Merima Malkočević, dipl. ing. el. - Magistarski rad

Fakultet/Akademija	FAKULTET ELEKTROTEHNIKE
Tip Rada	Magistarski rad
Kandidat, zvanje	Merima Malkočević, dipl. ing. el.
Naziv Teme	Enkripcija na podatkovnom sloju telekomunikacijskog sistema po distributivnim energetskim vodovima
Rezime/Abstract	Problem sigurne komunikacije poznat je kroz cijelu istoriju čovječanstva. Osnovna ideja sigurne komunikacije je prenijeti poruku s jednog mjesta na drugo što je moguće sigurnije, tj. osmisliti algoritam koji bi orginalnu poruku učinio nerazumljivom neovlaštenim osobama koje bi došle u njen posjed. Nauka koja se bavi metodama očuvanja tajnosti informacija naziva se kriptografija. Kriptografija i njena primjena u PLC sistemima osnovni su sadržaj ovog rada. Prva dva poglavlja obrađuju osnove PLC sistema, pri čemu su u prvom poglavlju predstavljene osnovne karakteristike, struktura i realizacija PLC mreže, dok je drugo poglavlje bazirano na PLC MAC podsloju. Osim osnovnih osobina MAC podsloja, u ovom poglavlju, predstavljeni su i koncepti višestrukog pristupa, dijeljenja resursa i kontrole pristupa. Razvoj simetrične kriptografije i njeni najznačajniji algoritmi predstavljeni su u trećem poglavlju. Naravno, u prvom planu je AES kriptografski algoritam koji se primjenjuje u PLC sistemima. Simetrična kriptografija ili kriptografija tajnog ključa je forma kriptografije, kod koje se jedan ključ koristi i za kriptovanje i za dekriptovanje poruke. Kod ove vrste kriptografije najveći je problem u sigurnoj distribuciji ključeva, tj. kako dostaviti tajni ključ primaocu na siguran način. Upravo, problem distibucije ključeva i uspostavljanje sigurne veze u PLC sistemima obrađen je u četvrtom poglavlju. U ovom poglavlju dat je kratak pregled IEEE 1901 standarda i opisane su metode enkripcije definisane ovim standardom. U AES algoritmu do sada nisu pronađene nesigurni ili potencijalno nesigurni ključevi koji bi mogli narušiti sigurnost. Koristeći CrypTool software, u petom poglavlju izvršena je simulacija AES algoritma, kao i simulacija "brute force" napada kroz analizu kriptograma i u slučaju kada je poznat dio otvorenog teksta. U ovom poglavlju takođe su predstavljeni i sigurnosni problemi komunikacije po distributivnim energetskim vodovima.
Datum	28.02.2013
Predsjednik	Dr sc. Nermin Suljanović, vanredni profesor - predsjednik, Uža naučna oblast "Komunikacije" Fakultet elektrotehnike Univerziteta u Tuzli
Mentor	Dr sc. Aljo Mujčić, vanredni profesor – mentor i član, Uža naučna oblast „Komunikacije“ Fakultet elektrotehnike Univerziteta u Tuzli
Član komisije	Dr sc. Suad Kasapović, vanredni profesor - član, Uža naučna oblast "Komunikacije" Fakultet elektrotehnike Univerziteta u Tuzli
Član komisije	-
Član komisije	-
Zamjenski član	-
Dodatni detalji i lokacija	28. 02. 2013. godine u 16,oo sati na Steleksu Fakulteta elektrotehnike Univerziteta u Tuzli
Zavrsne Odredbe	Magistarski rad može se pogledati u Sekretarijatu Fakulteta, radnim danom od 10,oo do 14,oo sati. Pristup javnosti je slobodan