RESEARCH AND DEVELOPMENT

Name of the Researcher	Department	Research Topic	Date of Completion
Dr. Z.J. Khan Dr. S.G. Akojwar Ms. Alka Sawlikar	Department of Electronics Engineering	Parametric Evaluation of Cryptographic Techniques for Enhancement of Energy Efficiency in Wireless Communication Network	**Ongoing**

BRIEF SUMMARY OF THE WORK: This work is basically pursuing as a part of Doctoral work at R.C.E.R.T.Chandrapur. This research, introduces a new compression and encryption algorithm, which is based on bit quantization, chaos and multistage missing value concept and is the robust technique which requires less encoding and decoding time and is energy efficient. We focus on the energy efficiency of secure communication in wireless sensor networks (WSNs). Our research considers link layer security of WSNs, investigating both the ciphers and the cryptographic implementation schemes, including aspects such as the cipher mode of operation and the establishment of initialization vectors. We evaluate the computational energy efficiency of different symmetric key ciphers considering both the algorithm characteristics and the effect of channel quality on cipher synchronization. Results show that the computational energy cost of block ciphers is less than that of stream ciphers when data is encrypted and transmitted through a noisy channel. We further investigate different factors affecting the communication energy cost of link layer cryptographic schemes, such as the size of payload, the mode of operation applied to a cipher, the distribution of the initialization vector, and the quality of the communication channel. Hardware implementation has been done for small distance communication using Bluetooth, keypad matrix, microcontroller and display device. At the end the best cryptographic combination is transferred wirelessly and found parameters which are energy efficient. The best combination for encryption and compression of the data transmission, energy optimization is found out and implemented in NS2 for finding different parameters like delay, energy and throughput through secure protocol.

RELEVANCE: In the present-day, beyond the obvious need to keep military orders secret, government-sponsored cyber-war means cryptography is a national security concern. The goal of all of this research is that one day, it will be possible to ensure security of important information wherever it might be — on our computers, mobile devices, and even in the cloud. This work can guide software designers or hardware manufacturers to reconstruct a power-effective security system. Businesses will respond faster to increase in computing power. If the algorithms described in this work implemented on audio and video then everybody came to know how important to keep our particulars safe not only with key but with lock also. Improving existing algorithms and timely changing codes in different modes always help human beings to feel safe from hackers.

RESEARCH OUTCOMES : Three Paper in Journals and two papers in Proceedings of International Conferences have been published on this work.