**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** | **Addressing the Attributes of Complex Engineering Problems** | |
| Depth of knowledge required | P1 | 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 | P2 | 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 | P3 | 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 | P4 | 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 | P5 | The algorithm is designed applying AES cryptosystem. |

**6.1**  **Complex Engineering Activities Associated with The Thesis**

Selecting an optimal secret key size to achieve desired security levels and generating new random secret keys for each message transmission. Designing key generation, encryption, and decryption algorithms to operate with θ(n) time complexity. The engineering tasks outlined for this thesis are detailed in Table 6.2.

Table 6.2: Range of complex engineering problems

|  |  |  |
| --- | --- | --- |
| **Attributes** | **Addressing the Attributes of Complex Engineering**  **Activities** | |
| Range of resources | A1 | Designing the proposed encryption algorithm involves utilizing computational power (hardware resources) for testing and optimization, with programming tools and platforms (software resources) for implementing and validating the algorithm. |
| Level of interaction | A2 | Creating the proposed encryption algorithm requires substantial collaboration among cryptographers, government entities, industries, open-source communities, end users, and developers. Continuous interaction, feedback, and peer reviews are essential to establish a resilient and efficient solution. |
| Innovation | A3 | To make the encryption algorithm efficient a recursive function used which is built based on Fermat’s Little theorem. |