

SCCE: SECURE COMMUNICATION BASED ON A CHAOTIC SYSTEM FOR MODERN WIRELESS COMMUNICATION

P. KARTHIK¹, P. S. RANJITH² & M. JAYAGANESH³

¹Assistant Professor, Department of Electronics and Communication Engineering, SNS College of Engineering,
Coimbatore, Tamil Nadu, India

^{2,3}Under Graduate Scholar, Department of Electronics and Communication Engineering, Anna University,
SNS College of Engineering, Coimbatore, Tamil Nadu, India

ABSTRACT

Wireless communication networks use interconnected devices within a relatively small area that is generally within a person's reach. The term Wireless network is defined as a network, which is of any type and uses some form of wireless network connection and hence more susceptible to malevolent attacks. The present system is encrypted based on algorithms and certain proposed standards which detects and restricts the high malevolent behaviour detection rates in certain circumstances, which does not greatly affect the network performances by using a digital signature algorithm, S-ACK (secure acknowledgment). However the wide usage of algorithms and proposed standards are published and the methodologies are exposed to the world's view. In an instance it allows the hackers to intrude any type of communication systems and made them vulnerable to attacks. Hence, by adopting the different methodologies rather than the existing methodologies enhances the security. The suggested system is to overcome the drawbacks of existing encryption methodologies such as DES, RSA by enhancing the security of the data by the chaotic encryption method. This method involves the use of commutative codes and above algorithms to reassure the security of the transmitted data. By adopting the above technique the data transmission and reception is highly secure than existing methods.

KEYWORDS: Wireless Communication Networks, Digital Signature Algorithm, Malevolent Behaviour, DES, RSA, Chaotic Encryption Method