УГРОЗЫ И МЕТОДЫ ЗАЩИТЫ В СБОРНЫХ СЕНСОРНЫХ УЗЛАХ ЛЕТАЮЩИХ СЕНСОРНЫХ СЕТЕЙ

Матвеев В.А.[1], Бельфер Р.А.[2], Глинская Е.В.[3]

При проектировании летающих сенсорных сетей (ЛСС) необходимо учитывать информационную безопасность от атак DoS с потенциально высокой вероятностью и ущербом при их реализации. В частности, это относится к атакам, нарушающим функции шлюза сборных узлов информации от сенсорных датчиков с беспилотными летательными аппаратами (БПЛА) FANET. Такие атаки называются sinkhole. Рассмотрены способы осуществления таких атак и методы их предотвращения, что позволяет получить экспертные оценки вероятности и ущерба на разных уровнях атак sinkhole. В плане продолжения исследований планируется разработка методики расчета на основе этих экспертных данных с целью выбора узла с функцией шлюза.

***Ключевые слова**: летающая Ad Hoc сеть, беспилотные летающий аппарат, сборный узел, беспроводная сенсорная сеть, мобильная Ad Hoc сеть, атака «воронка», анонимность*

Введение.

С конца 90-х годов наблюдается рост создания и использования беспроводных сенсорных сетей WSN (wireless sensor network) в гражданской и военной областях [1-3]. Примерами приложения в гражданской области может быть мониторинг окружающей среды, здравоохранение и др. Примером приложения в военной области - наблюдение за полем боя. Необходимость расширения приложений WSN и качества предоставляемых услуг явились причиной проведения работ по созданию использования этой сети в комбинации с мобильной Ad Hoc сетью MANET (Mobile Ad Hoc Netwoks). MANET так же, как и WNS, используется в гражданской и военной областях [4]. В работах [5,6] отмечается возможность крупномасштабного развертывания сети WSN-MANET. Рассматривается предоставление в городах (умный город, smart city) многих услуг – мониторинг шума, света, загрязнения окружающей среды, движения транспортных средств, противоугонная защита, контроль по предотвращению обрушения старых зданий, мостов, экстренная медицинская услуга, услуги пожилым людям и др. Для выполнения требования по ограничению задержки в доставке срочных данных в алгоритме взаимодействия WSN и MANET предусматривается приоритетное обслуживание данных сенсорной сети. При этом следует отметить, что в этой работе не приводится конкретное предложение по реализации сети MANET, которая позволяет получать данные всего города. В настоящее время ведутся работы над несколькими проектами «умного города» с многомиллионным населением (в Бразилии, США, Германии, Европейском Союзе, Южной Корее, Китае). Во многих работах уделяется большое внимание проблемам обеспечения ИБ в таких проектах. В работе [7] приводятся несколько таких проблем, включая защиту от угроз, приводящих к прекращению функционирования всей системы.

В работах российских специалистов [8,9] предлагается новое направление использования WSN в комбинации с летающей Ad Hoc сетью FANET (Flying Ad Hoc Netwoks). Такая сеть WSN- FANET получила название летающие сенсорные сети (ЛСС).

Сеть FANET, включающая беспилотные летающие аппараты БПЛА (Unmanned Air Vehicles, UAVs), использовалась в военной области. В результате недавних технических усовершенствований эти сети применяются для удаленного получения изображений, мониторинга стихийных бедствий, видеотрансляции и других гражданских областей [10].

Отмечается, что FANET имеет более сложные проблемы информационной безопасности (ИБ) по сравнению с MANET, требующие дополнительного исследования. Одними из причин является: более высокая мобильность (скорости БПЛА в диапазоне 20-40 м/сек) и соответственно более быстрое изменение топологии сети; большее расстояние

1 Матвеев Валерий Александрович, профессор, доктор технических наук, МГТУ им. Н.Э. Баумана, Москва, a.matveev@bmstu.ru.
2 Бельфер Рувим Абрамович, доцент, кандидат технических наук, МГТУ им. Н.Э. Баумана, Москва, a.belfer@yandex.ru.
3 Глинская Елена Вячеславовна, МГТУ им. Н.Э. Баумана, Москва, glinskaya-iu8@rambler.ru.

между БПЛА, чем между узлами в MANET.

При использовании аэростатов, высотных телекоммуникационных платформ (High Altitude Platform, HAP) длина земной площади охвата БПЛА составляет 150 км. [9,11], что расширяет возможности использования ЛСС по сравнению с WSN-MANET. Это позволяет применить эту систему при создании «умных городов» с многомиллионным населением и большой территорией.

Взаимодействие FANET с WSN в рамках ЛСС требует дополнительного исследования в обеспечении информационной безопасности. В настоящей работе рассматривается одно из таких направлений - исследование обеспечения информационной безопасности ЛСС от воздействия атак DoS с потенциально высоким ущербом при их реализации. Таким уязвимым местом являются сборные узлы в WSN. Результаты работы предназначены для дальнейших исследований учета ИБ при проектировании ЛСС.

Сборные узлы WSN, подверженные атакам DoS типа sinkhole. На рис.1 показана трехуровневая схема иерархии уровней сборных узлов информации сенсорных датчиков сети WSN для одного их возможных приложений ЛСС.

Самому нижнему уровню соответствуют головные узлы кластеров (cluster heads, CH), собирающие информацию от группы сенсорных датчиков. Сборные пункты, собирающие информацию сенсорных датчиков от группы головных узлов кластера, выполняют функцию второго уровня этой иерархии, которые будем называть транзитными узлами. Самый верхний уровень объединяет информацию от группы узлов sink и называется базовой станцией БС (Base Station). На рисунке показаны две БС. Такая трехуровневая схема иерархии может быть принята, например, для WSN, обеспечивающего функционирование «умного города» с многомиллионным населением и расположенным на большой территории. Другим примером может быть зона боевых действий на большой территории. При проектировании ЛСС стоит задача выбора узла иерархии в качестве шлюза для взаимодействия с группой БПЛА в FANET. Для выбора шлюза важную роль играют результаты анализа угроз ИБ с большим ущербом и вероятностью их реализации. Злоумышленник может препятствовать внутри WSN получению сборным пунктом на каждом уровне полных и корректных сенсорных данных. Такая угроза ИБ в WSN относится к атаке DoS и называется атакой sinkhole (воронка) и таким образом создает серьёзную угрозу нанесения ущерба приложениям [4]. Для создания такой атаки злоумышленник, например, создает маршрут либо в обход БС или транзитного сборного пункта, либо передает в БС искаженную информацию сенсорных датчиков [12,13 и др.]. Наибольший ущерб от реализации такой атаки может быть в том случае, когда функцию шлюза выполняет БС, собирая информацию от всех сенсорных датчиков или большого количества в случае нескольких БС в WSN. Транзитные сборные сенсорные пункты в общем случае так же

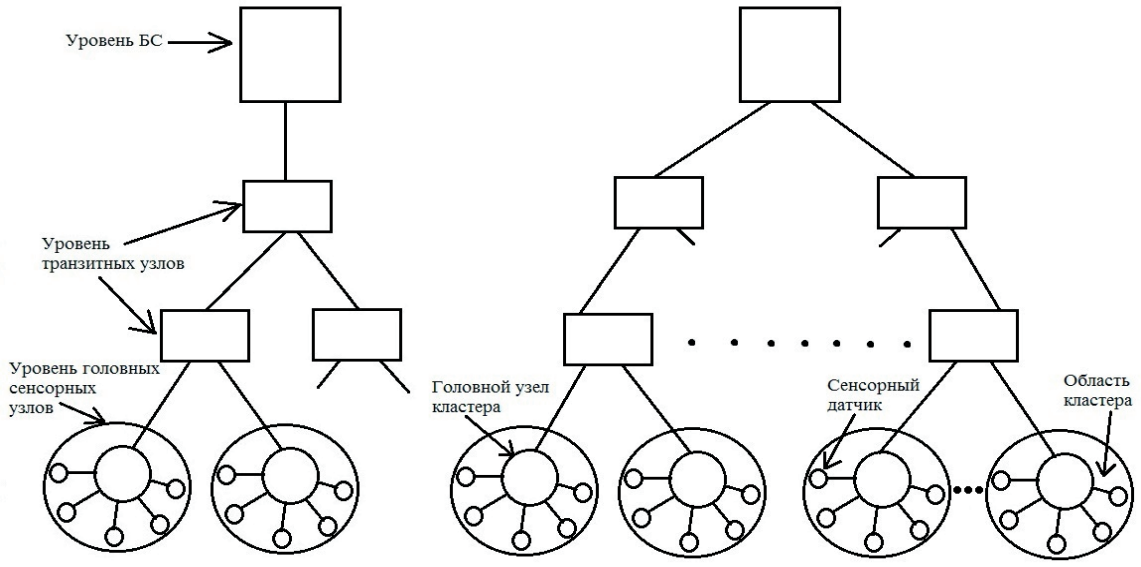

Рис.1 Схема иерархии уровней сборных узлов WSN

***Рис. 1**. Схема иерархии уровней сборных узлов WSN*

представляют многоуровневую иерархическую структуру. При выполнении функций шлюза в транзитных сенсорных узлах второго уровня иерархии ущерб от реализации такой атаки может быть так же значительный и зависит от того, в узлах какого уровня предусмотрена функция шлюза. Чем ближе транзитный сенсорный узел с этой функцией к БС, тем выше может быть ущерб от реализации атаки sinkhole. Наименьший ущерб от атаки такой атаки может быть при выполнении функций шлюза в головном узле кластера, выраженный потерей информации только тех сенсорных датчиков, которые обслуживаются этим узлом.

Во всех рассмотренных случаях, ущерб зависит от числа узлов одного уровня, в которых предусмотрена эта защита.

Выбор шлюза с БПЛА определяется не только ущербом, но и вероятностью реализации атаки sinkhole, которая зависит от предусмотренной степени защищенности от нее.

Защита БС от атаки DoS типа sinkhole. Поскольку вопросы обеспечения безопасности одинаковы для обоих уровней иерархии, то защита от атак DoS типа sinkhole будем рассматривать относительно БС. Много работ по обеспечению ИБ в WSN посвящено обеспечению ИБ WSN предотвращением реализации атак DoS базовых станций с помощью sinkhole. Согласно работе [2] Министерство обороны США придает большое значение обеспечению защиты от этих атак. В условиях военного применения уничтожение функции БС по сбору критически важной информации может привести к частичному или полному прекращению функционирования сети.

Большинство исследований ИБ в WSN относятся к безопасности маршрутизации, управлению ключами и другим вопросам. Механизмы шифрования, аутентификации и др. не могут обеспечить ИБ базовой станции от рассматриваемой атаки DoS типа sinkhole. Наиболее успешной защитой от этой атаки является обеспечение ее анонимности. В работе [14] анонимность (anonymity) объекта (в данном случае БС) с точки зрения злоумышленника означает, что он не может правильно определить ее среди множества объектов (анонимного множества, anonymity set).

Для БС наиболее актуальны три формы анонимности – анонимность подлинности объекта, анонимность месторасположения объекта, анонимность роли объекта в сети и анонимность подлинности [15]. Основное требование для обеспечения анонимности конкретного объекта является то, что должно быть множество объектов с похожими характеристиками. Все множество объектов с разными характеристиками относится к тем объектам, из которых злоумышленник предполагает выбрать те, в отношении которых им будут предприняты угрозы нарушения их ИБ. В случае WSN такими объектами являются сенсорные узлы, головные сенсорные узлы и базовые станции. Первоначально у злоумышленника нет тех знаний, которые позволили бы ему определить конкретный объект (к какому множеству с похожими характеристиками он относится). Например, если WSN включает N узлов, то на этот момент каждый узел имеет 1/N вероятность быть БС. Со временем по результатам анализа системы злоумышленник может изменить эти вероятности и приступить к решению своих задач к определенным объектам (в случае WSN – к БС). Стоит задача скрыть от злоумышленника местонахождения БС [16].

Много опубликованных статей посвящено исследования по оценке анонимности БС и технике повышения ее анонимности. Все предлагаемые в этих работах методы по измерению анонимности рассматриваются с точки зрения злоумышленника. В качестве такой оценки может быть принята, например, вероятность того, что злоумышленнику не удается идентифицировать БС (из множества множеств узлов сети, которые еще не определены злоумышленником) в течение времени t.

Большинство исследований в области анонимности на сегодняшний день были сосредоточены на повышении анонимности данных на физическом, канальном и сетевом уровне на участке между источником и сборным пунктом при получении злоумышленником возможности просматривать эти данные. К такому методу относится анонимность расположения источника (source-location anonymity) и анонимность расположения сборного узла (sinklocation anonymity) [2]. Первый из этих методов предусматривает передачу фиктивных данных между сенсорными узлами по отдельному маршруту с низким трафиком. Задача состоит в том, что определив путь маршрутизации при передаче из конца в конец этих данных, увести злоумышленника от нахождения местоположения БС. Второй метод основан на создании группы из нескольких узлов с одинаковыми характеристиками, что и у ближайших к БС узлов.

При этом следует отметить, что при использовании этих методов повышения анонимности БС сопровождается увеличением потребления электроэнергии сенсорных узлов, увеличиваются за-

держки и снижается пропускная способность даже при отсутствии угрозы злоумышленника. В некоторых работах рассматривается возможность снижения этих характеристик потерь. Экономия электроэнергии в сенсорных узлах в связи с малыми размерами и небольшим ресурсом во многих сенсорных сетях является приоритетной задачей. Существует много алгоритмов функционирования WSN, предусматривающих экономию электроэнергии. В упоминаемой выше работе [2] рассматривается использование алгоритма LEACH (Low Energy Adaptive Cluster Hierarchy), одной из задач которого минимизация энергопотребления сенсорных узлов. Отмечается ряд ограничений LEACH, самым большим из которых является то, что основной задачей при его разработке было повышения времени его работы. При этом не учитывались вопросы обеспечения безопасности. В последующие годы после опубликования LEACH проводились дополнительные исследования для разрешения некоторых из ограничений. Были выпущены такие алгоритмы - E-LEACH, M-LEACH, LEACH-C and V-LEACH. Однако эти алгоритмы не обеспечили снятие всех ограничений.

Приведем другие предложения по технике повышения анонимности:

- установление фиктивных сборных узлов;
- изменение маршрута;
- БС ретранслирует принятые кадры с различной интенсивностью, что бы для злоумышленника она выглядела так же, как и другие узлы сети;
- использование мобильной БС и др.

Планирование продолжения исследований с использованием проведенного анализа. Проведенный анализ атак DoS типа sinkhole в иерархической трехуровневой схеме сборных узлов может быть использован в качестве одного из показателей при проектировании структуры ЛСС. Это относится к рациональному выбору узлов с функцией шлюза взаимодействия WSN с БПЛА сети FANET на основании расчета уровней риска ИБ атак DoS. Как отмечалось выше, этот критерий безопасности не является единственным при решении этой задачи. Для определения риска безопасности DoS атаки необходимо провести исследования по разработке методики, позволяющей оценить уровень риска безопасности атак DoS типа sinkhole. Примером подхода к разработке такой методики могут служить работы [17,18] для другой сети связи (системы сигнализации SIP проводной сети связи следующего поколения). Такие методики предусматривают возможность получения экспертных данных каждой из характеристик риска ИБ угрозы - вероятность реализации злоумышленником и ущерб при ее реализации. Изложенный выше материал дает возможность получить эти характеристики для рассматриваемой атаки в иерархической структуре сборных узлов WSN. Расчет значения риска ИБ атак Dos позволит так же приять меры по повышению защищенности (в данном случае анонимности узла, выполняющего функции сбора информации от сенсорных датчиков).

Выводы

1. При проектировании структуры ЛСС необходимо учесть обеспечение ИБ от воздействия потенциальных угроз злоумышленника с высоким уровнем риска безопасности.

2. Для расчета уровней риска угроз безопасности в ЛСС необходимо разработать методику с использованием в качестве исходных данных экспертных оценок, учитывающих вероятность реализации угроз и ущерб при реализации угроз.

3. Приведенный анализ атак DoS типа sinkhole при различных вариантах выполнения функций шлюза в WSN с БПЛА позволяет получить эти экспертные оценки для расчета уровня риска этих атак.

4. Результаты расчета могут быть учтены при проектировании ЛСС для определения сборных сенсорных узлов WSN с функциями шлюза с БПЛА.

При этом следует учесть, что показатели ИБ не являются единственными критериями выбора шлюза с БПЛА сети FANET. При решении принимаются во внимание технические требования к конкретной прикладной системе ЛСС (время задержки сообщений, надежность, вероятность доставки информации и др.), возможность доступа к БПЛА информации от узлов с учетом ограничений на энергопотребление и др. Например, в ЛСС может оказаться, что ограниченность энергообеспечения не позволяет выполнять функцию шлюза некоторыми сенсорными узлами уровней головных и транзитных сенсорных узлов.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта N15-07-09431а «Разработка принципов построения и методов самоорганизации для летающих сенсорных сетей»

Литература:

1. Ward J. R., Younis M. A Physical Layer Metric for Measuring Base Station Anonymity in Wireless Sensor Networks. First IEEE International Workshop on Security and Forensics in Communication Systems. 2012, pp. 6689-6693.
2. Callanan A.F. Thulasiraman P. Achieving sink node anonymity under energy constraints in tactical wireless sensor networks. Cognitive Methods in Situation Awareness and Decision Support (CogSIMA). IEEE International Inter-Disciplinary Conference. 2015, pp. 186-192. DOI = 10.1109/ICC.2012.6364745.
3. Гольдштейн Б.С., Кучерявый А.Е. Сети связи пост-NGN. - СПб.: БХВ-Петербург, 2013. - 160 с.
4. Бельфер Р.А. Угрозы информационной безопасности в беспроводных саморегулирующихся сетях // Вестник Московского государственного технического университета им. Н.Э. Баумана, серия: Приборостроение. - 2011. - № SPEC - С. 116 - 124.
5. Bellavista, P., Cardone, G., Corradi, A., Foschini, L. Convergence of MANET and WSN in IoT Urban Scenarios. IEEE Sensors Journal, vol. 13, N 10, 2013. pp. 3558-3567. DOI = 10.1109/JSEN.2013.2272099.
6. Cardone, G., Bellavista, P., Corradi, A., Foschini, L. Effective collaborative monitoring in smart cities: Converging MANET and WSN for fast data collection. Kaleidoscope 2011: The Fully Networked Human? - Innovations for Future Networks and Services, Proceedings of ITU. - 2011. 1-8 pp.
7. Silva Ferraz F., Guimaraes Ferraz C.A., Smart City Security Issues: Depicting Information Security Issues in the Role of an Urban Environment, Utility and Cloud Computing (UCC). IEEE/ACM 7th International Conference, 2014. pp. 842-847. DOI = 10.1109/UCC.2014.137.
8. Кучерявый А.Е., Владыко А.Г., Киричек Р.В., Парамонов А.И., Прокопьев А.В., Богданов И.А., Дорт-Гольц А.А. Летающие сенсорные сети // Электросвязь. - 2014. - № 9. - С. 2-5.
9. Кучерявый А.Е., Владыко А.Г., Киричек Р.В. Теоретические и практические направления исследований в области летающих сенсорных сетей. // Электросвязь. - 2015. - № 7. - С. 9-11.
10. Razzaqi A.A., Mustaqim M., Khawaja B.A., Antenna array design for multi-UAVs communication in next generation Flying Ad-Hoc Networks (FANETs). High-capacity Optical Networks and Emerging/Enabling Technologies (HONET): 11th Annual. 2014. pp. 25-28. DOI = 10.1109/HONET.2014.7029355.
11. Temel S., Bekmezci I. On the performance of Flying Ad Hoc Networks (FANETs) utilizing near space high altitude platforms (HAPs). Recent Advances in Space Technologies (RAST), 2013 6th International Conference on, 2013. pp. 461-465. DOI = 10.1109/HONET.2014.7029355.
12. Salehi, S.A., Razzaque M.A., Naraei P., Farrokhtala A. Detection of sinkhole attack in wireless sensor networks, Space Science and Communication (IconSpace), 2013 IEEE International Conference on. 2013. pp. 361 - 365. DOI = 10.1109/IconSpace.2013.6599496.
13. Ngai, E.C.-H., Jiangchuan L., Lyu M.R. On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks. Communications, 2006. ICC '06. IEEE International Conference on, 2006. Vol. 8. pp. 3383 - 3389. DOI = 10.1109/ICC.2006.255595.
14. Andreas P., Marit H. Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminolog, v.0.31, 2008, P. 83. URL: https://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.31.pdf.
15. Ward, J.R. Younis, M. Base station anonymity distributed self-assessment in Wireless Sensor Networks, Intelligence and Security Informatics (ISI). IEEE International Conference. 2015. pp. 103-108. DOI = 10.1109/ISI.2015.7165947.
16. Acharya U., Younis M. An Approach for Increasing Base-Station Anonymity in Sensor Networks, Communications. IEEE International Conference. 2009. pp. 1-5. DOI = 10.1109/ICC.2009.5198720.
17. Yao J., Kangfeng Z., Yixian Y., Shoushan L., Jianpeng Z. Evaluation Model for DoS Attack Effect in Softswitch Network. Communications and Intelligence Information Security (ICCIIS), 2010 International Conference on. 2010. pp. 88-91. DOI = 10.1109/ICCIIS.2010.30.
18. Матвеев В.А., Морозов А.М., Бельфер Р.А. Методика ранжирования угроз фрода и DoS в системе SIP, основанная на методах анализа иерархий и анализа пар // Электросвязь. - 2013. - № 8. - С. 25-27.

THREATS AND PROTECTION METHODS IN SINK SENSOR NODES FLYING SENSOR NETWORKS

Matveev V.A.[4], Belfer R.A.[5], Glinskaya E.V.[6]

When designing a flying sensor networks (FSN) should be considered information security against DoS attacks with potentially high probability and damage in their implementation. In particular, this applies to the attacks, in violation of a gateway sink node of information from sensors to unmanned aerial vehicles (UAVs) FANET. Such attacks are called sinkhole. Considered the methods of such attacks, and how to avoid them to provide expert assessments of probability and damage at various levels of attacks sinkhole. In terms of further research is planned to develop a methodology based on the basis of the expertise to select the node with the function of the gateway.

Keywords*: FANET, UAV, sink node, WSN, MANET, attack sinkhole, anonymity*

4 Valeriy Matveev, Professor, Dr.Sc., Bauman Moscow State Technical University, Moscow, v.a.matveev@bmstu.ru.

5 Ruvim Belfer, Associated Professor, Ph.D., Bauman Moscow State Technical University, Moscow, a.belfer@yandex.ru.

6 Elena Glinskaya, Bauman Moscow State Technical University, Moscow, glinskaya-iu8@rambler.ru.

References:

1. Ward J. R., Younis M. A Physical Layer Metric for Measuring Base Station Anonymity in Wireless Sensor Networks. First IEEE International Workshop on Security and Forensics in Communication Systems. 2012, pp. 6689-6693.
2. Callanan A.F. Thulasiraman P. Achieving sink node anonymity under energy constraints in tactical wireless sensor networks. Cognitive Methods in Situation Awareness and Decision Support (CogSIMA). IEEE International Inter-Disciplinary Conference. 2015, pp. 186-192. DOI = 10.1109/ICC.2012.6364745.
3. Gol'dshteyn B.S., Kucheryavyy A.E. Seti svyazi post-NGN. SPb.: BKhV-Peterburg, 2013. 160 p.
4. Bel'fer R.A. Ugrozy informatsionnoy bezopasnosti v besprovodnykh samoreguliruyushchikhsya setyakh, Vestnik Moskovskogo gosudarstvennogo tekhnicheskogo universiteta im. N.E. Baumana, seriya: Priborostroenie. - 2011. - № SPEC - pp. 116 - 124.
5. Bellavista, P., Cardone, G., Corradi, A., Foschini, L. Convergence of MANET and WSN in IoT Urban Scenarios. IEEE Sensors Journal, vol. 13, N 10, 2013. pp. 3558-3567. DOI = 10.1109/JSEN.2013.2272099.
6. Cardone, G., Bellavista, P., Corradi, A., Foschini, L. Effective collaborative monitoring in smart cities: Converging MANET and WSN for fast data collection. Kaleidoscope 2011: The Fully Networked Human? - Innovations for Future Networks and Services, Proceedings of ITU. - 2011. 1-8 pp.
7. Silva Ferraz F., Guimaraes Ferraz C.A., Smart City Security Issues: Depicting Information Security Issues in the Role of an Urban Environment, Utility and Cloud Computing (UCC). IEEE/ACM 7th International Conference, 2014. pp. 842-847. DOI = 10.1109/UCC.2014.137.
8. Kucheryavyy A.E., Vladyko A.G., Kirichek R.V., Paramonov A.I., Prokop'yev A.V., Bogdanov I.A., Dort-Gol'ts A.A. Letayushchie sensornye seti, Elektrosvyaz'. - 2014. - N 9, - pp. 2-5.
9. Kucheryavyy A.E., Vladyko A.G., Kirichek R.V. Teoreticheskie i prakticheskie napravleniya issledovaniy v oblasti letayushchikh sensornykh setey, Elektrosvyaz'. - 2015. - № 7, - pp. 9-11.
10. Razzaqi A.A., Mustaqim M., Khawaja B.A., Antenna array design for multi-UAVs communication in next generation Flying Ad-Hoc Networks (FANETs). High-capacity Optical Networks and Emerging/Enabling Technologies (HONET): 11th Annual. 2014. pp. 25-28. DOI = 10.1109/HONET.2014.7029355.
11. Temel S., Bekmezci I. On the performance of Flying Ad Hoc Networks (FANETs) utilizing near space high altitude platforms (HAPs). Recent Advances in Space Technologies (RAST), 2013 6th International Conference on, 2013. pp. 461-465. DOI = 10.1109/HONET.2014.7029355.
12. Salehi, S.A., Razzaque M.A., Naraei P., Farrokhtala A. Detection of sinkhole attack in wireless sensor networks, Space Science and Communication (IconSpace), 2013 IEEE International Conference on. 2013. pp. 361 - 365. DOI = 10.1109/IconSpace.2013.6599496.
13. Ngai, E.C.-H., Jiangchuan L., Lyu M.R. On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks. Communications, 2006. ICC '06. IEEE International Conference on, 2006. Vol. 8. pp. 3383 - 3389. DOI = 10.1109/ICC.2006.255595.
14. Andreas P., Marit H. Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminolog, v.0.31, 2008, P. 83. URL: https://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.31.pdf.
15. Ward, J.R. Younis, M. Base station anonymity distributed self-assessment in Wireless Sensor Networks, Intelligence and Security Informatics (ISI). IEEE International Conference. 2015. pp. 103-108. DOI = 10.1109/ISI.2015.7165947.
16. Acharya U., Younis M. An Approach for Increasing Base-Station Anonymity in Sensor Networks, Communications. IEEE International Conference. 2009. pp. 1-5. DOI = 10.1109/ICC.2009.5198720.
17. Yao J., Kangfeng Z., Yixian Y., Shoushan L., Jianpeng Z. Evaluation Model for DoS Attack Effect in Softswitch Network. Communications and Intelligence Information Security (ICCIIS), 2010 International Conference on. 2010. pp. 88-91. DOI = 10.1109/ICCIIS.2010.30.
18. Matveev V.A., Morozov A.M., Bel'fer R.A. Metodika ranzhirovaniya ugroz froda i DoS v sisteme SIP, osnovannaya na metodakh analiza ierarkhiy i analiza par, Elektrosvyaz'. – 2013. – № 8, – pp. 25-27.