Распределенное самозапускающееся вторичное управление частотой на основе хэш-технологии, устойчивое к FDI атакам, для изолированных микросетей

Син Хуан, Ю Линь[*], Дунлянь Ця [a,b,*], Юньфэн Яна [a,b], Шаохуа Ян [c], Ин Вэн [a], Сяньбо Ван [b]

[a] Институт Электротехники, Чжэцзянский Университет, г. Ханчжоу 310027, КНР

[b] Хайнаньский институт Чжэцзянского университета, г. Санья 572000, КНР

[c] Государственная ключевая лаборатория Интернета вещей для умного города, Университет Макао, 999078, Специальный административный район Макао, Китай

Аннотация. Учитывая быстрое развитие современных информационных систем, микросети (МС) страдают от большего количества потенциальных атак, которые влияют на их эксплуатационные характеристики. Традиционное распределенное вторичное управление с небольшим фиксированным периодом времени выборки неизбежно приводит к расточительному использованию коммуникационных ресурсов. В данной статье предлагается схема самозапускающегося вторичного управления при возмущениях от FDI атак. Мы разработали линейный тактовый генератор для каждой DG для запуска его контроллера в апериодические и прерывистые моменты времени. Впоследствии был разработан защитный механизм на основе хэша (HDM) для обнаружения и устранения вредоносных данных, проникших в МС. С помощью HDM схема самозапускающегося управления достигает целей вторичного управления даже при наличии FDI атак. Строгий теоретический анализ и результаты моделирования показывают, что внедренная схема вторичного управления значительно снижает затраты на связь и повышает устойчивость МС к FDI атакам.

Ключевые слова: Микросети; Распределённое вторичное управление; Самостоятельно запускаемое управление; Хэш-алгоритм; Атака с использованием ложных данных

0 Введение

Тесная интеграция киберсетей и физических энергосистем стимулировала развитие киберфизических систем (КФС) [1,2]. Микросети переменного тока (МС) являются типичными активными КФС распределительных сетей, которые наследуют характеристики КФС [3,4]. Однако повсеместное применение передовых информационных технологий в МС является палкой о двух концах: с одной стороны, оно обеспечивает многочисленные преимущества, такие как большая гибкость, надежность и адаптивность для работы МС; с другой стороны, оно представляет более высокий риск для безопасности и устойчивости МС, особенно в более сложной внешней среде [5].

МС могут работать как в режиме подключения к сети, так и в изолированном режиме. Иерархическая структура управления признана эффективной схемой, которая включает три уровня управления: первичный, вторичный и третичный [6]. Среди них вторичное управление имеет наиболее важное значение для надежной работы МС в изолированном режиме, поскольку приоритетной целью изолированных МС является поддержание эксплуатационной стабильности. Вторичное управление можно разделить на централизованное[7], децентрализованное[8] и распределенное[9]. Централизованное вторичное управление требует наличия мощного центра управления и сложной сети связи «один ко всем» для достижения цели вторичного управления. Однако его недостатками являются наличие единой точки отказа и очень плохая масштабируемость. Напротив, децентрализованное вторичное управление достигает целей управления локально, не задействуя какую-либо связь; однако оно не может поддерживать точную оптимизацию глобальных целей. Однако распределенное вторичное управление сочетает в себе преимущества локального

управления и соседней связи, что соответствует практическим применениям МС. Поэтому мы уделяем больше внимания распределенному вторичному управлению [10].

Было исследовано несколько распределенных стратегий вторичного управления для достижения вторичного управления МС распределенным образом [11–13]. Однако все вышеупомянутые стратегии распределенного вторичного управления основаны на непрерывных во времени контроллерах, которые потребляют большой объем коммуникационных и вычислительных ресурсов, когда МС входят в стационарный режим работы. Чрезмерное использование полосы пропускания связи может привести к перегрузке связи и увеличению затрат, что способствует разработке метода для дискретного и апериодического режима связи [14].

Следовательно, для решения этих проблем (таких как нерациональное использование ресурсов) вводятся протоколы связи, запускаемые событиями. Существующие исследования показали, что механизмы связи, запускаемые событиями, могут значительно снизить нагрузку на передачу данных, сохраняя при этом заданную производительность работы в МС [10,14-17]. В [14] была предложена распределенная стратегия управления, запускаемая событиями, с надлежащими условиями проверки для одновременного достижения восстановления частоты и равномерного распределения мощности. В [17] был принят метод управления, запускаемый событиями, для решения проблемы распределения мощности в подключенных к сети МС переменного тока. Однако для каждого DG, оснащенного механизмом связи, запускаемой событиями, требуется выделенный наблюдатель для обнаружения условий срабатывания в реальном времени. Это может значительно увеличить потребление мониторинга через аппаратные устройства. Кроме того, эффект Зенона [18] должен быть явно исключен, путем обеспечения того, чтобы минимальный интервал смежных событий был больше нуля, что не может быть гарантировано стопроцентно.

Принимая во внимание вышеупомянутые проблемы, самозапускающееся управление считается лучшим решением. С помощью самозапускающегося управления каждый DG автоматически вычисляет следующий момент срабатывания на основе текущих состояний [19-21]. Однако требуется непрерывное прослушивание, поскольку соответствующий момент срабатывания вычисляется во время выполнения в [19,20]. В самозапускающийся контроллер вводится локальная переменная часов, чтобы избежать избыточного наблюдения и прослушивания.

Хотя самозапускающиеся контроллеры могут значительно снизить нагрузку на мониторинг и связь, они по-прежнему подвержены различным кибератакам и вызывают общесистемные эффекты, такие как катастрофический каскадный отказ в МС. Например, отключение энергосистемы Украины в декабре 2015 года было признано знаковой кибератакой на энергосистемы [22]. К конкретным кибератакам относятся инъекция ложных данных, обман и атаки типа «отказ в обслуживании» [23–26]. Среди этих угроз FDI атаки считаются наиболее разрушительными, поскольку они могут быть легко созданы злоумышленниками и приспособлены для распределенного вторичного управления. В этом исследовании основное внимание уделяется FDI атакам. В последнее время широко исследуются подходы, включающие методы, устойчивые к FDI атакам. В [27] авторы предложили новый адаптивный консенсусный контроллер для обеспечения равномерной конечной ограниченности и сопротивления FDI атакам. Однако FDI атака, смоделированная в [27], представляет собой непрерывную во времени атаку, которую трудно запустить на практике из-за ограниченных ресурсов. Поэтому стохастические FDI атаки, подчиняющиеся распределению Бернулли, были систематически смоделированы в [28], где был разработан алгоритм управления на основе наблюдателя, запускаемый событиями, для достижения консенсуса $H\infty$ и обнаружения неисправностей при FDI атаках. Однако такой алгоритм в значительной степени полагается на конкретную математическую модель и не подходит для иных сценариев неопределенности. Основные недостатки текущих исследований заключаются в следующем:

1) Существующий самозапускающийся контроллер по-прежнему требует постоянного прослушивания для определения следующего момента срабатывания.

2) Методы защиты от FDI атак не всегда практичны из-за их ограниченной энергии.

Эти анализы побудили автора данного исследования предложить стратегию распределенного самозапускающегося управления, устойчивую к FDI атакам, основанную на хэшировании, для дальнейшего снижения затрат на связь и повышения устойчивости МС, ориентированных на атаки. Ниже представлены основные выводы данного исследования**:**

1) Мы предлагаем линейный распределенный самозапускающийся механизм на основе тактового сигнала для локального распределения активной мощности и восстановления частоты, который решает проблему экономичного вторичного управления. В частности, с помощью этой самозапускающейся конструкции цели управления могут быть достигнуты с помощью апериодических и прерывистых управляющих воздействий, что значительно снижает затраты на мониторинг и связь, исключая при этом эффект Зенона.

2) Мы исследуем спонтанные FDI атаки на основе распределения Бернулли, которые являются более распространенными и практичными для распределенного самозапускающегося контроллера. Создав модель спонтанной FDI атаки, мы проанализировали принцип того, как спонтанные FDI атаки влияют на передаваемые данные, что закладывает необходимую основу для разработки алгоритмов, устойчивых к атакам.

3) Мы предлагаем защитный механизм на основе хэширования (HDM) для противодействия спонтанным FDI атакам на коммуникационную сеть самозапускающейся вторичной системы управления. Используя HDM, спонтанные FDI атаки могут быть эффективно обнаружены и устранены, что значительно повышает устойчивость МС к атакам.

Следующая часть статьи организована следующим образом: в разделе 1 представлены предварительные сведения о модели микросетевой системы. В разделе 2 представлены наши основные стратегии, связанные с троичными самозапускающимися контроллерами, моделью спонтанной FDI атаки и HDM. В разделе 3 проведено численное моделирование с использованием инструментария MATLAB/Simulink для проверки эффективности предлагаемой схемы управления. Наконец, в разделе 4 представлены выводы.

1 Система управления в микросетях

В этом разделе мы кратко рассмотрим иерархическую структуру управления и распределенное вторичное управление, необходимые для моделирования систем МС.

1.1 Иерархическая структура управления

Трехуровневая иерархическая структура управления с различными временными масштабами всегда реализуется для повышения стабильности и устойчивости изолированных МС. Первичное управление с использованием механизма управления спаданием играет важную роль в балансировке нагрузок и генерации. Характеристики спада можно обобщить следующим образом

$$\begin{cases} \omega_i = \omega_{ni} - m_{pi} P_i \\ \upsilon_i = V_{ni} - n_{qi} Q_i \end{cases}, \qquad (1)$$

где ωni и V ni относятся к первичным опорным значениям частоты и напряжения i-го DG соответственно; ωi и υi относятся к частоте и амплитуде напряжения соответственно; Qi и Pi представляют собой измеренную реактивную мощность и активную мощность на клеммах i-го DG соответственно; а nqi и mpi представляют собой коэффициенты спада.

.

Однако регулятор статизма неизбежно может вызвать отклонения частоты и напряжения. Поэтому для устранения отклонений, вызванных первичным регулированием на основе статизма, требуется вторичное регулирование, одновременно гарантируя точное распределение активной мощности между DG. Вторичное регулирование устанавливает задания ωni и V ni по отдельности для регулирования частоты и амплитуды напряжения до номинальных значений. Таким образом, можно достичь следующих вторичных целей, используя в качестве примера вторичное регулирование ω-P**.**

$$\lim_{t\to\infty} |\omega_i - \omega_{\text{ref}}| = 0 \qquad (2)$$

где i=1,2,⋯,n, a ωref установлено на 50 Гц**.**

$$m_{p1}P_1 = \cdots = m_{pn}P_n \qquad (3)$$

Третичный контроль придает большее значение экономической эффективности и оптимальному управлению МС. Кроме того, в этом исследовании мы не обсуждали третичное управление, поскольку приоритетной целью изолированных МС является поддержание эксплуатационной стабильности**.**

1.2 Стратегия распределенного вторичного контроля

Распределенная структура управления повышает устойчивость МС за счет повышенной надежности, гибкости и масштабируемости. Такая структура достигает глобальных целей только посредством локального управления и соседней связи, и, следовательно, для реализации распределенного вторичного управления требуется коммуникационная сеть.

1) Предварительные сведения о теории графов: топология коммуникационной сети математически представлена неориентированным графом G = （V,E）, где V = {1,2,...,n} представляет собой непустое конечное множество узлов, а ребра E ⊆V ×V, соответственно. Если DG i получает информацию от DG j, соответственно, DG j называется соседом DG i. Множество соседей DG i обозначается как Ni = {j|（i,j） ∈E}. Матрица смежности, связанная с графом G, определяется как A=[aij], где aij = 1, если （i,j ） ∈E, и aij = 0 в противном случае. Между тем, матрица степеней выражается как D=diag {di }∈Rn×n с элементами di =∑j∈Niaij. Эта топология представляет собой связный граф близости, который зависит от состояний всех DGs и определяется локально для каждого DG в этом отрывке.

2) Реализация распределенного вторичного управления: Цель вторичного управления частотой может быть преобразована в консенсусное поведение, которое указывает на то, что частота асимптотически сходится к 50 Гц. Каждый DG генерирует активную мощность на основе профиля равномерного использования. Дифференцируя вторичное управление частотой, показанное в уравнении (1), получаем

$$\dot{\omega}_i = \dot{\omega}_{ni} - m_{pi}\dot{P}_i = u_{\omega i}, \qquad (4)$$

где uωi представляет собой вспомогательный вход управления частотой, определяемый информацией DG i и его соседей. Соответственно, uωi формулируется как

$$u_{\omega i} = -k_\omega \left[\sum_{j\in N_i} a_{ij}(\omega_i - \omega_j) + b_i(\omega_i - \omega_{\text{ref}}) \right], \qquad (5)$$

где kω ＞0 обозначает коэффициент усиления связи по частоте. Коэффициент усиления закрепления bi =1 подразумевает, что DG i подключен к опорному источнику. Согласно уравнениям (4) и (5), ωni можно записать как

$$\omega_{ni} = \int \left(u_{\omega i} + m_{pi}\dot{P}_i\right) \mathrm{d}t. \qquad (6)$$

Между тем, активная мощность DG должна распределяться согласно уравнению (3). Следовательно, upi равно

$$u_{pi} = -k_p \sum_{j \in N_i} a_{ij} \left(m_{pi} P_i - m_{pj} P_j \right). \tag{7}$$

где kp $>$ 0 представляет собой коэффициент усиления активной связи по мощности. Объединяя уравнения (5) и (7), уравнение (6) становится

$$\omega_{ni} = \int \left(u_{\omega i} + u_{pi} \right) \mathrm{d}t. \tag{8}$$

Традиционные распределенные стратегии вторичного управления, упомянутые выше, требуют, чтобы каждый DG постоянно вычислял входные сигналы вторичного управления и обменивался данными со своими соседями, что является расточительным использованием ограниченных ресурсов. Кроме того, системы вторичного управления подвержены угрозам ухудшения работы, вызванным хакерами, что может поставить под угрозу производительность MC. Мы разработали распределенную самозапускающуюся схему вторичного управления для снижения коммуникационной нагрузки с целью решения этой проблемы. Мы изучили, как FDI атаки влияют на систему управления, и внедрили защитные меры для противодействия этим эффектам.

2 Устойчивые распределенные схемы самозапускающегося управления на основе хэша

В этом разделе мы представляем наши основные стратегии для создания распределенной конструкции самозапускающегося вторичного контроллера, модели спонтанной FDI атаки и механизма устойчивости к FDI атакам на основе хэша.

2.1 Распределенная конструкция самозапускающегося контроллера

Мы предлагаем линейный протокол самозапускающегося управления на основе тактового сигнала для выполнения задач вторичного управления и минимизации требований к связи. Конструкция контроллера выглядит следующим образом:

1) Восстановление частоты: Первоочередной задачей является поддержание стабильной работы системы, поэтому для синхронизации частот целесообразно использовать локальное управление частотой. То есть,

$$u_{\omega_i} = -k_{\mathrm{P}}(\omega_i - \omega_{\mathrm{ref}}) - k_{\mathrm{I}} \int (\omega_i - \omega_{\mathrm{ref}}) \mathrm{d}t \tag{9}$$

где kP и kI представляют собой пропорциональный и интегральный коэффициенты регулятора соответственно.

2) Для активного распределения мощности: Для каждого DG был предложен линейный протокол самозапускающегося управления на основе тактового сигнала, позволяющий сбалансировать активную мощность между распределительными генераторами в соответствии с профилем равномерного использования с полным распределением.

Мы проектируем самозапускающуюся систему ∈R3n,

$\left(m_p P, u, \theta \right)$ **∈R^{3n}** удовлетворяющий эволюции

$$\begin{cases} m_{pi}\dot{P}_i = u_{pi} = \sum_{j\in N_i} u^{ij} \\ \dot{u}^{ij} = 0 \\ \dot{\theta}^{ij} = -1 \end{cases}, \qquad (10)$$

где mpiPi представляет собой переменную состояния активной мощности DG i; uij представляет собой локальный вход управления активной мощностью, определяемый относительной разницей между DG i и DG j, которая принадлежит множеству ; $\{-\gamma, 0, \gamma\}$ **;** а θij представляет собой переменную часов на конкретном канале связи (i,j)∈E**.**

Соответствующее правило обновления выглядит следующим образом:

Когда θ^{ij} достигает 0, запрашивает состояние активной мощности DG j, обновляет управляющий вход u^{ij}**,** и одновременно сбрасывает тактовую переменную θ^{ij}**.** Для краткости мы определяем $m_{\mathrm{ed}}^{ij}(t) = m_{pj}P_j(t) - m_{pi}P_i(t)$ как относительную разницу активной мощности между DG i и DG j.

Протокол обновления управляющего входа $\mathbf{u^{ij}}$ определяется как

$$u^{ij}(t^+) = \begin{cases} \mathrm{sign}_\varepsilon\left(m_{\mathrm{ed}}^{ij}(t)\right), & \text{if } \theta^{ij}(t) = 0 \\ u^{ij}(t), & \text{otherwise} \end{cases} \qquad (11)$$

где $\mathrm{sign}_\varepsilon\left(m_{\mathrm{ed}}^{ij}(t)\right)$ удовлетворяет**.**

$$\mathrm{sign}_\varepsilon\left(m_{\mathrm{ed}}^{ij}(t)\right) = \begin{cases} \gamma \mathrm{sign}\left(m_{\mathrm{ed}}^{ij}(t)\right), & \text{if} \left|m_{\mathrm{ed}}^{ij}(t)\right| \geqslant \varepsilon \\ 0, & \text{otherwise} \end{cases} \qquad (12)$$

где знак $(\cdot)$ представляет собой функцию знака**,** а γ представляет собой положительную константу. Параметр чувствительности ε определяет конечную консенсусную область. Кроме того, закон обновления переменной часов θ^{ij} задается формулой

$$\theta^{ij}(t^+) = \begin{cases} f^{ij}\left(m_{pi}P_i(t)\right), & \text{if } \theta^{ij}(t) = 0 \\ \theta^{ij}(t), & \text{otherwise} \end{cases} \qquad (13)$$

где

$$f^{ij}\left(m_{pi}P_i(t)\right) = \begin{cases} \frac{\left|m_{\mathrm{ed}}^{ij}\right|}{2\gamma\left(d_i+d_j\right)}, & \text{if} \left|m_{\mathrm{ed}}^{ij}\right| \geqslant \varepsilon \\ \frac{\varepsilon}{2\gamma\left(d_i+d_j\right)}, & \text{otherwise} \end{cases} \qquad (14)$$

Приведённые выше уравнения показывают, что $\mathbf{u^{ij}}$ **и** θ^{ij} θij обновляются одновременно, поскольку значение $m_{\mathrm{ed}}^{ij}(t)$ когда канал связи **(i,j) ∈E** работает нормально.

Кроме того**,** $\theta^{ij} = \theta^{ji}$ и $\mathbf{u^{ij} = -u^{ji}}$ гарантированы, поскольку выполняются условия $m_{\mathrm{ed}}^{ij}(t) = -m_{\mathrm{ed}}^{ji}(t)$ and $\left|m_{\mathrm{ed}}^{ij}(t)\right| = \left|m_{\mathrm{ed}}^{ji}(t)\right|$ приемлемые, в сочетании с уравнениями (10)-(14).

Соответственно, самозапускающиеся моменты времени можно выразить как

$$t_{k+1}^{ij} = t_k^{ij} + f^{ij}\left(m_{pi} P_i\left(t_k^{ij}\right)\right) \quad (15)$$

где t_{k+1}^{ij} и t_k^{ij} относятся к （k+1）-му и k-му моментам времени самопроизвольного срабатывания соответственно.

2.2 Модель спонтанной FDI атаки на основе распределения Бернулли

Рассматривая линию связи от DG i к DG j, FDI атаку на одностороннюю линию связи в обычном распределенном вторичном управлении можно определить как

$$P_i^{\mathrm{com}} = P_i + \delta_{ij} \quad (16)$$

где P_i^{com} и $\mathbf{P_i}$ представляют собой искаженную и реальную активную мощность, передаваемую от DG i к DG j соответственно. Далее, δij вводится с ложными данными, которые удовлетворяют $\| \delta_{ij} \| \leqslant \overline{\delta}_{ij}$, где $\overline{\delta}_{ij}$ представляет собой известный положительный скаляр.

Согласно этому определению, злоумышленники могут агрессивно перехватывать передаваемые данные, вызывая значительные сбои и нестабильность в изолированных МС. Однако для злоумышленников нерационально инициировать FDI атаку, показанную в (16), в распределенной самозапускающейся вторичной системе управления, поскольку моменты времени срабатывания самозапускающегося контроллера являются апериодическими и нерегулярными. Даже если злоумышленники FDI могут перехватывать передаваемые данные, постоянно контролируя каналы связи, они вряд ли перехватят данные из-за их более высокой скорости передачи. DG могут быстро обнаружить внедрения, если злоумышленники постоянно вводят ложные данные в контролируемый канал связи. Кроме того, непрерывные атаки трудно инициировать, поскольку злоумышленники имеют ограниченную энергию и мощность. Спонтанная FDI атака может привести к серьезным последствиям (например, нестабильности частоты и отключениям электроэнергии), что требует дальнейшего изучения. Поэтому мы сосредоточимся на модели спонтанной FDI атаки на основе распределения Бернулли со следующими предположениями.

Предположение 1. В данной статье всесторонне рассматриваются FDI атаки на мультиканалы связи. В связи с ограниченной энергией в реальных сценариях, появление FDI атак носит спонтанный характер. Более того, вводимые ложные данные часто являются «мягкими», чтобы их было трудно обнаружить.

Независимая переменная $\Gamma_{ij}(t)$ указывает, подвергается ли канал связи **(i,j)** FDI атакам в момент времени t, и выражается как

$$\Gamma_{ij}(t) = \begin{cases} 1, & \text{if the one - way communication} \\ & \text{link } (i,j) \text{ is attacked} \\ 0, & \text{otherwise} \end{cases} \quad (17)$$

FDI атака, более применимая в распределенной самозапускающейся структуре управления, может быть математически построена как

$$P_i^{\text{com}}(t) = \begin{cases} (1-\Gamma_{ij})P_i(t_k^{ij}) \\ \Gamma_{ij}(\delta_{ij}(t) + P_i(t_k^{ij})) \end{cases} \quad (18)$$

Γ_{ij} был разработан для соответствия распределению Бернулли с целью лучшего моделирования практических спонтанных FDI атак. Это было выражено как

$$\mathbb{P}\{\Gamma_{ij} = 1\} = p_{ij}, \mathbb{P}\{\Gamma_{ij} = 0\} = 1 - p_{ij} \quad (19)$$

где p_{ij} обозначает вероятность $\Gamma_{ij}=1.p_{ij}$ скаляр, заранее рассчитанный с использованием $p_{ij} \in [0,1$.

На рис. 1 представлена схема злоумышленников, которые манипулируют ложными данными через каналы связи в распределенной системе вторичного управления с самостоятельным запуском. Следовательно, мы можем сделать вывод, что обнаружение ввода ложных данных затруднено из-за самостоятельных коммуникаций, что побудило нас исследовать актуальное решение для своевременного скрининга ввода ложных данных.

2.3 Схема защиты от FDI атак на основе хэша

DG i не может знать моменты времени, когда он получает информацию о состоянии от DG j из-за апериодической и прерывистой связи самозапускающегося управления. Кроме того, временные интервалы между любыми двумя соседними моментами времени достаточно велики для выполнения простого вычисления. Эти качества стимулируют нас исследовать политику устойчивости к атакам для определения того, страдают ли изолированные MC от FDI атак, и устранения активных FDI атак.

FDI атаки на распределенные системы управления всегда скрытны, поскольку система не имеет глобальной информационной перспективы. Чтобы достичь нашей цели, мы спроектировали HDM в соответствии со следующим принципом, рассматривая алгоритм хэширования с характеристиками безопасности, однонаправленности и чувствительности [29]: Каждый DG передает свое собственное значение активной мощности и соответствующий ему хэш-код, сгенерированный алгоритмом хэширования, своим соседям. Приемник выполняет алгоритм хэширования для полученного значения активной мощности после того, как соседние DG получают соответствующий пакет данных, а затем мы получаем новый хэш-код и сравниваем его с полученным хэш-кодом для определения правильности передаваемых данных. Когда два хэш-кода не равны, это трактуется как сигнал FDI атаки. Поэтому ключевой вопрос заключается в правильной разработке алгоритма хэширования для удовлетворения требований однозначного соответствия между хэш-кодом и значением активной мощности**.**

Прежде чем разрабатывать алгоритм хеширования, нам необходимо выполнить двоичное переключение. Двоичное число значения активной мощности **DG j'** определяется как $(P_j)_2 = B_{pj}$. Следовательно, алгоритм хеширования можно выразить как

$$H(B_{pj}) = B_{pj} << 3, \quad (20)$$

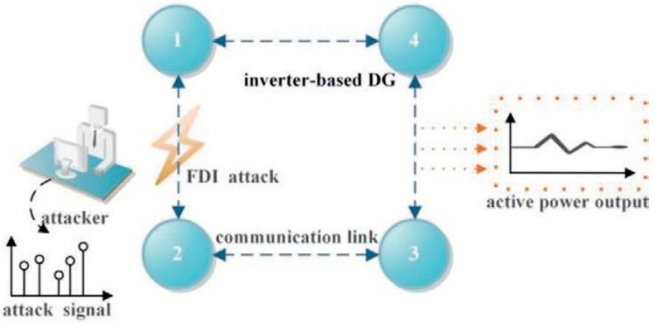


Рис.1 Схема вторичного контроля при спонтанной FDI атаке**.**

где H（B_{pj}） возвращает B_{pj} сдвинутый влево на три бита, что эквивалентно умножению на 2^3, что далее в статье сокращенно будет обозначаться как H_j. Таким образом, двоичный хэш-код отправителя активной мощности DG j представлен как $P_j \rightarrow H_j$.

Если рассматривать DG i в качестве примера, то DG j является соседом DG i. Для отправителя информации DG j значение активной мощности и его хэш-код должны быть доставлены соседям DG i в каждый успешный момент времени срабатывания, т. е. θ^{ij} **（t）=0.** Кроме того, мы выполняем алгоритм хэширования для одного из полученных данных P'_j таким образом $P'_j \rightarrow H'_j$, чтобы при получении приемником информации DG i пакет данных (P_j, H_j), отправленный от DG j. Сравнивая H'_j **и H_j,** приходим к выводу, что если H'_j **=H_j,** то, в противном случае λ^{ij} **（t）=0,** что указывает на успешное обнаружение скрытых FDI атак. HDM справляется с поврежденными данными передачи, внесенными вредоносными FDI атаками на каналы связи в изолированных MC.

На рис. 2 показана схема распределенного самозапускающегося управления на основе хэша, устойчивая к FDI атакам.

Теорема 1. Пусть каждый DG оснащен системой распределения активной мощности, представленной уравнением (10), которая активируется согласно (15), предполагая, что сеть связи G является связной и ненаправленной, а FDI атака – (18). Цель управления распределением активной мощности (3) может быть достигнута асимптотически с желаемой малой ошибкой сходимости, независимо от того, подвергается ли система атаке. В частности,

$$m_p P^* \in \left\{ \left| m_{pj} P_j - m_{pi} P_i \right| < \varepsilon, \forall (i,j) \in E \right\} \qquad (21)$$

где mpP* относится к точке равновесия активной мощности. Выбор ε позволяет сделать область сходимости сколь угодно малой.

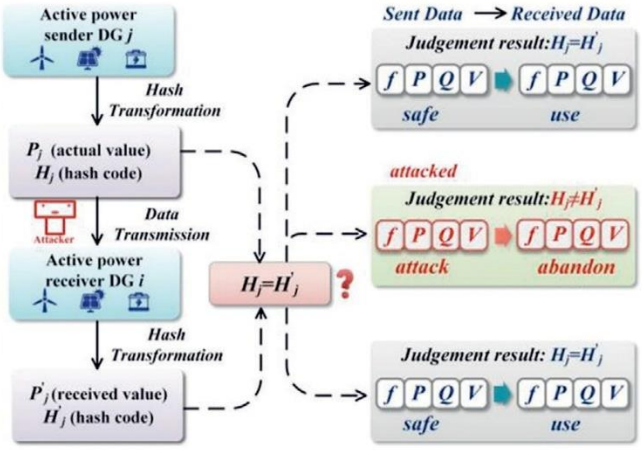


Рис.2 Иллюстрация хэш-устойчивого к атакам FDI самозапускающегося управления.

Замечание 1. Уравнение (21) показывает, что активная мощность может сходиться к ε-окрестности консенсуса. Однако «расхождение» можно сделать сколь угодно малым, выбрав достаточно малое ε. Если ε выбрано равным нулю, предлагаемая стратегия сводится к обычному усредненному консенсусному управлению. Уравнение (21) подразумевает, что ε определяет количество срабатываний. Чем больше значение выбранного ε, тем меньше время срабатывания. Следовательно, существует компромисс между ошибкой сходимости и временем срабатывания.

Доказательство теоремы 1. Для каждого t ≥0 и γ ＞0 допустимая функция Ляпунова V（t）проектируется как

$$V(t)=\frac{1}{2}\left[m_pP(t)\right]^{\mathrm{T}}\left[m_pP(t)\right], \tag{22}$$

where $m_pP(t)=\left[m_{p1}P_1(t),\ldots,m_{pn}P_n(t)\right]^{\mathrm{T}}$, and note that $V(t)=0$.

Следовательно, производная по времени функции Ляпунова V (t) равна

$$\dot{V}(t)=\frac{1}{2}\left[m_{pi}\dot{P}_i(t)\right]^{\mathrm{T}}\left[m_{pi}P_i(t)\right]+\frac{1}{2}\left[m_{pi}P_i(t)\right]^{\mathrm{T}}\left[m_{pi}\dot{P}_i(t)\right] \tag{23}$$

Подставляя уравнения (9)-(11) в уравнение (23), получаем

$$\begin{aligned}\dot{V}(t)=&\sum_{i=1}^{n}\left(m_{pi}P_i(t)\sum_{j\in N_i}u^{ij}(t)\right)=\\&\sum_{i=1}^{n}\left(m_{pi}P_i(t)\sum_{j\in N_i}\mathrm{sign}_{\varepsilon}\left(m_{\mathrm{ed}}^{ij}(t)\right)\right)=\\&-\gamma\sum_{A}m_{\mathrm{ed}}^{ij}(t)\mathrm{sign}\left(m_{\mathrm{ed}}^{ij}\left(t_k^{ij}\right)\right)\end{aligned} \tag{24}$$

where $A=\left\{\left|m_{\mathrm{ed}}^{ij}\left(t_k^{ij}\right)\right|\geqslant\varepsilon,\forall(i,j)\in E\right\}$.

Using Eq. (15), we observe that for $t\in\left[t_k^{ij},t_{k+1}^{ij}\right)$, if $m_{\mathrm{ed}}^{ij}\left(t_k^{ij}\right)\geqslant\varepsilon$, then

$$\begin{aligned}m_{pj}P_j(t)-m_{pi}P_i(t)&\geqslant m_{pj}P_j\left(t_k^{ij}\right)-m_{pi}P_i\left(t_k^{ij}\right)\\&-\gamma\left(d_i+d_j\right)\left(t-t_k^{ij}\right)\geqslant\frac{m_{\mathrm{ed}}^{ij}\left(t_k^{ij}\right)}{2}\end{aligned} \tag{25}$$

Similarly, if $m_{\mathrm{ed}}^{ij}\left(t_k^{ij}\right)\leqslant-\varepsilon$, then

$$m_{pj}P_j(t)-m_{pi}P_i(t)\leqslant\frac{m_{\mathrm{ed}}^{ij}\left(t_k^{ij}\right)}{2} \tag{26}$$

Therefore, if $\left|m_{\mathrm{ed}}^{ij}\left(t_k^{ij}\right)\right|\geqslant\varepsilon$ and $med^{ij}(t)$ maintain the symbol during the continuous evolution, we obtain

$$\begin{aligned}m_{\mathrm{ed}}^{ij}(t)\mathrm{sign}_{\varepsilon}\left(m_{\mathrm{ed}}^{ij}\left(t_k^{ij}\right)\right)&=m_{\mathrm{ed}}^{ij}(t)\mathrm{sign}_{\varepsilon}\left(m_{\mathrm{ed}}^{ij}(t)\right)\\&=\left|m_{\mathrm{ed}}^{ij}(t)\right|\end{aligned} \tag{27}$$

Moreover,

$$\begin{aligned}\left|m_{\mathrm{ed}}^{ij}(t)\right|&\geqslant\left|m_{pj}P_j\left(t_k^{ij}\right)-m_{pi}P_i\left(t_k^{ij}\right)\right|\\&-\gamma\left(d_i+d_j\right)\left(t-t_k^{ij}\right)\geqslant\frac{m_{\mathrm{ed}}^{ij}\left(t_k^{ij}\right)}{2}\end{aligned} \tag{28}$$

Следовательно, объединив уравнения (25) и (26), уравнение (23) можно переписать как

$$\dot{V}(t) \leqslant -\gamma \sum_{A} \frac{\left|m_{\mathrm{ed}}^{ij}\left(t_k^{ij}\right)\right|}{2} \leqslant -\gamma \sum_{A} \frac{\varepsilon}{2} \tag{29}$$

поскольку γ ＞0, где $\dot{V}(t)$ определена строго отрицательно.

Обратите внимание, что существует конечное время T* такое, что для любого (i ,j)∈E и $t_k^{ij} \geqslant T^*,\ med^{ij}\left(t_k^{ij}\right) < \varepsilon.$ Согласно уравнениям (10)–(14) легко определить, что локальный управляющий вход upi равен нулю, а активная переменная состояния мощности mpiPi постоянна для t ≥T*, что подразумевает сходимость алгоритма самозапускающегося управления, устойчивого к FDI атакам на основе хэша. Кроме того, эффекта Зенона можно избежать благодаря уравнениям (14) и (15), где ошибка сходимости ε не является бесконечно малым числом.

Рассматривая сценарий спонтанной FDI атаки на основе распределения Бернулли, смоделированный уравнением (18), вредоносные данные, внедренные в канал связи, могут быть эффективно обнаружены путем сравнения отправленных и полученных хэш-значений. Таким образом, переменная состояния активной мощности $m_{pi}P_i$ （t） сходится к точке равновесия m_pP^* * с использованием HDM, выраженной в уравнении (20), независимо от того, подвергается ли система атаке.

$$m_pP^* \in \left\{\left|m_{pi}P_i - m_{pj}P_j\right| < \varepsilon, \forall(i,j) \in E\right\} \tag{30}$$

Доказательство готово.

В каждом DG должны быть установлены две подсистемы с применением HDM: одна для алгоритма хеширования и другая для проверки двух хеш-кодов до и после алгоритма хеширования. Эти две подсистемы позволяют каждому DG распознавать спонтанные FDI атаки, внедренные в канал связи при постоянных возмущениях. Таким образом, HDM может противостоять любому типу спонтанной FDI атаки (включая неограниченные атаки). Кроме того, алгоритм хеширования содержит только математические операции с бинарным сдвигом влево и проверку подлинности передаваемых данных, требующие только трехкратных и одноразовых фиксированных затрат соответственно. Таким образом, HDM не вызывает видимой задержки времени, влияющей на работу MC. Напротив, производительность механизма устойчивости к FDI атакам на основе хеширования «интеллектуально» улучшена, что является существенным преимуществом.

Для ясности подробные этапы предлагаемого HDM обобщены в Алгоритме 1.

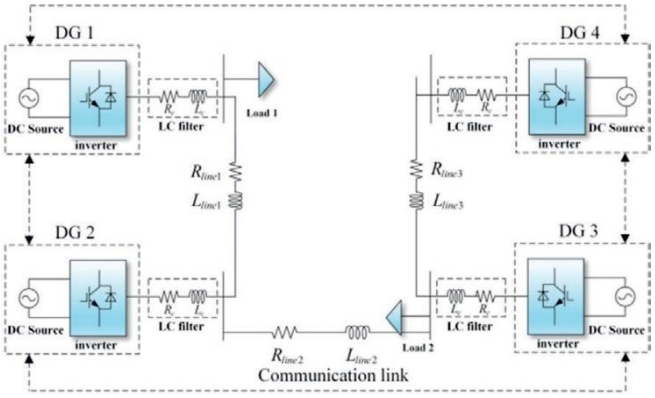


Рис. 3. Структура связи изолированной тестовой системы микросети.

Алгоритм 1. Устойчивый к FDI атакам протокол самозапускающегося управления на основе хэширования

Initialization: For DG i and $j \in N_i$, set clock and variable $\theta^{ij}(0) = 0$, detection function $\lambda^{ij}(0) = 1$, control input $u^{ij}(0) = 0$
for $i = 1$ to n **do**
  for $j \in N_i$ **do**
    while $\theta^{ij}(t) > 0$ **do**
      DG i applies the control input $u_{pi}(t) = \sum_{j \in N_i} u^{ij}(t)$;
      update θ^{ij} according to $\dot{\theta}^{ij} = -1$;
    end while
    if $\theta^{ij}(t) = 0$ **then**
      active power information sender DG j;
        do hash transformation for $P_j \rightarrow H_j$;
        send data package (P_j, H_j) to DG i;
      active power information receiver DG i;
      if (P_j, H_j) information is received **then**
        do hash transformation for $P'_j \rightarrow H'_j$;
        if $H'_j = H_j$ **then**
          $\lambda^{ij}(t) = 1$;
            update $u^{ij}(t)$ and $\theta^{ij}(t)$;
        else
              $\lambda^{ij}(t) = 0$;
            refuse P_j
            waiting for next triggering
        end if
      end if
    end if
  end for
end for

3 Пример исследования

В этом разделе мы проверяем эффективность предлагаемой распределенной схемы вторичного управления на основе хэш-функции, устойчивой к FDI атакам, путем моделирования изолированного генератора с помощью инструментария MATLAB/Simulink. Структура связи тестовой системы МС показана на рис. 3. Эта структура состоит из четырех DG, взаимодействующих друг с другом через двунаправленную сеть связи. Параметры тестовой МС приведены в таблице 1. Коэффициент усиления связи по частоте k_ω в уравнении (5) и входной параметр управления γ в уравнении (12) установлены равными 40 и 0,2 соответственно. Аналогично, опорная частота и область схождения активной мощности установлены равными $\boldsymbol{\omega}_{\mathbf{ref}}$ =50 Гц и ε = 0,01 соответственно**.**

Мы смоделировали резкие изменения нагрузки в тестовом генераторе и сценарии для различных атакуемых каналов связи, вероятностей атак и форм атак, чтобы проверить эффективность и реализуемость предлагаемого контроллера, что будет подтверждено позже.

Таблица 1. Параметры системы испытаний МС.

	DG1 & DG2 (10.64 kW)		**DG3 & DG4 (8.0 kW)**	
DGs	m_p	9.4×10^{-5}	m_p	12.5×10^{-5}
	R_c	0.2	R_c	0.2
	L_c	3×10^{-3}	L_c	3×10^{-3}
	Line 1 & 3		**Line 2**	
Lines	$R_{\text{line1\&3}}$	0.23	R_{line2}	0.35
	$L_{\text{line1\&3}}$	0.318×10^{-3}	L_{line2}	1.847×10^{-3}
Loads	P_{load1}	15.6×10^3	P_{load2}	15.6×10^3

Процесс моделирования организован следующим образом: 1) t = 0 с, МС работает в изолированном режиме; 2) t = 1 с, активируется предлагаемый хэш-устойчивый к FDI атакам распределенный самозапускающийся контроллер; 3) t = 2 с, нагрузка 1 резко уменьшается на 3 кВт; 4) t = 3,5 с, запускается спонтанная FDI атака; и 5) t = 5 с, нагрузка 1 резко увеличивается до 3 кВт. Общая продолжительность моделирования установлена равной 7 с.

3.1 Пример А: Все каналы связи подвергаются FDI атакам с различной вероятностью.

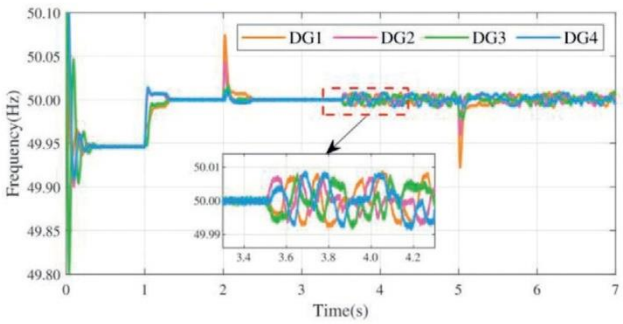
Рассмотрев сценарии, в которых все каналы связи подвергаются атакам с различной вероятностью, мы демонстрируем устойчивость предлагаемой стратегии.

Пример А.1 (Все каналы связи подвергаются атакам с $\mathbb{P}\{\Gamma_{ij} = 1\} = 0.1$): В этом случае мы вводим

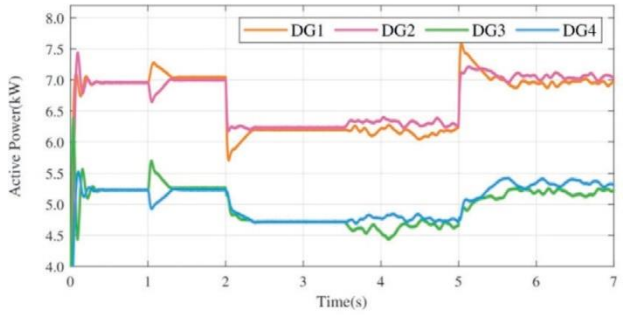
$$\mathbb{P}\{\Gamma_{ij} = 1\}$$

ложные данные $|\delta_{ij}|$=0,1 кВт на каналах связи между DG i и DG j с **= 0.1,** где **i,j=1,2...n.** Использование $\delta_{ij} = -\delta_{ji}$ =0,1(кВт) использовалось для моделирования

Пример А.1 (Все каналы связи подвергаются атакам с. В этом случае мы вводим ложные данные |δij|=0,1 кВт на каналах связи между DG i и DG j с = 0,1, где i, j = 1, 2...n. Использование δij =-δji =0,1(кВт) использовалось для моделирования одиозной среды.



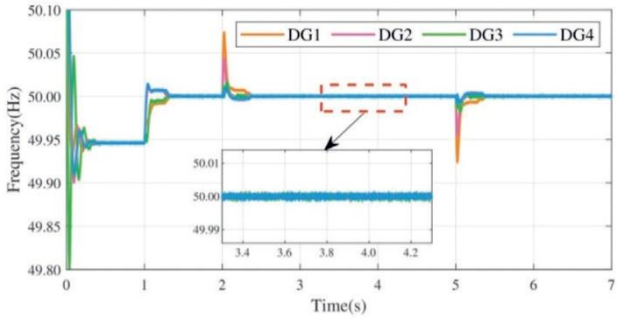
(a) frequency



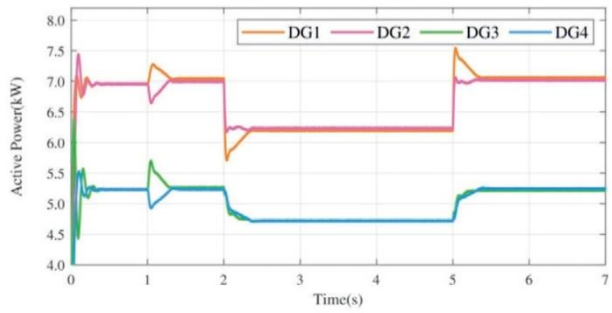
(b) active power

Рис.4. Характеристики при спонтанных FDI атаках с $|\delta_{ij}|$=0,1 кВт и $\mathbb{P}\{\Gamma_{ij}=1\}$ = 0.1 1 без внедрения HDM.

На рис. 4 показаны стабильность частоты и характеристики распределения активной мощности самозапускающихся контроллеров без реализации HDM. На рис. 4(a) показаны частоты DG, отклоняющиеся от опорного значения, вызванные первичным управлением на основе спада, когда микросеть работает в изолированном режиме. Цели вторичного управления выполняются между t ∈ [2, 3,5] с, что подтверждает эффективность предлагаемой схемы распределенного самозапускающегося управления. Однако при наличии FDI атак частота не может поддерживаться на уровне 50 Гц. Между тем, значение активной мощности каждого DG расходится и превышает предварительно определенный порог из-за эффекта спонтанных FDI атак, запущенных после t = 3,5 с. Другими словами, FDI атаки приводят к уязвимости микросетей.



(a) frequency



(b) active power

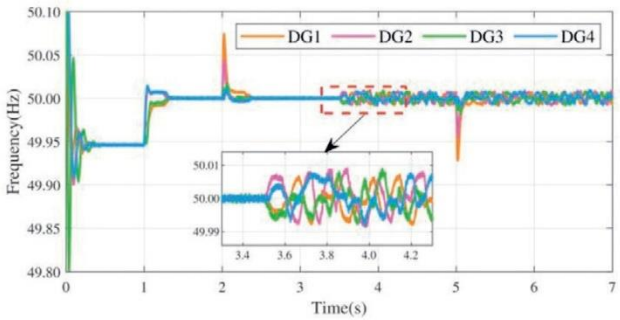
Рис. 5. Характеристики при спонтанных FDI атаках с $|\delta_{ij}|$=0,1 кВт и $\mathbb{P}\{\Gamma_{ij}=1\}$ = 0,1 с использованием HDM.

На рис. 5 показаны характеристики самозапускающихся контроллеров, использующих предлагаемый HDM, что свидетельствует о том, что этот механизм дополнительно повысил устойчивость распределенной сети при спонтанных FDI атаках. Сравнение рис. 4 и 5 показало, что, особенно в интервалах времени, описанных как t ∈[3,3,4,3] с, HDM может поддерживать стабильность частоты и обеспечивать точное распределение активной мощности в заданных стабильных диапазонах независимо от наличия спонтанных FDI атак. Предлагаемый закон устойчивости к FDI атакам на основе хэш-функции позволяет эффективно обнаруживать FDI атаки тем самым устраняя их негативные последствия.

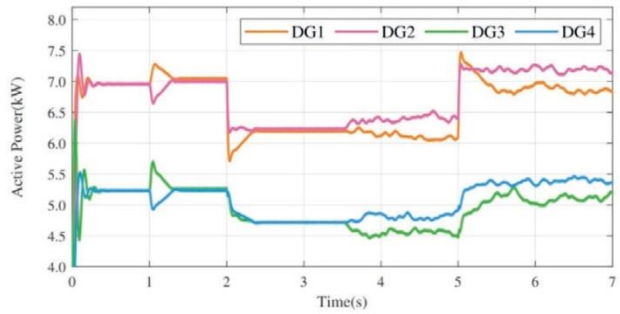
Пример A.2 (Все линии связи подвергаются атакам с $\mathbb{P}\{\Gamma_{ij}=1\}=0.3$): В этом случае остальные параметры те же, за исключением условий, которые описывают P {Γ_{ij} =1}= 0,3 как отличные от примера A.1.

Отклики частоты и активной мощности без какой-либо защиты показаны на рис. 6, а результаты моделирования после применения HDM показаны на рис. 7.

На рис. 6(a) и (b) показано, что спонтанные атаки с $\mathbb{P}\{\Gamma_{ij}=1\}=0.3$ приводят к потере желаемой частоты и распределения активной мощности, где частота отклоняется от 50 Гц и демонстрирует колебательное поведение для активной мощности. Кроме того, наблюдается, что частота на рис. 4 с $\mathbb{P}\{\Gamma_{ij}=1\}=0.1$ имеет больше незначительных отклонений от 50 Гц, чем на рис. 6. На рис. 4 и рис. 6 показано, что более высокая вероятность атак может привести к более серьезным последствиям.

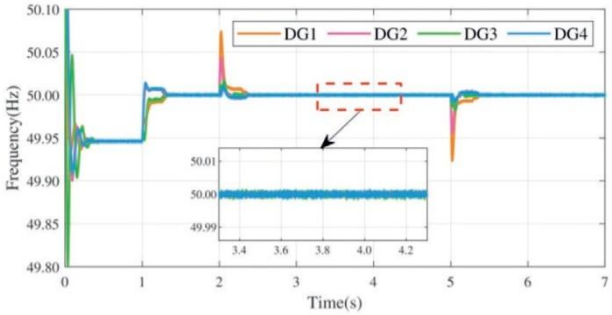


(a) frequency

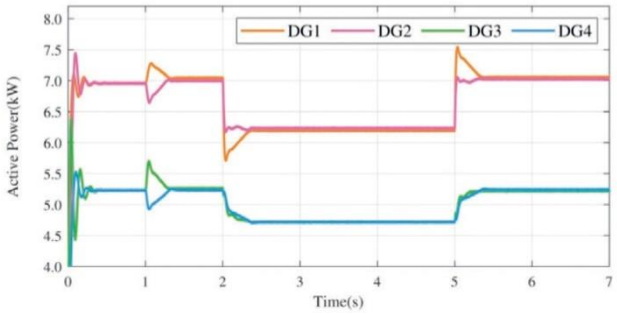


(b) active power

Рис.6. Характеристики при спонтанных FDI атаках с $|\delta_{ij}|$=0,1 кВт и $\mathbb{P}\{\Gamma_{ij}=1\}$ = 0,3 без использования HDM.



(a) frequency



(b) active power

Рис.7. Характеристики при спонтанных FDI атаках при $|\delta_{ij}|$=0,1 кВт и $\mathbb{P}\{\Gamma_{ij}=1\}$ = 0,3 с использованием HDM.

На рис. 7 показано, что частоты блоков DG были восстановлены до 50 Гц после применения HDM в момент времени t=3,5 с. При этом активная выходная мощность радиосигналов блоков DG восстанавливается в пределах определенного диапазона сходимости ε=0,01.

Рис. 8 (a) показывает, что моменты времени срабатывания DG i и DG j при самозапускающихся контроллерах являются апериодическими и прерывистыми в диапазоне между t ∈ [2,0, 3,0] с. Рис. 8. (b) и (c) показывают моменты времени срабатывания каждой пары отдельных DG при самозапускающихся контроллерах без и с реализацией HDM в диапазоне между t ∈ [3,4, 3,8] с соответственно. Контроллеры без использования HDM приводят к апериодическому и меньшему количеству срабатываний, особенно после t = 3,5 с. Это объясняется FDI атаками, которые делают $|m_{\mathrm{ed}}^{ij}(t)| \geq \varepsilon$ увеличивая временной интервал между срабатываниями в устойчивом состоянии. Однако спонтанный ввод ложных данных приводит к более значительному отклонению и нерегулярным моментам времени срабатывания, вызывая огромные колебания и резкие колебания. Таким образом, метод обнаружения и смягчения на основе HDM играет важную роль в обеспечении характеристик вторичного управления.

3.2 Пример B: Каналы связи при неограниченных во времени FDI атаках

В этом подразделе мы проверяем эффективность HDM в условиях неограниченных, изменяющихся во времени FDI атак. Далее мы рассматриваем сценарий, в котором злоумышленники манипулируют всеми каналами связи и заменяют фактическую активную мощность

неограниченными, изменяющимися во времени дополнительными ложными данными, представленными как $\delta_{ij} = -\delta_{ji} = 0{,}5(t-3{,}5)$ кВт при t=3,5 с с вероятностями $\mathbb{P}\{\Gamma_{ij} = 1\} = 0.3.$

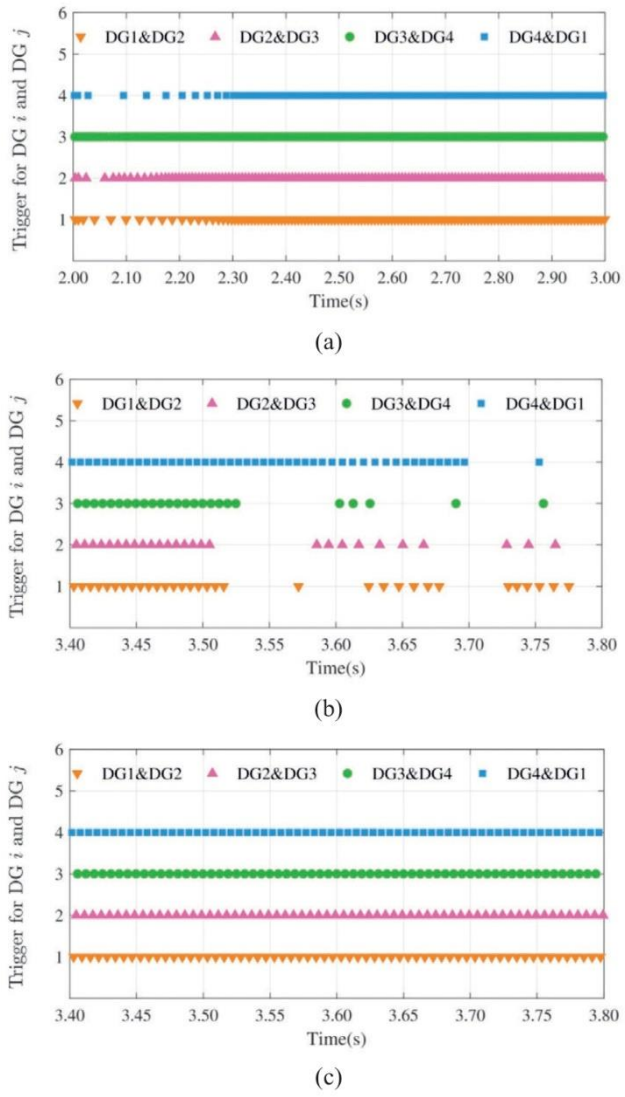
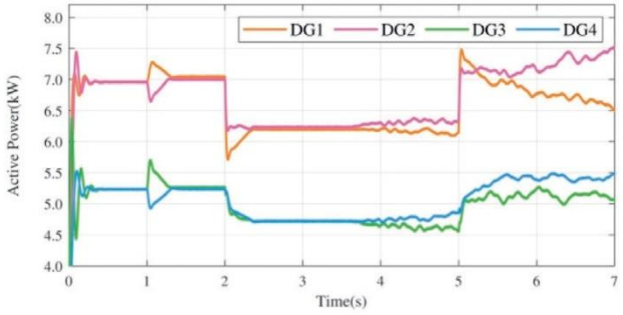
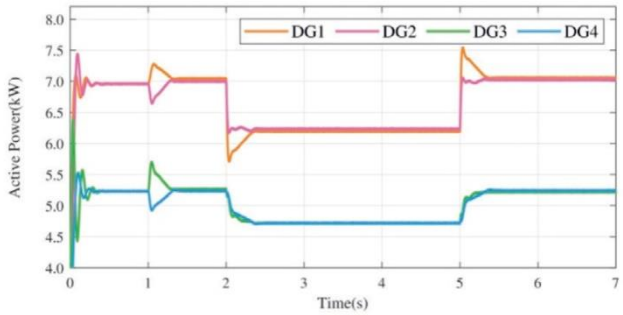


Рис.8. Моменты времени самосрабатывания каждой пары DG при спонтанных FDI атаках с |δij|=0,1 кВт и $\mathbb{P}\{\Gamma_{ij} = 1\}$ = 0.3.

На рис. 9(a) показано, что значения активной мощности резко снижаются для скомпрометированных DG, поскольку вредоносные данные вводятся в момент времени t=3,5 с. Каждый DG не может одновременно вернуться в нормальное состояние. Характеристики активной мощности при неограниченных во времени атаках более серьезны, чем в сценарии, описанном в примере A. Как показано на рис. 9(b), после применения спроектированного HDM активная мощность между DG распределяется разумно на основе коэффициентов спада. Активная мощность может прийти к стационарному состоянию даже при ограниченных во времени FDI атаках в изолированной тестовой системе МС. Желаемая синхронизация активной мощности от DG 1 до 4 по-прежнему может быть достигнута независимо от форм FDI атак, обеспечивая стабильную работу системы. По сравнению с рис. 6, неограниченные во времени FDI атаки могут привести к более серьезным последствиям для распределения активной мощности микросетей. Мы приходим к выводу, что HDM успешно предотвратит пагубное воздействие FDI атак независимо от форм атаки.



(a)



(b)

Рис.9. Характеристики активной мощности при спонтанных FDI атаках при $|\delta_{ij}|$=0,5 (t-3,5) кВт и $\mathbb{P}\{\Gamma_{ij}=1\}$ = 0.3.

4 Заключение

В этом исследовании подчеркиваются проблемы вторичного управления P-ω в изолированных МС с использованием механизма самозапуска при спонтанных FDI атаках. Сначала мы разрабатываем линейную распределенную схему самозапуска на основе тактового сигнала для достижения активного распределения мощности между DG и локального восстановления частоты. Разработанный механизм самозапуска может значительно снизить коммуникационную и вычислительную нагрузку. Ложные данные, введенные в МС, могут быть легко обнаружены и устранены путем проектирования HDM. Этот метод является гибким и может применяться во многих системах, включая, помимо прочего, системы управления с апериодической и прерывистой связью. Результаты моделирования подтверждают, что этот метод устойчивости к FDI атакам на основе хэша может значительно повысить устойчивость микросетей к любым формам спонтанных FDI атак.

Дальнейшие статьи включают в себя разработку алгоритмов, устойчивых к атакам, в рамках направленной топологии и для непрерывных атак на контроллер и компоненты измерения. В будущем мы сосредоточимся на различных сценариях атак, таких как DoS, атаки с задержкой и атаки с повторным воспроизведением.

Об авторском вкладе CRediT

Син Хуан: написание, рецензирование и редактирование, написание исходного черновика, валидация, ресурсы, администрирование проекта, методология. Юйлинь Чэнь: написание, рецензирование и редактирование, ресурсы, исследование, концептуализация. Дунлянь Ци: написание, рецензирование и редактирование, валидация, руководство, исследование, формальный анализ. Юньфэн Янь: написание, рецензирование и редактирование, визуализация,

исследование. Шаохуа Ян: написание, рецензирование и редактирование. Ин Вэн: программное обеспечение, ресурсы, методология. Сяньбо Ван: ресурсы.

О конфликте интересов.

Авторы заявляют, что у них нет известных им конкурирующих финансовых интересов или личных отношений, которые могли бы повлиять на работу, представленную в настоящей статье.

Благодарности

Данная работа была поддержана Фондом естественных наук провинции Хайнань Китая (№ 524RC532), исследовательским стартовым финансированием Хайнаньского института Чжэцзянского университета (№ 0210-6602-A12202) и проектом Научно-технологического города залива Санья Ячжоу (№ SKJC-2022-PTDX-009/010/011).

Список используемой литературы

[1] J.Li, C.W.Sun, Q.Y.Su, Анализ каскадных отказов киберфизических систем электроснабжения с учётом атак с использованием ложных данных, Global Energy Interconnect.4 (2) (2021) 204-213.

[2] G.Magdy, A.Bakeer, M.Alhasheem, Управление системой искусственной инерции на основе сверхпроводящей технологии накопления энергии для улучшения динамических характеристик частоты в микросетях с высоким уровнем проникновения возобновляемых источников энергии, Prot.Control Mod.Power Syst.6(1)(2021)36.

[3] M.Y.Zhang, Y.Han, Y.X.Liu и др., Многовременное моделирование и анализ динамической устойчивости для устойчивых микросетей: современное состояние и перспективы, Prot.Control Mod.Power Syst.9 (3)(2024) 1-35.

[4] Т.К.Рой, С.К.Гош, С.Саха, Надёжный контроллер обратного шага с глобальным интегральным терминалом и скользящим режимом для повышения динамической устойчивости гибридных микросетей переменного/постоянного тока, Prot.Control Mod.Power Syst.8 (1) (2023) 1-13.

[5] Ч.Й.Чен, С.Чжан, М.Дж.Цуй и др., Оценка устойчивости системы управления вторичной частотой с динамическими атаками с использованием ложных данных, IEEE Trans.Ind.Inf.18 (5) (2022) 3224-3234.

[6]X.Huang, D.L.Qi, Y.L.Chen и др., Распределенное самозапускающееся вторичное управление с сохранением конфиденциальности для микросетей переменного тока на основе VSG, IEEE Trans.Smart Grid (2024), https://doi.org/10.1109/TSG.2024.3467392.

[7] Т. Хайнс, М. Йошевски, С. Картик Гурумурти и др., Централизованное управление с использованием прогнозирующей модели для управления переходной частотой в изолированных микросетях на основе инверторов, IEEE Trans.Power Syst.38 (3) (2023) 2641-2652.

[8] Дж. Ю. Лю, Х. Х. Сонг, Ч. Ю. Чен и др., Децентрализованное управление вторичной частотой автономных микросетей с помощью адаптивного робастного усиления, IEEE Trans.Smart Grid 15 (1) (2024) 67-76.

[9] Дж. Чой, С. И. Хабиби, А. Бидрам, Распределенное конечновременное управление частотой и напряжением микросетей переменного тока, IEEE Trans.Power Syst.37 (3) (2022) 1979-1994.

[10] Y.L.Chen, D.L.Qi, H.N.Dong и др., Распределенная стратегия вторичного управления, устойчивая к FDI атакам, для изолированных микросетей, IEEE Trans.Smart Grid 12 (3) (2021) 1929-1938.

[11] S.H.Huang, L.Y.Xiong, Y.Zhou и др., Распределенное управление вторичной частотой и средним напряжением в заданное время для изолированных микросетей переменного тока, IEEE Trans.Power Syst.38 (5) (2023) 4191-4205.

[12] Y.Shi, Y.Cheng, B.Xie и др., Адаптивная стратегия управления вторичной частотой микросети на основе идентификации параметров, Global Energy Interconnect, 6 (5) (2023) 592-600.

[13] L.Xu, Q.L.Guo, H.T.Zeng и др., Оптимизация топологии связи для киберфизических микросетей с задержкой времени под распределённым управлением, IEEE Trans.Smart Grid PP(99) (2024) 1.

[14] Y.L.Chen, C.Y.Li, D.L.Qi и др., Распределённое вторичное управление, запускаемое событиями, для изолированных микросетей с надлежащим периодом проверки условий срабатывания, IEEE Trans.Smart Grid 13 (2) (2022) 837-848.

[15] S.X.Weng, D.Yue, C.X.Dou и др., Распределенное кооперативное управление, запускаемое событиями, для обеспечения стабильности частоты и напряжения, а также распределения мощности в изолированной микросети на основе инвертора, IEEE Trans.Cybern.49 (4) (2019) 1427-1439.

[16]Z.W.Li, Z.P.Cheng, J.K.Si и др., Распределенное вторичное управление, запускаемое событиями, для регулирования среднего напряжения на шине и пропорционального распределения нагрузки в микросети постоянного тока, J.Mod Power Syst.Clean Energy 10 (3) (2022) 678-688.

[17]X.J.Zhang, Y.P.Zhang, R.R.Li, Распределенное управление, запускаемое событиями, для распределения мощности в микросети переменного тока, подключенной к сети, IEEE Trans.Power Syst.39 (1) (2024) 770-778.

[18] H.Yu, X.Chen, T.W.Chen и др., Двусторонний консенсус, инициируемый событиями, для многоагентных систем: анализ без эффекта Зенона, IEEE Trans.Autom.Control 65 (11) (2020) 4866-4873.

[19] А. Анта, П. Табуада, «Выполнять выборку или нет: самозапускающееся управление нелинейными системами», IEEE Trans.Autom.Control 55(9)(2010) 2030-2042.

[20] Й. Л. Чен, К. В. Лао, Д. Л. Ци и др., «Распределенное самозапускающееся управление для восстановления частоты и распределения активной мощности в изолированных микросетях», IEEE Trans.Ind.Inf.19(10)(2023) 10635-10646.

[21] Г. Сюй, Л. Ма, «Устойчивое самозапускающееся управление для восстановления напряжения и распределения реактивной мощности в изолированных микросетях при атаках типа «отказ в обслуживании», Appl.Sci.10(11)(2020) 3780.

[22] L.Xu, Q.L.Guo, Y.J.Sheng и др., Об устойчивости современных энергосистем: всесторонний обзор с киберфизической точки зрения, Renew.Sustain.Energy Rev.152 (2021) 111642.

[23] S.H.Yang, K.W.Lao, Y.L.Chen и др., Устойчивое распределенное управление против атак с использованием ложных данных для управления спросом, IEEE Trans.Power Syst.39 (2) (2024) 2837-2853.

[24] Y.S.Li, R.F.Ren, B.N.Huang и др., Безопасный подход к распределенной диспетчеризации на основе гибридного триггера для интеллектуальных сетей против DoS-атак, IEEE Trans.Syst.Man Cybern.: Syst.53 (6) (2023) 3574-3587.

[25] Б. Дж. Янь, З. З. Цзян, П. Ч. Яо и др., Оптимальное распределение защитных ресурсов на основе теории игр с неполной информацией в киберфизических энергосистемах против атак с вводом ложных данных, Prot. Control Mod. Power Syst. 9 (2) (2024) 115–127.

[26] С. Х. Янь, К. В. Лао, Х. С. Хуэй и др., Безопасное распределенное управление для управления спросом в энергосистемах против кибератак с использованием обмана и произвольных шаблонов, IEEE Trans. Power Syst. PP (99) (2024) 1–12.

[27] М. Мэн, Г. С. Сяо, Б. Б. Ли, Адаптивный консенсус для гетерогенных многоагентных систем при атаках с использованием датчиков и исполнительных механизмов, Automatica 122 (2020) 109–242.

[28] X.G.Guo, D.Y.Zhang, J.L.Wang и др., Консенсусное управление и обнаружение неисправностей многоагентных систем, подверженных стохастическим атакам с использованием ложных данных, основанное на событиях и наблюдении, IEEE Trans.Network Sci.Eng.9 (2) (2022) 481-494.

[29] B.Demir, L.Bruzzone, Масштабируемый поиск и извлечение изображений дистанционного зондирования на основе хеширования в больших архивах, IEEE Trans.Geosci.Remote Sens.54 (2) (2016) 892-904.

Получено 20 марта 2024 г.;

отредактировано 15 мая 2024 г.; принято 7 июля 2024 г.

Отсканируйте для получения более подробной информации.

Рецензирование под руководством Global Energy Interconnection Group Co.Ltd. *

* Автор-корреспондент

Адреса электронной почты: xinghuang@zju.edu.cn (С.Хуан), chenyl2017@zju.edu.cn (И.Чэнь), qidl@zju.edu.cn (Д.Ци), 21210004@zju.edu.cn (И.Янь), shaohuayang2022@gmail.com (С.Ян), 22360163@zju.edu.cn (И.Вэн), xbwang@zju.edu.cn (С.Ван). https://doi.org/10.1016/j.gloei.2024.07.001

Син Хуан получила степень бакалавра в области электротехники в Китайском университете горного дела и технологий в Сюйчжоу, Китай, в 2022 году. Она работает над получением степени доктора философии в области электротехники в Школе электротехники Чжэцзянского университета в Ханчжоу, Китай. Ее исследовательские интересы включают в себя стратегию распределенного управления и киберфизическую безопасность с приложениями в интеллектуальных сетях.

Юйлинь Чен получил степень бакалавра математики и прикладной математики, а также степень магистра электротехники в Северо-Восточном университете электроэнергетики в Цзилине, Китай, в 2014 и 2017 годах соответственно, а также степень доктора философии в области электротехники в Чжэцзянском университете в Ханчжоу, Китай, в 2021 году. Он является автором и соавтором более 30 журнальных статей, опубликованных в IEEE Trans.Smart Grid, IEEE Trans.Indus.Informat., IEEE Trans.SMC.Systems, Журнал CSEE по энергетике и энергетическим системам и т. д. В настоящее время его исследовательские интересы включают распределенное управление возобновляемыми источниками энергии и киберфизическую безопасность с приложениями в интеллектуальных сетях.

Дунлянь Ци получила докторскую степень в области теории управления и техники управления в Школе электротехники Чжэцзянского университета (Китай) в 2002 году. В настоящее время она является профессором и научным руководителем докторантуры в Чжэцзянском университете. Ее научные интересы включают интеллектуальную обработку информации, системы беспорядка, а также нелинейную теорию и ее применение.

Юньфэн Янь получила степень доктора философии в области электротехники в Чжэцзянском университете (Ханчжоу, Китай) в 2019 году. В настоящее время она является младшим научным сотрудником Чжэцзянского университета. Ее научные интересы включают системы машинного зрения и машинного обучения, а также распределенную оценку и управление сетевыми системами.

Шаохуа Ян получил докторскую степень в области электротехники и вычислительной техники в Университете Макао (Макао, Китай). В настоящее время он является научным сотрудником Государственной ключевой лаборатории Интернета вещей для умного города Университета Макао. Его исследовательские интересы включают киберфизические энергосистемы, управление гибкими ресурсами и качество электроэнергии, с особым упором на безопасность.

Ин Вэн получила степень бакалавра наук в Китайском университете горного дела и технологий в Пекине в 2023 году. Сейчас она учится на магистра наук в Чжэцзянском университете в Ханчжоу, Китай. Ее научные интересы включают оценку состояния и обнаружение атак с использованием ввода ложных данных.

Сяньбо Ван получил степень доктора философии (PhD) в области электромеханики в Университете Макао (Макао, Специальный административный район Китая) в 2018 году. В настоящее время он является младшим научным сотрудником Хайнаньского института Чжэцзянского университета (Санья, Китай). Его научные интересы включают преобразование энергии из возобновляемых источников, мониторинг состояния морских ветряных турбин, диагностику неисправностей вращающихся механизмов, а также проектирование конструкций и отказоустойчивое управление высокоэффективными и высокоскоростными внутриколёсными моторами.

(Редактор Юй Чжан)