

Dear Dr Rupp

I graduated from Sharif University of Technology, Tehran, Iran. I have defended my Master of Science thesis entitled “Security evaluation of public key based key management in MANET” under supervision of Mr. Mohajeri (Sharif University of Technology). My Thesis is included a survey of symmetric key based, public key based and ID-based key management for MANETs.

I have published a paper entitled “A certificate-less public key based key management with clustering for MANETs” to 9th International ISC Conference on Information Security and Cryptology (ISCISC), 2012 , (Farsi version). We used certificate-less public key cryptography to solve key screw in ID-based cryptography. It also doesn't need to exchange certificates. The proposed scheme employs clustering to decrease communication overhead and improve scalability and key revocation and omits cluster-heads for communication. We simulated our scheme and compared it with three other related schemes. I am recently studying on Privacy enhancing, E-voting & Mix Net, secret handshaking, IoT, Cloud and Industrial Control System (ICS) security.

I have also done various studies in the area of network security in my master studies and I am widely interested in its various challenges hence I find your open position suitable. I have also attached my CV, SoP, BSc and MSc transcripts to this email and will greatly appreciate it if you take the time to review my case. Please kindly let me know if I am a suitable PhD student in your research group.