СЕНАТУ УНИВЕРЗИТЕТА УНИОН У БЕОГРАДУ

ПРЕДМЕТ: Извештај комисије за оцену и одбрану докторске дисертације

Одлуком Сената Универзитета Унион, у Београду на седници одржаној 21.12. 2020. године, именовани смо за чланове Комисије за оцену и одбрану докторске дисертације Немање Радосављевића, мастера организационих наука, под насловом: *Безбедност и енергетска ефикасност Интернета ствари заснованог на бежичним сензорским мрежама*. Након прегледа добијене документације, Комисија у саставу:

1. др Селена Вукотић, доцент, Рачунарски факултет, Универзитет Унион,

2. др Дејан Драјић, ванредни професор, Електротехнички факултет, Универзитет у Београду,

3. др Ђорђе Бабић, ванредни професор, Рачунарски факултет, Универзитет Унион,

подноси Сенату Универзитета Унион следећи

И З В Е Ш Т А Ј

У току школске 2019/2020. године, Немања Радосављевић, мастер организационих наука, пријавио је тему докторске дисертације под насловом „Безбедност и енергетска ефикасност интернета ствари заснованог на бежичним сензорским мрежама“, након чега је Сенат Универзитета Унион именовао комисију за оцену подобности теме и кандидата. Комисија је Сенату Универзитета Унион поднела извештај у коме се прихвата предложена тема, након чега је одобрена израда докторске дисертације. За ментора је именован ванредни професор Рачунарског факултета, проф. др Ђорђе Бабић.

Истраживање у оквиру ове дисертације спада у област интернета ствари, која припада научној области рачунарског инжењерства, за коју је матичан Рачунарски факултет.

Немања Радосављевић рођен је 28.04.1985. у Београду. Основну школу и гимназију завршио је у Београду. Након завршетка гимназије, 2004. године уписује основне студије на Рачунарском факултету на коме дипломира 2008. године са радом на тему „ UWB бежичне комуникације“. После основних студија уписује мастер студије на Факултету организационих наука које завршава 2009. године одбраном мастер рада на тему: „Приступачност WEB-а“. Студије завршава са просечном оценом 9,43. Од 2009. до 2013. године ради као веб-девелопер у фирми ЦЕТ (Computer Equipment & Trade), а од 2013. године је у сталном радном односу на Рачунарском факултету у Београду са академским звањем: асистент.

У току досадашњег рада на истраживању у вези са темом предложене дисертације, кандидат Немања Радосављевић објавио је, или му је прихваћено за објављивање, један рад у часописима међународног значаја категорије М23 (часописи на SCI листи) као први аутор, један рад на међународним конференцијама категорије М33 и један рад у домаћим часописима категорије М 53.

1. Nemanja Radosavljević, Đorđe Babić, Power Consumption Analysis Model in Wireless Sensor Network for Different Topology Protocols and Lightweight Cryptographic Algorithms, prihvaćen za objavu u *Journal of internet technology*, 2020, ISSN: 1607-9264 (M23).
2. Nemanja Radosavljević, Đorđe Babić, Overview of security threats, prevention and protection mechanisms in wireless sensor networks, *Journal of Mechatronics, Automation and Identification Technology*, Vol. 5, No. 2, pp. 1 – 6, 2020 (M53).

3. Nemanja Radosavljević, Đorđe Babić, Pregled sigurnosnih pretnji i mehanizama prevencije i zaštite u bežičnim senzorskim mrežama s primenom u preciznoj poljoprivredi, *19th International Symposium INFOTEH-JAHORINA*, Mart 2020 (M33).

Дисертација је писана у складу са стандардном методологијом писања научних радова. Састоји се из осам основних целина: увода, технологија интернет ствари, бежичне сензорске мреже, процена оптималне комбинације протокола топологије и шифарског алгоритма, симулација и студија случаја, анализа резултата истраживања и на крају су дата закључна разматрања. Докторска дисертација има 133 страна, док списак референтне литературе има 89 наслова. Рад је прегледно написан, технички добро обрађен и организован, уз јасан садржај и пагинацију, индекс слика и табела.

Предмет

Предмет истраживања докторске дисертације су принципи безбедности бежичних рачунарских мрежа са становишта примене протокола и шифарских алгоритама. У дисертацији је предложен механизам за избор оптималног решења које задовољава задати ниво сигурности уз оптималну потрошњу енергије.

Научни допринос дисертације огледа се, пре свега, у математичком моделу процене потрошње енергије бежичних сензорских мрежа за задати скуп протокола топологије и криптографских алгоритама мале рачунске и имплементационе захтевности. Предложена метода процене потрошње енергије анализирана је кроз симулациони сценарио за четири протокола за конструкцију топологије и девет криптографских алгоритама. Модел је тестиран у симулационом окружењу где се бежичне сензорске мреже примењују као технологија за комуникацију на отвореном подручју између сензорских чворова и уређаја заснованих на технологији интернета ствари. Поред математичког модела представљена је и његова алгоритамска имплементација, која је коришћена за надоградњу симулационог окружења *Atarraya*. Анализом резултата симулације потврђена је тачност математчког модела за прорачун коефицијента подобности протокола топологије и шифарског алгоритма. На основу дефинисаног модела и резултата симулације представљена је сортирана листа коефицијената подобности комбинације протокола топологије и алгоритма шифровања. Поред наведених резултата до којих се дошло током израде тезе битно је истаћи и једноставност математичког модела чија имплентација није захтевна.

Резултати истраживања поред оптималног избора протокола топологије и шифарског алгоритма приказују и најоптималнија решења за најучесталије нападе на БСМ, боље разумевање постојећих проблема у области безбедности са аспекта енергетске ефикасности, као и проналажење ефикасних смерница за даљи развој система заснованих на БСМ.

Дисертација је организована у осам поглавља: (1) увод, (2) технологија интернет ствари, (3) бежичне сензорске мреже, (4) лагани шифарски алгоритми, (5) процена оптималне комбинације протокла топологије и шифарског алгоритма, (6) симулација и студија случаја, (7) анализа резултата истраживања и (8) закључак.

У уводном поглављу изложена је иницијална мотивација за израду дисертације и дат преглед основних појмова и аспеката којима се приступало приликом истраживања. Детаљно су размотрени циљ истраживања и основни алати и смернице који су том приликом коришћени.

Наредна три поглавља дата су са циљем да олакшају разумевање представљеног модела за процену оптималне комбинације протокла топологије и шифарског алгоритма.

У другом поглављу представљена је технологија интернет ствари. Направљен је сажети преглед технологије интернет ствари, представљена је структура паметних уређаја, њихова основна намена, изазови и проблеми са којима се сређемо, као и карактеристична подручја примене ове технологије.

У трећем поглављу изложена је технологија бежичних сензорских мреже као и слојеви њихове типичне архитектуре. Поред архитектуре представљени су и проблеми безбедности са којима се суочавамо, типични напади и механизми одбране. Поред наведеног приказани су протоколи топологија чије је разумевање од суштинског значаја за даље разумевање дисертације.

У четвртом поглављу приказани су шифарски алгоритми који нису рачунски захтевни, лагани шифарски алгоритми, од којих су издвојени: напредни стандард енкрипције, *NOEKEON*, *Present*, *LED*, *Piccolo*, *TWINE*, *KATAN* и *KTANTAN*, *Prince* и *Simon*. Карактеристике наведених шифарских алгоритама су један од улазних параметара за математички модел за одлучивање.

Пето поглавље садржи главне резултате и доприносе дисертације. У петом поглављу представљен је нови математички модел за одређивање коефицијента подобности комбинације шифарског алгоритма и протокола топологије описаних у претходна два поглавља. Овај модел представља главни научни допринос тезе. Поред модела дата је његова алгоритамска имплементација.

У шестом поглављу описано је симулационо окружење као и симулациони сценарио Математички модел је тестирани у симулатору за сваки пар протокола топологије и шифарског алгоритма. Дат је преглед резултата тестирања предложеног модела за оцену подобности.

У седмом поглављу изложени су преглед изведених закључака и кратка анализа резултата који потврђују научни допринос тезе.

Поред овога, у осмом поглављу представљене су смернице и препоруке које би биле од значаја за будућност ове области у циљу даљег развоја алгоритама и математичког модела за одређивање коефицијената подобности. .

ОЦЕНА ДИСЕРТАЦИЈЕ

Предложени математички модел за одређивање коефицијента подобности као и одређивање интервала прихватљивости коефицијената изложен у дисертацији представља нови приступ овом типу анализе. Доказ квалитета предложеног модела огледа се у великом броју симулација и параметара архитектуре система бежичних сензорских мрежа и шифарских алгоритама тестираних у раду. Поред изложеног модела у раду је креиран рачунарски код, који је једноставан за имплементацију и извршавање. Научно захтеван проблем оцене избора протокола топологије и шифарског алгоритма целовито је истражен са теоријског и практичног становништва. Рад се одликује квалитетним закључивањем, а писан је једноставним и јасним стилом.

У изради ове дисертације коришћено је 89 библиографских јединица. У попису литературе коришћене су домаће и иностране књиге, монографије, научни и стручни радови мањег обима као и интернет извори. Међу њима се налази и литература новијег датума, тј. са најновијим сазнањима из области истраживања. Обимна библиографија је извесно допринела квалитету рада. Технике коришћене за израду овог рада су популарни алати и адекватни су за примену у предметним истраживањима.

Докторска дисертација има јасан научни допринос у форми новог модела за оцену подобности шифарских алгоритама и протокола топологија. Предложени метод који укључује више различитих технологија користи се да би се процес оцене целовито сагледао и да би се приступило решавању проблема укључивањем великог броја аспеката који су од суштинске важности за све технологије које као за комуникацију користе технологију засновану на бежичним сензорским мрежама. Главни резултати дисертације објављени су у међународним часописима са рецензијом, и на међународној конференцији, чиме је научни допринос верификован од стране ширег аудиторијума. Поред тога, сматрамо да је домаћа научноистраживачка јавност добила допринос новог смера истраживања у области интернета ствари и бежичних сензорских мрежа.

Београд, 29. 12. 2020.

Чланови комисије:

Доц. др Селена Вукотић

Проф. др Дејан Драјић

Проф. др Ђорђе Бабић