CHAPTER VI

Complex Engineering Problems

MANETs are important for talking in places where regular networks can't reach. They help devices connect without needing a main system, which is great for things like disaster help, military missions, and vehicles talking to each other. The decentralized nature of MANETs and the absence of a fixed infrastructure create numerous security challenges, leaving them vulnerable to various types of attacks. Among the most harmful threats are wormhole and blackhole attacks, which can significantly disrupt communication, compromise data integrity, and weaken network reliability.

6.1 Complex Engineering Problems Associated with The Thesis

Developing a cryptographic algorithm poses various engineering challenges to ensure adequate security with better efficiency and user experience. The problems are stated below at Table 6.1.

Table 6.1: Range of complex engineering problems

Attributes	Problems
Depth of knowledge required	Addressing data security concerns necessitates a thorough understanding of Cryptography, including its core mathematical principles and theories. Proficiency in statistics is also essential for evaluating the scheme effectively. Additionally, the implementation of the scheme requires proficient programming skills.
Range of conflicting requirements	Balancing efficiency and security posses a significant challenge for cryptographic algorithms. When prioritizing security, efficiency tends to decrease. Conversely, achieving high efficiency often comes at the expense of compromised security.
Depth of analysis required	Extensive research and analysis have been conducted to devise methods for ensuring the efficiency and security of the algorithm. This involved examining, comprehending, and evaluating the methodologies, outcomes, and effectiveness of existing schemes. Ultimately, a viable approach for improving performance was identified.

Familiarity of issues	Mobile Network is very famous research field but it is very complex to deal with the problems. Many research on the mobile nodes and security was done. But a lot of modification and analysis is required to make it more secure and also reliable.
Extent of applicable codes	The algorithm is designed applying AES cryptosystem.