невозможности на неопределенный период совершать им ретрансляции. Руководствуясь всей этой информацией, У4 принимает решение об отправке сообщения на У7, которое, повторяя аналогичные действия, пересылает пакет адресату. На рисунке 2 приведен пример организации MANET параллельно с сотовой связью, благодаря которой можно отправлять пакеты за границу зоны покрытия MANET. Внутри сети пакет будет ретранслироваться между устройствами, и если учесть плотность их расположения в городской среде, то данный тип связи можно считать конкурентоспособным. Помимо этого, у станций сотовой связи есть свои зоны покрытия, в которые устройство может не попасть. В таком случае, если имеется узел MANET в пределах досягаемости, то он может ретранслировать запрос на станцию сотовой связи, тем самым реализуется расширение зоны покрытия.

III. Анализ предлагаемых вариантов применения Blockchain в MANET

В течение минувшего пятилетия было проведено большое количество исследований методов защиты информации в MANETs с помощью блокчейн. В данной работе были выделены наиболее содержательные статьи, которые в перспективе могут внести значительный вклад в развитие данного направления.

В работе [6] представлена система установления доверия на основе блокчейн, обеспечивающая распределенное, последовательное и защищенное от несанкционированного доступа хранение данных обо всех «хороших» и «плохих» действиях узлов мобильной ad hoc сети. Авторами учтена та нагрузка на вычислительные, пропускные и энергетические ресурсы MANET, которую подразумевает реализация блокчейн на широко используемом механизме консенсуса с доказательством работы (Proof-of-Work). Они предлагают использовать упрощенный основанный на консенсусе алгоритм «Delegated proof-of-trust» (DPoT) на базе проактивного протокола маршрутизации OLSR [7]. В такой реализации майнером может стать только узел с высоким показателем trust value (TV), т.е. с высоким уровнем репутации. TV накапливается в течение некоторого промежутка времени за счет оценок от других узлов. Сам по себе узел не может стать валидатором (майнером), ему требуется сосед, которому он отправляет заявку. Сосед пересылает заявку другим узлам с целью удостовериться в честности будущего майнера, а затем уже принимает решение.

В результате испытаний на базе симулятора NS-3 предложенная система оказалась эффективной для поиска уязвимостей. Еще одним достоинством стало значительное сокращение накладных расходов сети при повторных атаках тех же узлов. В статье [8] рассмотрена схема маршрутизации по самому короткому и наиболее известному пути, называемая BC-AODV (т.е. она базируется на реактивном протоколе маршрутизации AODV [7]), основанная на распространении информации о репутации через блокчейн. Если OLSR нагружает сеть периодической рассылкой сообщений «приветствия» и «контроля», то AODV предоставляет маршрут до адресата по требованию. Особенность же BC-AODV заключается в том, что информация о хорошем поведении (промежуточный узел осуществляет правильную пересылку предполагаемому соседу исходного узла) и плохом поведении (отбрасывание пакетов, изменение предполагаемого пути, истечение времени приема), заносится в блоки. Поле hop-count в сообщении RREQ в AODV заменяется полем route cost, которое увеличивается вместе со стоимостью канала на каждом проходящем узле. Роль «сторожей» выполняют майнеры, предполагается, что каждый майнер способен определить, является ли действие узла хорошим или плохим, благодаря сторожевому модулю (watchdog module). Майнерам в разных сетках назначаются разные значения сложности, так что среднее время создания действительного блока из каждой сетки остается постоянным. Следовательно, сетка с более высокой концентрацией майнеров может позволить создать блок с более высокой сложностью, в то время как сетка с меньшим количеством майнеров будет прибегать к меньшей сложности для добычи блока за то же время. В заключении работы BC-AODV был подвергнут сравнительному испытанию со стандартным протоколом маршрутизации AODV. Изначально кол-во отброшенных пакетов было одинаково в обоих случаях, так как требуется время для оценки поведения, но как только процедура оценивания была завершена, кол-во

отброшенных пакетов в BC-AODV резко снизилось, что нельзя сказать про AODV.

Авторами всех рассмотренных в настоящей статье исследований были предложены способы борьбы с информационными угрозами в MANET, основанные на одной технологии блокчейн, но на разных принципах консенсуса и протоколах маршрутизации. Недостатком DPoT стало использование проактивного протокола OLSR, сильно нагружающего пропускную способность сети. В BC-AODV не был рассмотрен процесс выбора майнеров среди всех узлов сети.

IV. Ключевые направления развития

В настоящее время стремление к децентрализации является повсеместным явлением, в частности, потому что лишает третьих лиц возможности управления личными данными пользователей. Распределенное хранение в связке с передачей информации от пользователя к пользователю с помощью ретрансляции пакета данных через узлы самоорганизующейся сети обеспечивает возможность реализации настоящей децентрализации, т.к. сообщение передается по различным путям, а не по иерархичной структуре, после чего остается храниться на устройствах пользователей или на их домашних серверах. Внедрение блокчейн в MANET позволяет создать более надежную сеть за счет записи оценок действий узлов.

Отрицательным моментом является высокая нагрузка на сеть, связанная с обменом найденными блоками, а также постоянными запросами к нодам с целью получения новой информации о состоянии блокчейн от обычных узлов. Кроме того, появление майнеров в сети означает зависимость ее устойчивости от их количества. При слишком большом количестве узлов-посредников ноды могут перестать успевать обрабатывать запросы, благодаря чему не будут способны делиться информацией, записанной в блоках, что понизит безопасность и пропускную способность сети

Приоритетным направлением развития должна стать работа над подстройкой технологии блокчейн под реалии работы в самоорганизующихся сетях с целью облегчения процесса майнинга, и как следствие, увеличению числа майнеров в сети.

V. Заключение

В настоящей статье рассмотрено внедрение блокчейн-технологии в MANET, проанализированы различные варианты ее реализации, основанные на разных принципах консенсуса и протоколах маршрутизации. В результате сравнения не было найдено совершенного решения, каждое из них имеет свои недостатки.

Список литературы:

1. Никонов, В. И. Проблемы безопасности протоколов маршрутизации в самоорганизующихся сетях беспроводных мобильных устройств / В. И. Никонов, Г. С. Никонова // Техника радиосвязи. – 2017. – № 4(35). – С. 23-34.

2. Актуальные вопросы обеспечения безопасности в MANET-сетях / Е. А. Брониковский, В. И. Никонов // Динамика систем, механизмов и машин. – 2020. – Т. 8. – № 4. – С. 113-119. – DOI 10.25206/2310-9793-8-4-113-119.

3. S. Nakamoto. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. [Online]. Available at: https://bitcoin.org/bitcoin.pdf.

4. Цыганов, С. Н. Возможности применения технологии блокчейн в здравоохранении / С. Н. Цыганов // Перспективы развития науки и образования : Сборник научных трудов по материалам XXI Международной научно-практической конференции, Москва, 30 сентября 2017 года / Под общей редакцией А.В. Туголукова. – Москва: Индивидуальный предприниматель Туголуков Александр Валерьевич, 2017. – С. 123-126.

5. Авилов, Я. Д. Перспективы применения технологии "блокчейн" в избирательном процессе:

способы реализации и правовая основа / Я. Д. Авилов // Юридическая наука. – 2017. – № 6. – С. 159-165.

6. Lwin, M.T.; Yim, J.; Ko, Y.-B. Blockchain-Based Lightweight Trust Management in Mobile Ad-Hoc Networks. Sensors 2020, 20, 698. https://doi.org/10.3390/s20030698

7. Павлов Алексей Андреевич, Датьев Игорь Олегович Протоколы маршрутизации в беспроводных сетях // Труды Кольского научного центра РАН. 2014. №5 (24).

8. M. A. A. Careem and A. Dutta, "Reputation based Routing in MANET using Blockchain", 2020 International Conference on COMmunication Systems & NETworkS (COMSNETS), Bengaluru, India, 2020, PP.