Чиж В. Класифікація атак на бездротові сенсорні мережі і шляхи їх візуалізації / Чиж В., Карпінський М., Балабан С. // Вісник ТНТУ. — 2012. — Том 66. — № 2. — С.191-197. — (приладобудування та інформаційно-вимірювальні технології).

УДК 004.94

В. Чиж; М. Карпінський, докт. техн. наук; С. Балабан, канд. техн. наук

Тернопільський національний технічний університет імені Івана Пулюя

КЛАСИФІКАЦІЯ АТАК НА БЕЗДРОТОВІ СЕНСОРНІ МЕРЕЖІ І ШЛЯХИ ЇХ ВІЗУАЛІЗАЦІЇ

Резюме. *Проведено аналіз можливих фізичних та інтелектуальних атак, представлено систему класифікації атак на бездротові сенсорні мережі, виділено характерні особливості окремих видів таких атак. Запропоновано методи візуалізації об'ємних бездротових сенсорних мереж і окремих видів фізичних та інтелектуальних атак на них.*

Ключові слова: *сенсор, бездротова сенсорна мережа, атака, візуалізація, тріангуляція Делоне, діаграма Вороного, класифікація.*

V. Chyzh, M. Karpinski, S. Balaban

CLASSIFICATION OF ATTACK ON WIRELESS SENSOR NETWORKS AND WAYS OF VISUALIZATION

The summary*. Classification of wireless sensor networks (WSN) according to the difference of sensors placement levels and radius of their action was interpreted. To classify WSN according to their structure a network of fire protection was used, which has sensors placed under strict rules in real residential areas. Thus, the network is a classical surface WSN. The network of fire protection is built on a multistoried building and is a conventional Volume WSN. Peculiarities of construction of a scheme of mutual relations between the neighboring sensors should take into account the mutual influence of horizontal layers of the network. WSN have a number of essential advantages over their wired analogues. But at the same time they are characterized by certain disadvantages, such as possibility of being attacked. Efficiency and reliability of the WSN functioning depends on prediction and effectiveness of control methods, of such attacks. In developing and evaluating the effectiveness of methods to withstand the attacks on WSN it is recommended to use a system of attacks classification.*

The system of classification of attacks on WSN was developed. Sensors, signals that are broadcasted in the network as well as confidential information may be subjected to the outside influence. That is why the attacks are divided into physical and intellectual. Physical attacks include mechanical and radio technical ones. The given classification of mechanical attacks makes it possible to facilitate the choice of method of visualization of attack area distribution and parameters of its calculation. Thus, for the visualization of a plain attack two characteristic linear dimensions which characterize the corresponding plane are used. Radio technical attacks involve destruction of an electromagnetic signal. For visualization of such attacks the measuring of a received signal power level is used. In this case the reduction in signal strength is considered as the result of increasing the distance between sensors and thus increasing the area of WSN.

Intellectual or logical attacks are divided into functional and confidential. The functionality of WSN corresponds to the correct operation of all sensors in a network, routing and physical level. Thus, functional attacks are aimed at the destruction of the functional parameters of WSN. These attacks hamper basic sensor to receive complete and correct information from sensors of the lower level. Confidential attacks are divided into traffic analysis information, eavesdropping and manipulation of information routing. Typically, as a result of these attacks the attacker is able to decrypt the information, determine the route and frequency of information transfer with the aim of further organization of functional attacks on WSN. For the visualization of these attacks famous Delaunay methods of triangulation and Voronoi decomposition are used.

The visualization of attacks on WSN is of primary importance. The scheme of plane attacks dissemination in the area of VWSN coverage, scheme of spherical attack distribution in the area of VWSN coverage, scheme of cylinder attack distribution in the area of VWSN coverage have been presented.

Key words: *sensor, wireless sensor networks, attack, visualization, Delaunay triangulation, Voronoi diagram, classification.*

Умовні позначення:

Δh – різниця рівнів розміщення сенсорів, м;

r – радіус дії сенсорів, м.

Постановка проблеми. Бездротові сенсорні мережі (БСМ) розвиваються швидкими темпами і в недалекому майбутньому займуть домінуюче місце серед систем збирання й передавання інформації. БСМ являють собою множину сенсорів, які здатні зчитувати (приймати) певну інформацію, перетворювати її в електромагнітні сигнали, передавати їх в ефір, приймати сигнали від сусідніх сенсорів і повторно передавати їх в ефір. Таким чином у зоні дії БСМ забезпечується поширення інформації і передавання її у потрібному напрямку оптимальним шляхом.

Розширення зон використання БСМ вимагає роботи над їх удосконаленням. Зокрема необхідно постійно збільшувати рівень захищеності сенсорів від фізичного виведення із ладу, сигналів від спотворення і знищення, інформації від розшифрування і викрадення. Перелічених впливів БСМ зазнають під час так званих атак. Для успішного прогнозування можливих атак на БСМ і ефективної боротьби з ними необхідно створити систему їх класифікації і виявити характерні для окремих груп атак особливості.

Аналіз останніх результатів досліджень і публікацій. У літературних джерелах [1, 2] БСМ представляють як поверхню, а для її математичного опису й візуалізації (графічного представлення) використовують, наприклад, методи тріангуляції Делоне, діаграми Вороного і т.д. Можливі атаки на БСМ розділяють на фізичні та інтелектуальні. При цьому аналізу фізичних атак практично не приділяють уваги, а інтелектуальні атаки розглядають як атаки на зміну або знищення сигналу, повне або часткове пошкодження, перехоплення або спотворення інформації [3, 4, 5].

Ступінь впливу на БСМ атаки або групи атак можна визначити візуалізацією атакованої мережі [2, 3, 6]. При цьому для візуалізації атак на силу сигналу використовують тріангуляцію Делоне, а для візуалізації атак – моніторинг трафіку (кількості переданої інформації) в окремих вузлах мережі.

Такий підхід дозволяє отримати позитивні результати, якщо радіус дії сенсорів перевищує різницю рівнів їхнього розміщення, або нехтування висотою поширення мережі не впливає на вибір оптимальної траєкторії передавання інформації. Недоліком представленого аналізу будови БСМ та атак на них є неможливість візуалізації “об’ємних” бездротових сенсорних мереж (ОБСМ) і рівня впливу на їхню роботу фізичних та деяких інтелектуальних атак.

Мета роботи. Постановка завдання. Обґрунтувати класифікацію БСМ за співвідношенням різниці рівнів розміщення сенсорів і радіусу їхньої дії. Запропонувати систему класифікації атак на БСМ. Дослідити характерні особливості візуалізації деяких схем фізичних атак на БСМ.

Результати дослідження. Поставлені завдання запропоновано вирішувати шляхом аналізу структури реально існуючих і ймовірних БСМ.

Як приклад, для класифікації БСМ за їхньою структурою використано ймовірну мережу протипожежної охорони, сенсори якої розміщені за строго встановленими

нормами в реальних житлових районах. Мережа протипожежної охорони збудована у житловому районі з одно- і двоповерховою забудовою являє собою класичну поверхневу БСМ. Особливості побудови візуальної картини такої мережі наведено в [1]. Макет поверхневої мережі зображено на рис. 1. Особливості організації режиму надійної роботи такої мережі передбачають, що співвідношення між різницею рівня розміщення сенсорів і радіусом їхньої дії повинно задовольняти умову (1)

$$\Delta h/r \leq 3. \quad (1)$$

Мережа протипожежної охорони, збудована на базі багатоповерхового будинку, для якої справедлива залежність (2), є класичною ОБСМ (рис. 2). Особливості побудови схеми взаємних зв'язків між сусідніми сенсорами повинні враховувати взаємний вплив горизонтальних шарів такої мережі [7, 8].

$$\Delta h/r > 3. \quad (2)$$

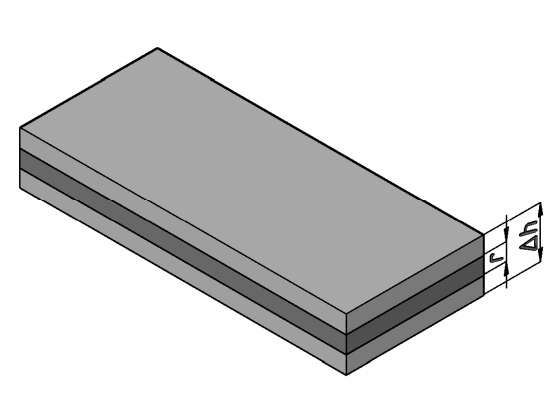


Рисунок 1. Макет поверхневої БСМ
Figure 1. Layout surface WSN

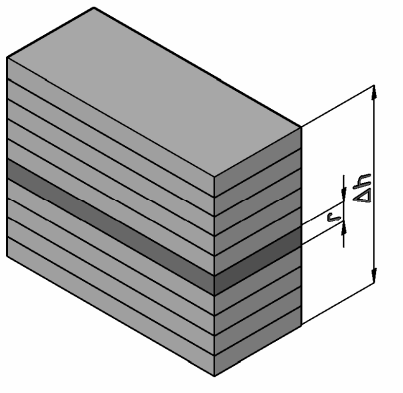


Рисунок 2. Макет ОБСМ
Figure 2. Model VWSN

У реальних умовах для організації БСМ використовують сенсори різних рівнів. При цьому мережу сенсорів вищих рівнів розглядають як поверхневу, а тому мережу в цілому слід розглядати як комбіновану (рис. 3). Отже, за структурними особливостями БСМ доцільно поділяти на поверхневі, об'ємні й комбіновані.

БСМ володіють низкою беззаперечних переваг перед своїми дротовими аналогами. Але одночасно їм характерні недоліки [3], які сповільнюють, а в ряді випадків роблять недоцільним використання в окремих сферах нашої діяльності. До таких недоліків дослідники надійності роботи БСМ відносять вразливість до атак проти них. Успішність і надійність роботи БСМ залежить від досконалості прогнозування та ефективності методів боротьби з такими атаками. Під час розроблення та оцінювання ефективності методів боротьби з атаками на БСМ доцільно опиратися на систему класифікації атак, яка б враховувала сьогоднішній рівень знань і досвід створення та експлуатації БСМ, а також прогнози щодо шляхів їх розвитку.

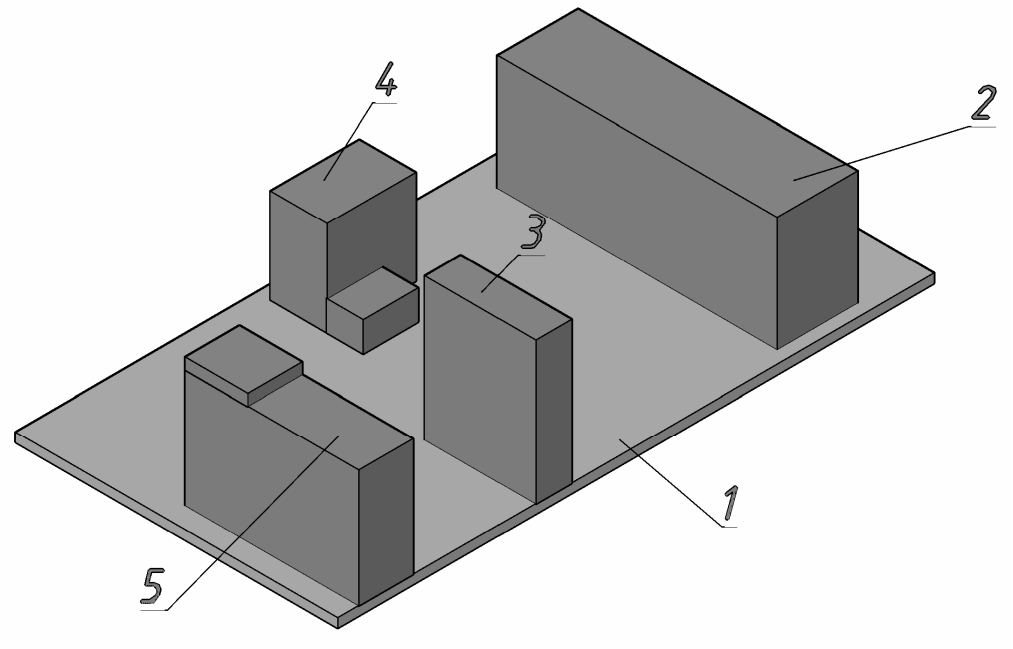
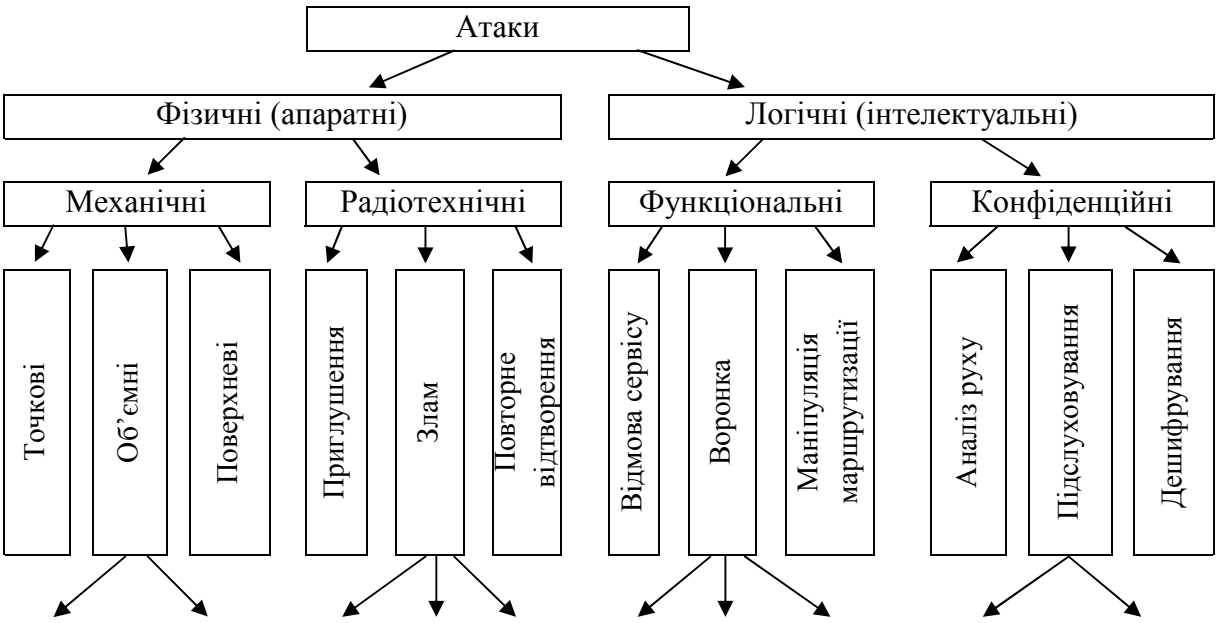


Рисунок 3. Макет комбінованої БСМ: 1) зона поверхневої БСМ; 2, 3, 4, 5) зони ОБСМ
Figure 3. Layout of the combined WSN: 1) the surface area of WSN; 2,3,4,5) zone VWSN

Як було вказано вище, атакам можуть піддаватися сенсори, сигнали, що транслюються у мережі, й конфіденційність інформації. Тому атаки розділяють на фізичні та інтелектуальні (рис. 4). При цьому до фізичних атак відносять механічні й радіотехнічні. Механічні атаки передбачають пошкодження або виведення з ладу сенсорів. Залежно від взаємного розташування пошкоджених сенсорів атаки можуть бути точковими, поверхневими або об'ємними.



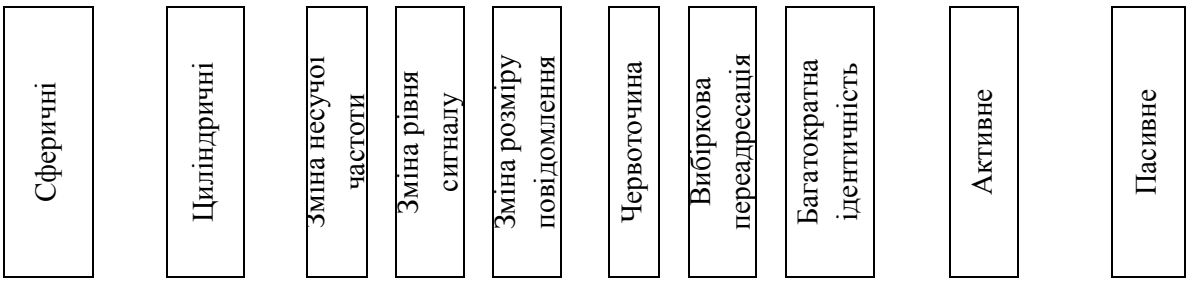


Рисунок 4. Класифікація атак на БСМ
Figure 4. Classification of attacks on WSN

Об’ємні механічні атаки доцільно розділяти за геометричними особливостями зон виведення з ладу мережі на сфероподібні й циліндроподібні.

Запропонована класифікація механічних атак дозволяє полегшити вибір методу візуалізації зони розповсюдження атаки і параметрів її розрахунку. Для візуалізації площинної атаки використовують два характерні лінійні розміри, які характеризують відповідну площину. При цьому третім просторовим напрямком нехтують. Для візуалізації сфероподібної атаки вважають, що зона атаки поширюється у трьох просторових напрямках, які є рівновеликими, тому її можна подати у вигляді сфери або множини сфер, які перетинаються. Для візуалізації циліндроподібних атак використовують три просторові напрямки їх поширення. При цьому два з них є практично незмінними, але достатньо великими, щоб ними нехтувати, а третій є визначальним і достатнім для характеристики напряму розповсюдження атаки. Приклади візуалізації таких атак наведено нижче.

Радіотехнічні атаки передбачають руйнування електромагнітного сигналу. Такого руйнування досягають повним або частковим його приглушенням, зламом з подальшою повною або частковою зміною параметрів сигналу і трансляцією його в мережі. Детальна класифікація атак, спрямованих на приглушення сигналу, подана в літературі [9]. Для візуалізації таких атак застосовують вимірювання рівня потужності прийнятого сигналу. При цьому зменшення потужності сигналу розглядають як результат збільшення відстаней між сенсорами і відповідно збільшення площі БСМ [8].

Атаки, що супроводжуються зламом сигналу, доцільно розділяти на атаки зі зміною несучої частоти, атаки зі зміною рівня сигналу й атаки зі зміною розміру повідомлення. Як правило, успішне проведення більшості радіотехнічних атак вимагає втручання у структуру сигналу, тому ряд авторів розглядають їх як функціональні атаки [3]. Візуалізацію атак, що супроводжуються зламом сигналу, виконують шляхом постійного аналізу структури сигналу [3] і у випадку виявлення відхилень вважають сенсор непрацюючим. Відповідно візуалізацію зон поширення таких атак доцільно проводити аналогічно візуалізації зон поширення механічних атак.

Атаки повторного відтворення передбачають несанкціоноване повторення інформації. При цьому може використовуватися попередньо підслухана або випадково придумана інформація [11]. Даний вид атаки потребує перебування вузла «шкідника» в одній локальній мережі, що й пошкоджуваний вузол. Вузол шкідник відносно просто може контролювати за обміном інформації та блокувати її [12]. Такий вузол перехоплює пакети інформації та імітує роботу звичайного вузла.

Інтелектуальні або логічні атаки розділяють на функціональні й конфіденційні. Під функціональністю БСМ розуміють коректну роботу всіх сенсорів мережі, маршрутизацію і фізичний рівень. Під конфіденційністю розуміють гарантію того, що інформація доступна тільки уповноваженим отримати її особам, які мають можливість отримувати дану інформацію у повному обсязі, своєчасно і без спотворень. Таким чином, функціональні атаки направлені на руйнування функціональних параметрів БСМ. Конфіденційні атаки спрямовані на прослуховування, розшифрування і викрадення інформації. Детальна класифікація й опис таких атак наведені у літературних джерелах [9]. Особливе місце серед функціональних атак займає так звана група атак "воронка" [5, 10]. Такі атаки перешкоджають базовим сенсорам отримувати повну й коректну інформацію від сенсорів нижчого рівня. З допомогою атак "воронка" можна отримати необхідний доступ до інформації в зоні БСМ, яка нас цікавить. Для проведення таких атак створюють шкідливий вузол, дія якого направлена на найближчі сенсори відповідно до маршрутизації. З-поміж групи атак "воронка" виділяють такі впливи на БСМ, як червоточина, вибіркова переадресація і багатократна ідентичність. Для візуалізації вказаних атак використовують відомі методи тріангуляції Делоне і діаграми Вороного [10].

Конфіденційні атаки розділяють на аналіз руху інформації, підслуховування і маніпуляцію маршрутизацією інформації. Як правило, в результаті таких атак зловмисник отримує можливість розшифрування інформації, визначення маршруту і частоти передавання інформації для подальшої організації функціональних атак на БСМ.

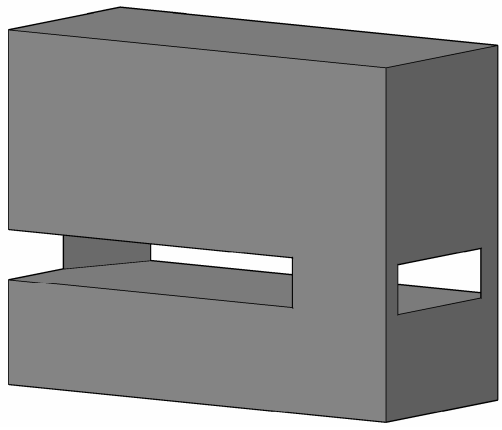


Рисунок 5. Схема розповсюдження площинних атак у зоні дії ОБСМ
Figure 5. Scheme of distribution of plane attacks in the area of VWSN

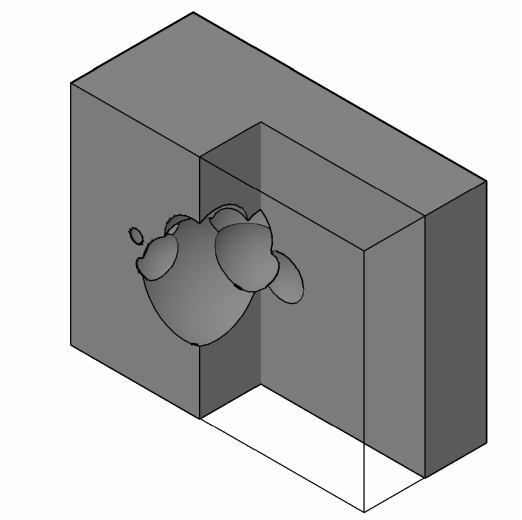


Рисунок 6. Схема розповсюдження сфероподібних атак у зоні дії ОБСМ
Figure 6. Scheme of distribution sferopodibnyh attacks in the area of VWSN

Як зазначалося вище, особливо важливою є візуалізація атак на БСМ. На рис. 5 наведена схема розповсюдження площинних атак у зоні дії ОБСМ, на рис. 6 – схема розповсюдження сфероподібної атаки в зоні дії ОБСМ, на рис. 7 – схема розповсюдження циліндроподібної атаки в зоні дії ОБСМ.

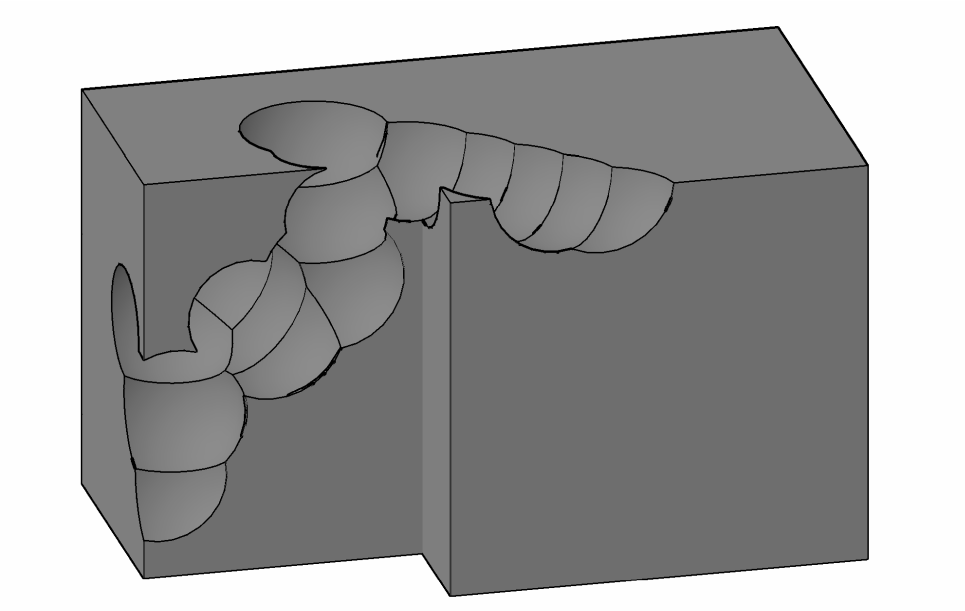


Рисунок 7. Схема розповсюдження циліндроподібних атак у зоні дії ОБСМ
Figure 7. Scheme of distribution of attacks in the cylindrical area of VWSN

Висновки. Доведено доцільність у процесі моделювання БСМ розглядати їх як площинні, об'ємні (ОБСМ) і комбіновані. Запропоновано схему класифікації атак на БСМ, в основу якої покладено аналіз їх впливу на фізичний стан сенсорів, якість і повноту сигналу, конфіденційність інформації. Наведено приклади візуалізації деяких видів механічних атак на ОБСМ.

Вбачається перспективним використання наведених результатів у подальшій роботі, направленій на підвищення надійності БСМ, зокрема, використання запропонованої схеми класифікації атак на БСМ полегшує вибір ефективних методів візуалізації зон уражених БСМ, а приклади візуалізації деяких видів механічних атак на ОБСМ є основою для створення математичних моделей їх поширення в мережах.

Conclusions. VWSN were proved to be treated as plain, three-dimensional (volume VWSN) and combined in the process of modeling. The scheme of WSN attacks classification, based on the analysis of their impact on the sensors physical state, the quality and completeness of the signal and information privacy has been developed. Examples of visualization of certain types of mechanical attacks on VWSN have been presented.

Obtained results are promising ones in the further research aimed at the increase of WSN reliability, the application of the proposed scheme of the classification of attacks on WSN in particular, while the examples of visualization of certain types of mechanical attacks on VWSN are the basis for creating mathematical models of their distribution in networks.

Список використаної літератури

1. Chinh T. Delaunay-triangulation based complete coverage in wireless sensor networks [Електронний ресурс] / Chinh T. Vu, Yingshu Li // PERCOM '09 Proceedings of the 2009 IEEE International Conference on Pervasive Computing and Communications. – 2009. - С. 1–5. - Режим доступу: http://www.cs.gsu.edu/yli/papers/percom2009.pdf. – Назва з екрану.

2. Reda ElHakim. Interactive 3D visualization for wireless sensor networks [Електронний ресурс] / Reda ElHakim, Mohamed ElHelw // The Visual Computer. – 2011. – Volume 21. - Режим доступу: http://www.springerlink.com/content/k4p6728468463149. – Назва з екрану.
3. Giannetsos T. Weaponizing Wireless Networks: An Attack Tool for Launching Attacks against Sensor Networks / Thanassis Giannetsos, Tassos Dimitriou, Neeli R. Prasad; 2010. – Режим доступу: http://www.ait.gr/export/sites/default/ait_web_site/faculty/tdim/various/attackTool-BlackHat10.pdf. – Назва з екрану.
4. A. Becher. Tampering with motes: Real-world physical attacks on wireless sensor networks / A. Becher, Z. Benenson, M. Dornseif // Volume 3934 of Lecture Notes in Computer Science, In J. A. Clark, R. F. Paige, F. Polack, and P. J. Brooke, editors, SPC. - 2006. - Pages 104–118.
5. Chris Karlof. Secure routing in wireless sensor networks: attacks and countermeasures / Chris Karlof, David Wagner // AdHoc Networks Journal, University of California at Berkeley, Berkeley, CA 94720, USA. – Volume 1, Issues 2–3, September 2003. - Pages 293–315.
6. Ioannis Krontiris. SCooperative Intrusion Detection in Wireless Sensor Networks / Ioannis Krontiris, Zinaida Benenson, Thanassis Giannetsos, Felix C. Freiling, Tassos Dimitriou // EWSN '09 Proceedings of the 6th European Conference on Wireless Sensor Networks. – Springer-Verlag Berlin, Heidelberg 2009. – Pages 263–278.
7. Карпінський, М. Перспективні засоби моделювання бездротових сенсорних мереж для мінімізації енерговитрат [Текст] / М. Карпінський, С. Балабан, В. Чиж // Матеріали першої науково-технічної конференції «Інформаційні моделі системи та технлогії». – Тернопіль, 20 травня 2011 р. – С. 36.
8. Карпінський, М.П. Геометричне моделювання у графічному представленні сенсорних мереж [Текст] / М.П. Карпінський, С.М. Балабан, В.М. Чиж // Прикладна геометрія та інженерна графіка. Міжнародний науково-технічний збірник. Доповіді VII міжнародної науково-практичної конференції, присвяченої 65-річчю ДВНЗ «Ужгородський національний університет» та 125-річчю національного технічного університету «Харківський політехнічний інститут» «Геометричне моделювання, комп'ютерні технології та дизайн: теорія, практика освіта». – К.: Віпол, 2011. - Вип. 87. - С. 154–158.
9. Kurytnik I. P. Bezprzewodowa sieć sensorów / I. P. Kurytnik, M. Mikulski, W. Karpinski // Pomiary Automatyka Kontrola. – 2010. – Vol. 56, Nr 6. – P. 548–551. – ISSN 0032-4140.
10. Пат. на корисну модель 64391 Україна: МПК H04W 12/00 [Текст] / Карпінський В.М., Євтух П.С., Боровік Б.Л., Карпінський М.П.; власник патенту Тернопільський національний технічний університет ім. І. Пулюя. – № u 2011 03578; заявл. 25.03.11; опубл. 10.11.2011, Бюл. № 21. – 4 с.
11. Johnson David B. Mobility Support in IPv6 / David B. Johnson, Charles E. Perkins, Jari Arkko // Internet Request for Comments RFC 3775. – June 2004. – P. 165. – Режим доступу: http://www.cs.rice.edu/~dbj/pubs/rfc3775.txt. – Назва з екрану.
12. Шнитман, В.З. Реализация функций мобильности в протоколе IPv6 и анализ их безопасности [Текст] / В.З Шнитман [Електронний ресурс]. – Режим доступу: http://ipv6.ispras.ru/mobile_rev.pdf. – Назва з екрану

Отримано 13.02.2012