Р Е З Ю М Е

НА НАУЧНИТЕ ТРУДОВЕ

на д-р инж. ГРИГОР РАЙКОВ ВЕЛЕВ

Научните трудове са представени в три категории:

I. Монографични трудове
II. Научни статии и доклади
III. Научно-изследователска и развойна дейност

I. МОНОГРАФИЧНИ ТРУДОВЕ

II.1.1. Велев Г., **Телекомуникационни мрежи (монография)**

Настоящата монография представя телекомуникационни технологии, стандарти и принципи на цифровите комуникационни системи.

Монографията е разделена на пет части и е предназначена да даде отговори на следните основни въпроси:

- *Теоретичните и физическите основи на комуникационните среди на базата на OSI модела и протоколите от TCP/IP протоколен стек, както и на значението на стандартите и основните стандартизационни органи в сферата на телекомуникациите;*
- *Обработката на сигнали, тяхното предаване и основните ограничаващи фактори за скоростта на предаването на информация през предавателен канал, основните техники, използвани в системи за предаване през цифрова телекомуникационна мрежа;*
- *Основните разлики между техниките за превключване на вериги и пакети;*
- *Локални мрежи и организиране на връзките през LAN;*
- *Предоставяне на широколентов достъп до Интернет, протоколи и тяхната работа;*
- *Процеса на проектиране на ведомствена комуникационна мрежа.*

II.1.2. Велев Г., **Маршрутизация в мобилни самоорганизиращи се мрежи (книга на база на дисертационен труд)**

В настоящият труд са определени същността и основните характеристики на мобилните самоорганизиращи се мрежи. Анализирани са маршрутизиращите протоколи за MANET, като класификацията им е допълнена за целите на изследването. Прегледани са методите и техниките за моделиране и формално описание на процеси и алгоритми.

Предложен е формален модел на MANET и е описан алгоритъмът за откриване на маршрут в AODV протокола. Предложен е модел на модифициран AODV с отчитане на параметри на състоянието на междинните устройства, изграждащи маршрута. Разработен е модел за йерархична клъстерна маршрутизация за MANET на тактическо ниво, при който се използва логическо разделяне на подмрежи за управление на мобилността на членовете на организационната група.

Построен е обобщен мрежов модел, моделиращ процесите на предложената във втора глава, йерархична клъстерна маршрутизация. Анализирана е ефективността на модифицирания AODV протокол в сравнение с AODV, на базата на симулационни изследвания.

II. НАУЧНИ СТАТИИ И ДОКЛАДИ

II.2.1. Велев Г., **Подходи за изграждане на MPLS-базирани ведомствени телекомуникационни мрежи** (Научна конференция с международно участие "Военни технологии и системи за осигуряване на отбраната"(MT&S 2011), Сборник доклади, стр.198 – 204, ISBN 978-619-90024-1-4, София, 2011г.)

Изборът на най-подходящия подход за изграждане на телекомуникационна мрежа е от решаващо значение за реализация на даден проект. Докладът представя различни варианти за изграждане на телекомуникационни мрежи от ново поколение, използващи протоколи IP, MPLS и ATM.

II.2.2. Велев Г., **Анализ и класификация на маршрутизиращи протоколи за мобилни разпределени мрежи** (Шеста международна научна конференция „Решения и технологии за интелигентна отбрана", Хемус 2012, Сборник доклади, стр. II-37 - II-42, ISSN 1312-2916, София, 2012г.)

Тази статия предоставя класификация на протокола за маршрутизиране MANET. За сравняване и анализиране на протоколи за маршрутизиране на мобилна ad hoc мрежа е от съществено значение подходящата класификация. Дизайнът на протоколите се ръководи от специфични цели и изисквания, базирани на съответните допускания за свойствата на мрежата или областта на приложение.

II.2.3. Велев Г., **Развитие и усъвършенстване на стационарната комуникационна система на БА** (Списание CIO, ИТ сигурност 2012, стр. 55-56, юли 2012г. , ISSN 1312-5605)

Бурното развитие на телекомуникационните технологии в последните години оказва силно въздействие на всички области от обществения живот, включително и в сферата на сигурността и отбраната. Особено съществена е ролята на изградените комуникационни способности, в контекста на „интелигентната отбрана" на принципа на „обединяване и споделяне". Усъвършенстването на комуникационната система, като основен елемент от системата за командване и управление, комуникации, компютри и разузнаване (C4I) е един от основните приоритети на МО.

II.2.4. Велев Г., **Мобилни разпределени мрежи – приложение за целите на отбраната** (Списание CIO, ИТ сигурност 2013, стр. 50–51, юли 2013г. , ISSN 1312-5605)

За създаване на ефективни и динамични комуникации за военни цели (на бойното поле), при извънредни ситуации и оказване на помощ при бедствия е необходимо бързото разгръщане на мобилни потребители. При тези важни мрежови сценарии не може да се разчита на организирана или централизирана свързаност, а е необходимо използването на т. нар. мобилни разпределени мрежи (Mobile Ad Hoc NETworks – MANETs). На латински терминът „ad hoc" означава „за тази цел само" и е точно описание на спецификата на този вид безжични мрежи. MANETs се очаква да играят важна роля в бъдещите цифрови бойни полета (Digital Battle Fields), осигурявайки необходимите тактически мрежи.

II.2.5. **Велев Г., Модел на ad hoc on-demand distance vector маршрутизиращ алгоритъм с отчитане на параметри на състоянието на междинните устройства, изграждащи маршрута** (Научна конференция с международно участие „Военни технологии и системи за осигуряване на отбраната-2013 (MT&S-2013)", Сборник доклади, стр. II-41-51, ISSN 2367-5942, София, 2014г.)

През последните години мобилните и безжичните мрежи имат огромен ръст в технологичния напредък. Поради динамично променящата се топология на MANET е желателно да се проектират ефективни алгоритми за маршрутизиране, които могат да адаптират поведението си към честите промени в мрежата. Докладът предлага модел на модифициран алгоритъм за векторно маршрутизиране на разстояние при поискване Ad hoc за мобилни ad-hoc мрежи и включва показатели за оценка на състоянието на възлите в процеса на откриване на маршрут.

II.2.6. Велев Г., **Проблеми на сигурността в мобилните самоорганизиращи се мрежи** (Научна конференция-2015, „Новите предизвикателства пред системите за информационна сигурност", Сборник научни трудове, стр. 296 – 300, ISBN 978-954-9681-65-9, Шумен, 2015 г.)

Мобилната ad hoc мрежа (MANET) е система от безжични мобилни възли, които динамично се самоорганизират в произволни и временни мрежови топологии. Предоставянето на услуги за сигурност в MANET е свързано с набор от предизвикателства, специфични за тази нова технология. В този доклад се обсъждат проблеми със сигурността, уязвимостта на мобилната ad hoc мрежа и основните видове атаки, които съществуват в нея.

II.2.7. Велев Г., **Архитектура на мобилна самоорганизираща се мрежа за тактическо ниво** (Списание CIO, ИТ сигурност 2016, стр. 62 – 63, юли 2016, ISSN 1312-5605)

Мобилните самоорганизиращи се мрежи са се появили като концепция за военни динамични безжични мрежи още през 70-те години на миналия век. Настоящето развитие на преносимите устройства, които непрекъснато увеличават своята изчислителна мощност, стават с все по-малки размери, по-евтини, по-удобни и с възможности за изпълнение на все повече приложения и мрежови услуги, както и усъвършенстването на технологиите за безжични комуникации, предизвикаха интереса на изследователите и индустрията към тези мрежи отново, в началото на нашия век. Специфичните им свойства ги правят приложими в много области – за тактически мрежи за военни и специални операции, при бедствени ситуации, виртуални класни стаи, домашни и офис мрежи и др.

II.2.8. N. Stoianov, M. Bozhilova, G. Velev, **Towards security requirements of the SPIDER project** (Proceedings Scientific Conference with International Participation on Cyber security in the Information Society, pp. 25-31, ISBN 978-954-9681-82-6, Shumen, Bulgaria, 2017г.)

Необходимостта от използване на сензорни системи и мрежи за вътресградна ситуационна осведоменост при градски военни операции предявява строги изисквания за тяхната сигурност и надеждност. Докладът дефинира понятия, свързани със сигурността в съответствие с предназначението и функциите на сензорната система.

II.2.9. Enev, E., Grigor Velev, Nikolai Stoianov, and Maya Bozhilova, **Requirements to the Sensor Platform and Network for Indoor Deployment and Exterior Based Radiofrequency Awareness** (International Research Conference "105 Years Research and Knowledge for the Security and Defence, Bulgarian Military Academy "G. S. Rakovski", pp. 299 – 303, ISBN 978-619-7478-00-6, Sofia, 2017)

Докладът представя резултати от проучването на проблемите, свързани с използване на сензорна платформа и мрежа за вътрешно разгръщане и външно базирано радиочестотно осведомяване в градски операции. Избрани са основни тактически изисквания и пространствено-времеви параметри, в които трябва да работят техническите средства за придобиване на информация и данни. Докладът представлява и допълнителна информация за бъдещите тенденции на експерименти в този проект.

II.2.10. Велев, Г., Илиев Р., **Обобщеномрежов модел за маршрутизация в MANET-мрежи чрез използване на йерархичен клъстерен алгоритъм** (Девета международна научна конференция „Научните изследвания, иновации и индустриално сътрудничество в интерес на общата Европейска отбрана и сигурност Хемус 2018", Сборник доклади, II-97 - 109, 31.05.2018. Пловдив, ISSN 1312-2916, София, 2018 г.)

В доклада е представен обобщен мрежов модел на маршрута в мобилните ad hoc мрежи (MANETs), използващ йерархичен клъстерен алгоритъм m-AODV (модифициран AODV) за подобряване на търсенето на маршрут чрез анализиране на параметрите на състоянието в междинни мрежови устройства.

II.2.11. Стоянов Н., М. Божилова, Г. Велев, **Технологии от ново поколение подпомагат операциите в града** (CIO, ИТ в отбраната, бр. 7, 2018, pp.68-69, https://cio.bg/digitalizacia/2018/07/24/3432763_tehnologii_ot_novo_pokolenie_podpomagat_operaciite_v/, ISSN1312-5605)

Статията представя проектът за разработване на иновативна система за подпомагане на военни операции в градски условия, чрез подобряване на ситуационната осведоменост за вътрешността на сградите. Основната задача на проекта е да се предостави в реално време карта на вътрешността на сградата от интерес, откриване и локализиране на присъствие на хора в тази сграда, като се използват данни от вътрешни и външни сензори, осигуряващи недостижима по друг начин информация на участващите в операцията.

II.2.12. Велев Г., Божилова М., **Модел на клъстърен маршрутизиращ алгоритъм за мобилни самоорганизиращи се мрежи за отбрана и сигурност** (Деста международна научна конференция "Научните изследвания и инвестициите в технологични иновации - решаващ фактор за отбраната и сигурността" Хемус 2020 Сборник доклади, стр.от II-179 до II-186, 1.10.2020 г. Пловдив, ISSN 1312-2916, София, 2020г.)

Мобилна самоорганизираща се мрежа е система от мобилни безжични устройства, които динамично се самоорганизират във временна мрежова топология, без да е необходимо съществуването на предварително изградена инфраструктура. Създаването на надеждни и

устойчиви клъстери, които да не се преконфигурират в по-голям период от време е трудна задача, поради мобилността на устройствата. В доклада е предложен подход за разделяне на MANET на клъстъри, с отчитане на приемното ниво на сигнала от главния възел и ограничаване на броя на членовете на клъстъра. Главният възел се избира на базата на енергийната мощност на устройството и степента му на комуникационна свързаност. Предложеният подход позволява повишаване на стабилността на клъстърната структура, а следователно и ефективността на маршрутизацията в MANET.

II.2.13. N.T. Stoianov, M.G. Bozhilova, G.R. Velev, **Honeypot types as a possible data source for the CYRADARS project** (Математичне та Імітаційне Моделювання Систем, МОДС 2020, П'ятнадцята Міжнародна Науково-Практична Конференція, p.p.144 - 146, УДК 004.94(063), ISBN 978-617-7571-93-2, Україна, м. Чернігів, 2020)

Докладът представя преглед на видовете honeypots от гледна точка на проект CyRADARS. Honeypot може да се използва за събиране на модели на атаки от зловреден софтуер, изучаване на поведението на хакери, търсене на вътрешни атаки от вътрешни лица и т.н. Изучаването на заплахите без въздействие върху производствените системи и мрежи е обещаващ инструмент за събиране на изследователски данни. Проучването разглежда honeypots с отворен код. Целта е да се изберат най-приложимите типове honeypots и начините, по които те трябва да бъдат разположени, така че инструментите на CYRADARS да получат подходящи данни.

II.2.14. Yanakiev, Y., Stoianov N., Kirkov D., & Velev G., **Defence Strategy and New Disruptive Technologies Nexus: Implications for the Military Organisations** (Journal of Defence & Security Technologies. 3(1), 2020, pp. 7-41.https://www.jdst.eu/publications/defence-strategy-and-new-disruptive-technologies-nexus-implications-military, ISSN 2534-9805 (print), ISSN 2534-9813 (electronic), NACID: 1763).

Тази статия има за цел да проучи ролята на стратегията в областта на отбраната, със специален фокус върху това как технологичните иновации могат да повлияят на развитието на стратегията. Ключовият въпрос е как и по какви начини технологичният напредък може да повлияе на развитието на отбранителната стратегия. Започва с еволюция на концепцията за отбранителна стратегия през последните години, както и нейната възможна бъдеща трансформация, успоредно на тенденциите на новите и възникващи отбранителни технологии. След това се анализират различни концептуални модели на отбранителна стратегия на основа на стратегически документи в областта на отбраната на страните, представени в консорциума по проект на ЕС „Predictive methodologY for TecHnology Intelligence Analysis" (PYTHIA), както и на документи на ЕС и НАТО. Накрая, статията обобщава някои изводи относно динамичния характер на взаимовръзката между развитието на отбранителните стратегии и технологичните иновации. Освен това, са представени някои идеи относно това, как научните изследвания в областта на отбраната могат да отговорят на оперативните нужди, като подкрепят с нови знания производството и доставката на най-необходимите оръжейни системи.

II.2.15. Laso, P.M., L. Salmon, M. Bozhilova, I. Ivanov, N. Stoianov, G. Velev, C. Claramunt, Y. Yanakiev, **ISOLA: An Innovative Approach to Cyber Threat Detection in Cruise Shipping.** (Developments and Advances in Defense and Security. Smart Innovation, Systems and Technologies, vol 255, pp.71-81, https://doi.org/10.1007/978-981-16-4884-7_7, Springer, Singapore, 2022)

Днешните круизни кораби могат да превозват повече от 5500 пътници и 2200 членове на екипажа със средно време на пътуване от седем дни. Круизната индустрия представлява голяма част от туристическия пазар и търсенето нараства. Въпреки големия брой хора на борда, докладването на престъпления на круизните кораби досега е сравнително ниско. Докато самият кораб е изправен пред заплахи за сигурността, дейностите на борда и на брега предоставят много възможности за използване на цели и проблеми със сигурността. С разполагането на дейности и сензори за данни на борда има спешна нужда от разработване на алгоритми за обединяване на данни, за да се осигури глобален поглед върху информационната среда. Изследването, представено в този документ е анализ на текущите кибер рискове в морето, със специфичен фокус върху круизни кораби, които в момента са в процес на разработка в рамките на проекта H2020 ISOLA. В статията са описани и обсъдени няколко алгоритма за синтез на данните и най-накрая са обсъдени по-нататъшните нужди от по-сигурни кибер среди.

II.2.16. Велев Г., **Машинно самообучение и 5G мрежи,** (Единадесета международна научна конференция „Научните изследвания, технологии и иновации – основа за изграждане на нови отбранителни способности Хемус-2022, стр.II-153-159, 2-3.06.2022 Пловдив, ISSN 1312-2916, София, 2023г.)

През последните години има нужда от по-високо ниво на интелигентност в мобилните мрежи, за да се изучи задълбочено и точно работната среда и поведението на потребителите, с цел да се изградят проактивни и ефективни (само)обновяващи се мрежи. Този доклад описва ролята на машинното обучение в 5G мрежите за изграждане на адаптивна производителна мобилна мрежа от следващо поколение.

II.2.17. Велев Г., **Облачни технологии и услуги в комуникациите** (Единадесета международна научна конференция „Научните изследвания, технологии и иновации – основа за изграждане на нови отбранителни способности Хемус-2022, стр.II-153-159, 2-3.06.2022 Пловдив, ISSN 1312-2916, София, 2023г.)

В доклада са разгледани облачните технологии в областта на комуникациите и предоставяните услуги за електронен обмен на информация при съвместна работа, обучение, бизнес процеси и др. Предложен е подход за използване на различни софтуерни решения за организиране на комуникационен обмен между работни екипи свързани със сигурността и отбраната.

III. НАУЧНО-ИЗСЛЕДОВАТЕЛСКА И РАЗВОЙНА ДЕЙНОСТ

(ТИД, ТТЗ, проекти, програми, методики и др.)

В този раздел са включени учебно-методически трудове, свързани с участие на автора при разработване на технико-икономически доклади, тактико-технически задания, проекти за изграждане и развитие на комуникационни и информационни системи, както и програми и методики за изпитване и приемане на комуникационни системи, автоматизирани информационни системи и подсистеми, както и на други изходни документи, необходими за придобиване на комуникационни и информационни продукти за нуждите на Министерство на отбраната, Българската армия и подчинените им структури.

През 2000 г. беше изготвено тактико-техническо задание за изграждане на фрагмент от стационарната цифрова интегрирана свързочна система на БА(СЦИСС-БА) – "СТРАНДЖА-2" (Х. Петков-ръководител, Г. Велев-разработчик) основаващо се на иновативни комуникционни технологии за модернизиране на стационарната комуникационна система на БА.

През 2001 г. са разработени работни проекти за изграждане на стационарната комуникационна и информационна система на БА, в които са проектирани различните подсистеми. Авторът самостоятелно е разработил подсистема "Радиорелейни преносни системи" и Приложения – Част II, включващи карта с нанесени всички ОСВ и КИВ на СЦИСС, изчисляване на радиорелейни интервали и оптически кабелни линии. В приложението е отразена цялата топология на СЦИСС-БА. Като съавтор при проектирането, участва в разработването на общосистемни въпроси за системата, функционални изисквания и комплектация на доставките за изграждане на фрагмента от СЦИСС на БА.

През 2006 г. авторът участва при разработването на програми и методики за провеждане на изпитвания за въвеждане в експлоатация на подсистемите от фрагмента от СЦИСС-БА „Странджа-2" и системата като цяло. Фрагмента от СЦИСС-БА „Странджа-2" е въведен в експлоатация през 2007 г.

През 2008 г. от колектив (А. Темелков ръководител) е изготвено тактико-техническо задание за Разширяване и развитие на СКС на БА, чрез надграждане с MPLS/IP функционалност и оптимизиране на управлението на СКС на БА, в което авторът участва.

През 2013 г. е разработен технико-икономически доклад за развитие на корпоративната информационна система за отбрана (387 стр.), с включено обстойно изследване на съществуващи системи, технологии, решения и световни тенденции в изграждането на такива системи и модернизирането им върху облачна инфраструктура. Документът е разработен от: Г. Велев (ръководител), Р. Илиев, А. Генчев, Н. Стоянов, М. Ангелов, И. Иванов, И. Христозов, Й. Йорданов, Г. Грънчаров.

През 2014 г. е изготвено тактико-техническо задание (121 стр.) за изграждане на системата (от Г. Велев, А. Генчев и Р. Илиев), базирано на прилагане на съвременни облачни технологии и информационни среди за съвместна работа (прието от Съвета по въоръженията).

През 2017 г. беше изготвено тактико-техническо задание (145 стр.) за изграждане на „Комуникационна и информационна система на батальонна бойна група. В ТТЗ са включени системни, архитектурни и технически изисквания за изграждане на системата.

През 2017 г. беше изготвено тактико-техническо задание (38 стр.) за модернизиране на "Комуникационната преносна подсистема (мрежа) осигуряваща работата на „Брегова система за контрол на корабоплаването и охрана на морската граница – Екран-М". В ТТЗ са включени системни и технически изисквания при модернизиране на комуникационната мрежа осигуряваща абонатните системи от система Екран.