УДК 004.056.05 004.054

Н.В. Богач, К.Д. Вылегжанина, А.В. Милицын

ОНТОЛОГИЧЕСКИЕ МОДЕЛИ В РАЗРАБОТКЕ ИНСТРУМЕНТОВ ОЦЕНКИ КОММУНИКАЦИОННЫХ ПРОТОКОЛОВ ГЕТЕРОГЕННЫХ ИЕРАРХИЧЕСКИХ БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЕЙ

N.V. Bogach, K.D. Vilegzhanina, A.V. Militsyn

ONTOLOGY MODEL DRIVEN DEVELOPMENT OF ATTESTATION INSTRUMENTS FOR WIRELESS SENSOR NETWORKS

Предложен четырехуровневый иерархический каркас (фреймворк) в качестве средства разработки и аттестации коммуникационных протоколов беспроводных сетей сенсоров. Описаны модели, образующие верхний, онтологический, уровень иерархии.

БЕСПРОВОДНЫЕ СЕТИ; СЕНСОРЫ; ПРОТОКОЛ БЕЗОПАСНОСТИ; ОНТОЛОГИЧЕСКАЯ МОДЕЛЬ; КАРКАС; ФРЕЙМВОРК.

We propose a 4-level framework as a development and attestation instrument for secure communication protocols in wireless sensor networks. We also show how to build its baseline level - the ontology models.

WIRELESS SENSOR NETWORKS; SENSORS; SECURE COMMUNICATIONS; ONTOLOGY MODEL; FRAMEWORK.

Беспроводные сети сенсоров (БСС) находятся в фокусе внимания специалистов в течение последних десяти лет. Вопросы их безопасности выделены в самостоятельную область защиты информации. В зарубежных публикациях проблема защиты была впервые поставлена в [1], там же была предложена первая классификация уже известных компьютерных атак в приложении к БСС, а также рассмотрены две новых атаки, свойственные БСС, шторм hello-сообщений (hello flood) и «ложный сток» (sinkhole). БСС гетерогенной топологии представляют особенный интерес для исследователей ввиду двух обстоятельств: современная информационная среда имеет большое разнообразие аппаратных платформ для построения сетей сенсоров (горизонтальная гетерогенность), распределение ролей в сети сенсоров (наличие узлов с большими возможностями, полномочиями и энергопотреблением и узлов с ограниченной функциональностью и малым энергопотреблением) позволяет достичь лучших показателей по главным задачам поддержки жизненного цикла сети, обеспечивая меньшее суммарное энергопотребление и лучшую управляемость аппаратуры сети и данных (вертикальная гетерогенность).

В настоящее время существует большое количество протоколов для решения частных задач безопасной передачи данных в БСС [2–5] и др. Однако их объективное сравнение и анализ безопасности затруд-

нены вследствие отсутствия единой методологии и инструментов оценки. Представляется конструктивным использовать иерархический подход, при котором сеть сенсоров описывается на различных уровнях абстракции. В качестве инструмента предлагается каркас (фреймворк), состоящий из следующих уровней: *онтологический* (аппаратно, программно и вычислительно независимый уровень моделей, связывающих понятия предметной области БСС), *архитектурный* (аппаратно и программно независимый уровень функциональных блоков коммуникационного протокола), *программный* (аппаратно независимый уровень моделирования режимов работы БСС в сетевом симуляторе с целью количественной оценки параметров протокола), уровень *встраиваемой* программы, где производится оценка накладных расходов портирования программного кода поддержки протокола на конкретную целевую платформу. Интерфейсами между уровнями служат соответственно требования к протоколу, функции протокола и программный код (рис. 1).

Фреймворк универсален как для описания и разработки новых протоколов, так и для аттестации уже существующих. Такой подход к оценке коммуникационных протоколов БСС идейно связан с аналогичными методологиями, существующими, например, в компьютерных сетях (ISO/OSI, TCP/IP) [6], в программной инженерии (IBM RUP, MDA) [7], управлении качеством, менеджменте и бизнесе (Cobit, BSC) [8, 9]. Это закономерно, если иметь в виду, что БСС принадлежит к классу распределенных динамических систем [10, 11].

Разработка моделей уровня онтологий

Онтологический уровень фреймворка (рис. 1) состоит из классификации задач БСС, классификации атак на БСС и модели жизненного цикла БСС.

Классификация задач БСС учитывает связи со смежными областями через пять главных задач поддержки жизненного цикла сети: энергообеспечение, поддержку конфигурации сети, управление данными, локализацию узлов и маршрутизацию. Она отражает интеграцию задач информационной безопасности БСС в общий контекст жизненного цикла сети и является основой для практического применения подхода «обеспечение безопасности на этапе проектирования» (privacy by design) – одной из современных лучших практик безопасности [12]. Вопросы безопасности данных и каналов передачи информации являются критическим приоритетом и не могут решаться изолированно, поэтому проектирование функций безопасности должно вестись совместно с разработкой остальных функций системы.

Представленная далее классификация атак на сети сенсоров по их цели, в отличие от традиционных «плоских» перечислений, позволяет распределить ответственность по компонентам сети и достичь декомпозиции задачи обеспечения информационной безопасности в сетях сенсоров. Следующим шагом выполняется наложение динамики развития атак в БСС на фазы ее жизненного цикла в рамках общей среды моделирования. Совмещение двух предложенных моделей в диаграмме последовательностей жизненного цикла сети помимо выявления критически уязвимых точек жизненного цикла позволяет также сгенерировать требования к функциям протокола, чтобы перейти на следующий (архитектурный) уровень от уровня онтологических моделей. На следующем уровне производится сопоставление требований к протоколу с механизмами защиты, что служит основой разработки архитектуры протокола.

Классификация задач БСС. Сгруппируем задачи обеспечения функционирования беспроводной сенсорной сети следующим образом (см. рис. 2):

1. Поддержка конфигурации.
2. Локализация мобильных узлов.
3. Управление данными.
4. Маршрутизация.
5. Безопасность физической инфраструктуры и данных.

Сенсорный узел беспроводной сети ограничен в вычислительных возможностях и коммуникационных ресурсах. В связи с этим появляются специфические требова-

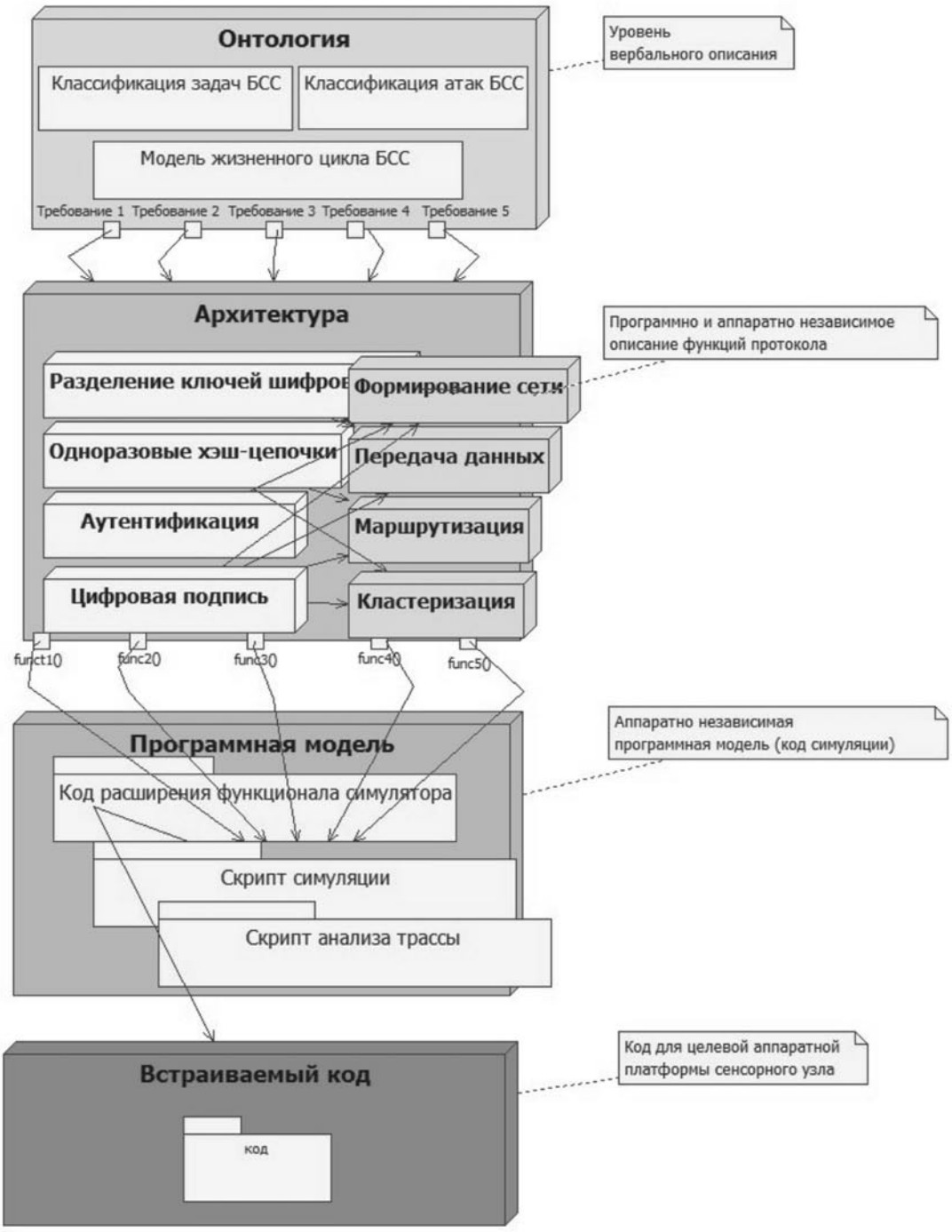

Рис. 1. Фреймворк для разработки и аттестации коммуникационных протоколов БСС

ния к механизмам защиты данных.

Классификация атак на БСС. Злоумышленник может прослушивать радиопередачи, вставлять сообщения и снова передавать ранее перехваченные пакеты. Далее злоумышленник может скомпрометировать рядовые узлы сети и управляющие узлы кластера. Это означает, что злоумышленник получит доступ ко всей информации, хранящейся на данных узлах (такой, как криптографические ключи). Предполагается, что злоумышленник не может скомпрометиро-

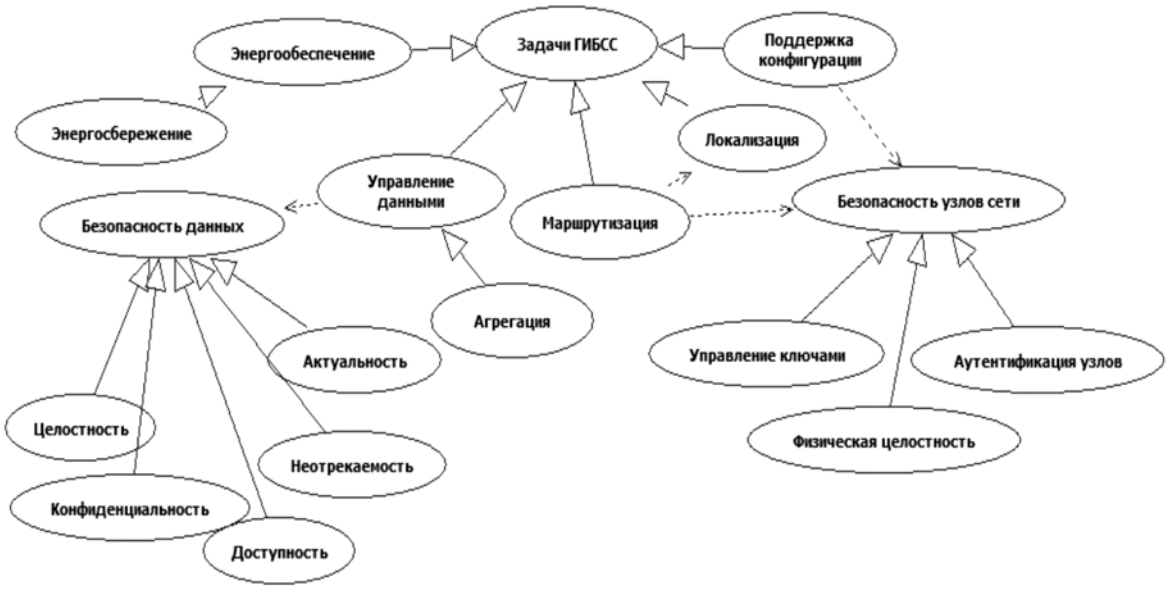

Рис. 2. Классификация задач БСС

вать базовую станцию, и ему требуется некоторое время, чтобы скомпрометировать каждый очередной узел. Целью злоумышленника является подделка информации маршрутизации таким образом, чтобы контролировать все пути маршрутизации между узлами, например, перенаправить себе все сообщения для прослушивания, понизить производительность сети, произвести атаку типа «отказ в обслуживании» [7].

В БСС сохраняется принятое в теории информационной безопасности деление атак на внутренние и внешние, пассивные и активные. Внешние угрозы исходят извне сети сенсоров и могут выражаться в подслушивании передачи данных, а могут быть расширены до вставки поддельных данных с целью потребления ресурсов сети и развертывания атаки отказа в обслуживании. Внутренние угрозы исходят от скомпрометированных узлов, отправляющих злонамеренные данные и злоумышленников, захвативших криптографическое содержимое узлов. Нарушители внутренний и внешний различаются по следующему признаку: внешнему не доступны ключи шифрования и прочие коды, используемые в сети. Пассивные и активные атаки также традиционно отличаются друг от друга тем, что пассивный атакующий заинтересован только в сборе секретных данных из сенсорной сети, т. е. нарушает только секретность и конфиденциальность. Это попытки воспользоваться данными без ведома их владельца. В таком случае атаку сложно распознать, поскольку целостность информации не нарушается, и предотвращение ее более успешно, чем попытки распознать в реальном масштабе времени.

Типичной для сетей сенсоров является разделение атак на атакующие класса «пыль» и атакующие класса «переносной компьютер». *Пылью* принято называть маломощные сенсорные узлы – в таком случае атакующему доступно несколько «пылинок» с такими же возможностями, как и остальные «пылинки» в сети, либо переносной компьютер. Беспроводные сети сенсоров, как и прочие беспроводные сети, поддаются определенным атакам ввиду преобладания широковещательной передачи сообщений и доступности передающей среды. Более того, сети сенсоров более уязвимы, т. к. сенсоры нередко устанавливаются в опасной и неблагоприятной среде, где их может захватить злоумышленник, и не обладают достаточными вычислительными способностями для реализации сильных надежных алгоритмов защиты, не обладают защищенной от подделки аппаратной частью. В случае иерархических БСС добавляются также атаки на управляющий узел кластера [12] (рис. 3).

Рассмотрим, каким образом можно увеличить информативность классификации

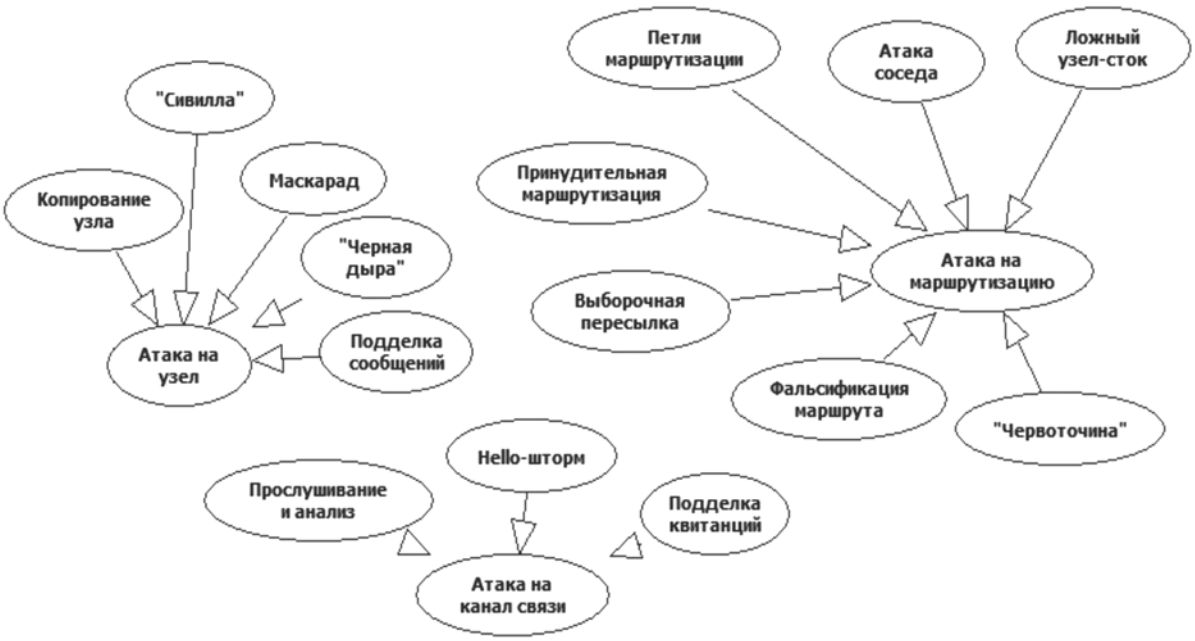

Рис. 3. Модель атак на БСС

атак на сети сенсоров, и выполним совмещение классификации атак с фазами жизненного цикла сети.

Совмещение моделей, выявление критически опасных фаз в жизненном цикле сети сенсоров. Для отображения фаз жизненного цикла сети сенсоров используем диаграмму последовательностей в UML-нотации. Будем считать, что сеть сенсоров имеет только вертикальную гетерогенность: в сети имеется базовая станция, управляющий узел и сенсорный узел. В радиусе вещания сети находится нарушитель, имеющий портативный компьютер с программным обеспечением, позволяющим принимать широковещательные пакеты. Рассмотрим наиболее неблагоприятный сценарий развертывания атаки: раннее внедрение нарушителя в сеть (рис. 4). Из приведенной диаграммы следует, что на фазе конфигурации обмен общесетевыми и общекластерными параметрами доступен злоумышленнику и, следовательно, при разработке или аттестации коммуникационного протокола необходимо ответить, например, на следующие вопросы.

Каким образом обеспечивается конфиденциальность рассылки общекластерных и общесетевых параметров от базовой станции?

Каким образом обеспечивается конфиденциальность ответов от управляющих узлов? От сенсорных узлов?

Имеется ли в протоколе процедура безопасного обнаружения соседей?

Если на раннем этапе у нарушителя существует возможность внедрения в сеть, то дальнейшие механизмы защиты в протоколе не имеют значения. Таким образом, можно выявить первый очевидный приоритет. При моделировании сценариев позднего вторжения в уже сконфигурированную сеть можно выявить два пути проникновения нарушителя: через временный локальный отказ в обслуживании и через фальсификацию маршрутов. Локальный отказ также может быть следствием небезопасной процедуры обнаружения соседей.

Способ внедрения нарушителя в сконфигурированную сеть через навязывание ложных маршрутов представляет значительную опасность для сети. Это дает основания полагать, что именно функция маршрутизации коммуникационного протокола несет наибольшую ответственность за безопасность сети в целом. Таким образом, задачей онтологического уровня является формирование набора требований к протоколу. В

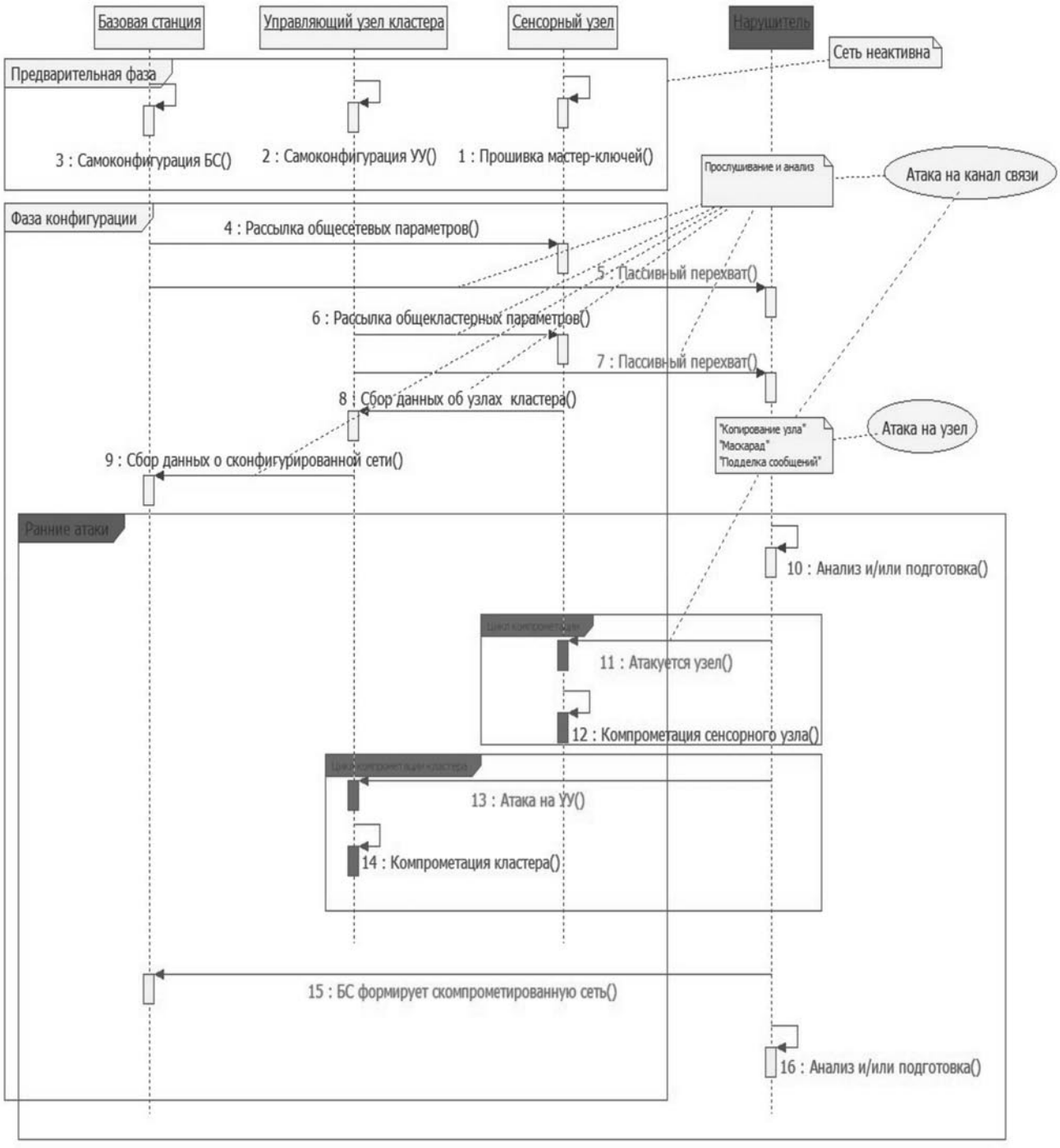

Рис. 4. Модель жизненного цикла БСС в присутствии раннего вторжения нарушителя

дальнейшем эти требования позволят обоснованно выбрать средства защиты при разработке архитектуры протокола.

В статье предложен четырехуровневый иерархический каркас (фреймворк) в качестве средства разработки и аттестации коммуникационных протоколов БСС. Описаны модели, образующие верхний, онтологический, уровень иерархии.

Анализ полноты и безопасности разрабатываемых протоколов для сетей сенсоров

может быть проведен на основе предложенных моделей более наглядно, чем при использовании плоских систем классификации. По результатам анализа формируется набор требований к протоколу, который является интерфейсом к следующему уровню иерархии – уровню архитектуры протокола. Применение иерархического каркаса в разработке или аттестации коммуникационного протокола БСС является основой методологии, имеющей много общего с общепринятыми методологиями и практиками разработки через моделирование (MDD).

СПИСОК ЛИТЕРАТУРЫ

1. **Perrig A. [et al.].** SPINS: Security Protocols for Sensor Networks // Wireless Networks. – 2002. – Vol. 8 – № 5. – P. 521–534.

2. **Wood A.D., Stankovic J.A.** Denial of Service in Sensor Networks // Computer.– 2002. – Vol. 35. –№ 10. –P. 54–62.

3. **Hu L., Evans D.** Secure Aggregation for Wireless Network // Proc. of the 2003 Symp. on Applications and the Internet Workshops (SAINT'03 Workshops). – P. 384–391.

4. **Karlof C., Wagner D.** Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures // Ad Hoc Networks 1. – 2003. – P. 293–315.

5. **Oliveira L.B., Wong H.Ch., Loureiro A.A.** LHA-SP: Secure Protocols for Hierarchical Wireless Sensor Networks. – 2005.

6. **Танненбаум Э.** Компьютерные сети. – 4-е изд. – СПб.: Питер, 2003. – 992 с.

7. **Крачтен Ф.** Введение в Rational Unified Process. – 2-е изд.; Пер. с англ. – М.: ИД «Вильямс», 2002. – 240 с.

8. COBIT 5: A Business Framework for the Governance and Management of Enterprise IT [электронный ресурс] / URL: http://www.isaca.org/Cobit/Pages/default.aspx (дата обращения 16.10.2013)

9. Balanced scorecard basics [электронный ресурс] / URL: https://balancedscorecard.org/bscresources/aboutthebalancedscorecard/tabid/55/default.aspx

10. **Cerpa A., Estrin D.** ASCENT: Adaptive Self-Configuring sEnsor Network Topologies // IEEE Transactions on Mobile Computing. – 2003. – Vol. 3(3). – P. 272–285.

11. **Liang Q.** Ad Hoc Wireless Network Traffic – Self-Similarity and Forecasting // IEEE Communiocation Letters. – 2002. – Vol. 6. – № 7. – P. 297–299.

12. **Dargie W., Poellabauer Ch.** Fundamentals of wireless sensor networks. Theory and practice. –Wiley, 2011.

REFERENCES

1. **Perrig A. et al.** SPINS: Security Protocols for Sensor Networks / Wireless Networks. – 2002. – Vol. 8 – № 5. – P. 521–534.

2. **Wood A.D., Stankovic J.A.** Denial of Service in Sensor Networks / Computer.– 2002. – Vol. 35. –№ 10. –P. 54–62.

3. **Hu L., Evans D.** Secure Aggregation for Wireless Network / Proc. of the 2003 Symp. on Applications and the Internet Workshops (SAINT'03 Workshops). – P. 384–391.

4. **Karlof C., Wagner D.** Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures / Ad Hoc Networks 1. – 2003. – P. 293–315.

5. **Oliveira L.B., Wong H.Ch., Loureiro A.A.** LHA-SP: Secure Protocols for Hierarchical Wireless Sensor Networks. – 2005.

6. **Tannenbaum E.** Komp'iuternye seti. – 4-e izd. –St.-Petersburg: Piter, 2003. – 992 s. (rus)

7. **Krachten F.** Vvedenie v Rational Unified Process. – 2-e izd.; Per. s angl. – Moscow: ID «Vil'iams», 2002. – 240 s. (rus)

8. COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. Available http://www.isaca.org/ Cobit/Pages/default.aspx (Accessed 16.10.2013).

9. Balanced scorecard basics. Available https://balancedscorecard.org/bscresources/aboutthebalancedscorecard/tabid/55/default.aspx

10. **Cerpa A., Estrin D.** ASCENT: Adaptive Self-Configuring sEnsor Network Topologies / IEEE Transactions on Mobile Computing. – 2003. – Vol. 3(3). – P. 272–285.

11. **Liang Q.** Ad Hoc Wireless Network Traffic – Self-Similarity and Forecasting / IEEE Communiocation Letters. – 2002. – Vol. 6. – № 7. – P. 297–299.

12. **Dargie W., Poellabauer Ch.** Fundamentals of wireless sensor networks. Theory and practice. –Wiley, 2011.

БОГАЧ Наталья Владимировна – *доцент Института информационных технологий и управления Санкт-Петербургского государственного политехнического университета.*
195251, Россия, Санкт-Петербург, ул. Политехническая, д. 29.
E-mail: n.v.bogach@gmail.com

BOGACH, Natalia V. *St. Petersburg State Polytechnical University.*
195251, Politekhnicheskaya Str. 29, St.-Petersburg, Russia.
E-mail: n.v.bogach@gmail.com

ВЫЛЕГЖАНИНА Карина Дмитриевна – *ассистент Санкт-Петербургского государственного политехнического университета.*
195251, Россия, Санкт-Петербург, ул. Политехническая, д. 29.
E-mail: k.vilegzhanina@gmail.com

VILEGZHANINA, Karina D. *St. Petersburg State Polytechnical University.*
195251, Politekhnicheskaya Str. 29, St.-Petersburg, Russia.
E-mail: k.vilegzhanina@gmail.com

МИЛИЦЫН Алексей Владимирович – *доцент Санкт-Петербургского государственного политехнического университета.*
195251, Россия, Санкт-Петербург, ул. Политехническая, д. 29.
E-mail: militsyn@gmail.com

MILITSYN, Alexei V. *St. Petersburg State Polytechnical University .*
195251, Politekhnicheskaya Str. 29, St.-Petersburg, Russia.
E-mail: militsyn@gmail.com