

**ENHANCED MOVING TARGET DEFENSE MECHANISMS TO
HANDLE CYBER ATTACKS**

CHAPTER 3

PROPOSED METHODOLOGY

3.1. Research Design

3.2. Contributions in each phase

3.3. Chapter Summary

3.1. Research Design

The proposed research work aims at increasing the accuracy level in monitoring, detecting and preventing data or information from cyber attacks. One of the main significance of this research work is to ensure security for the wireless local area network. The major steps involved in the research design are shown in figure. 3.1

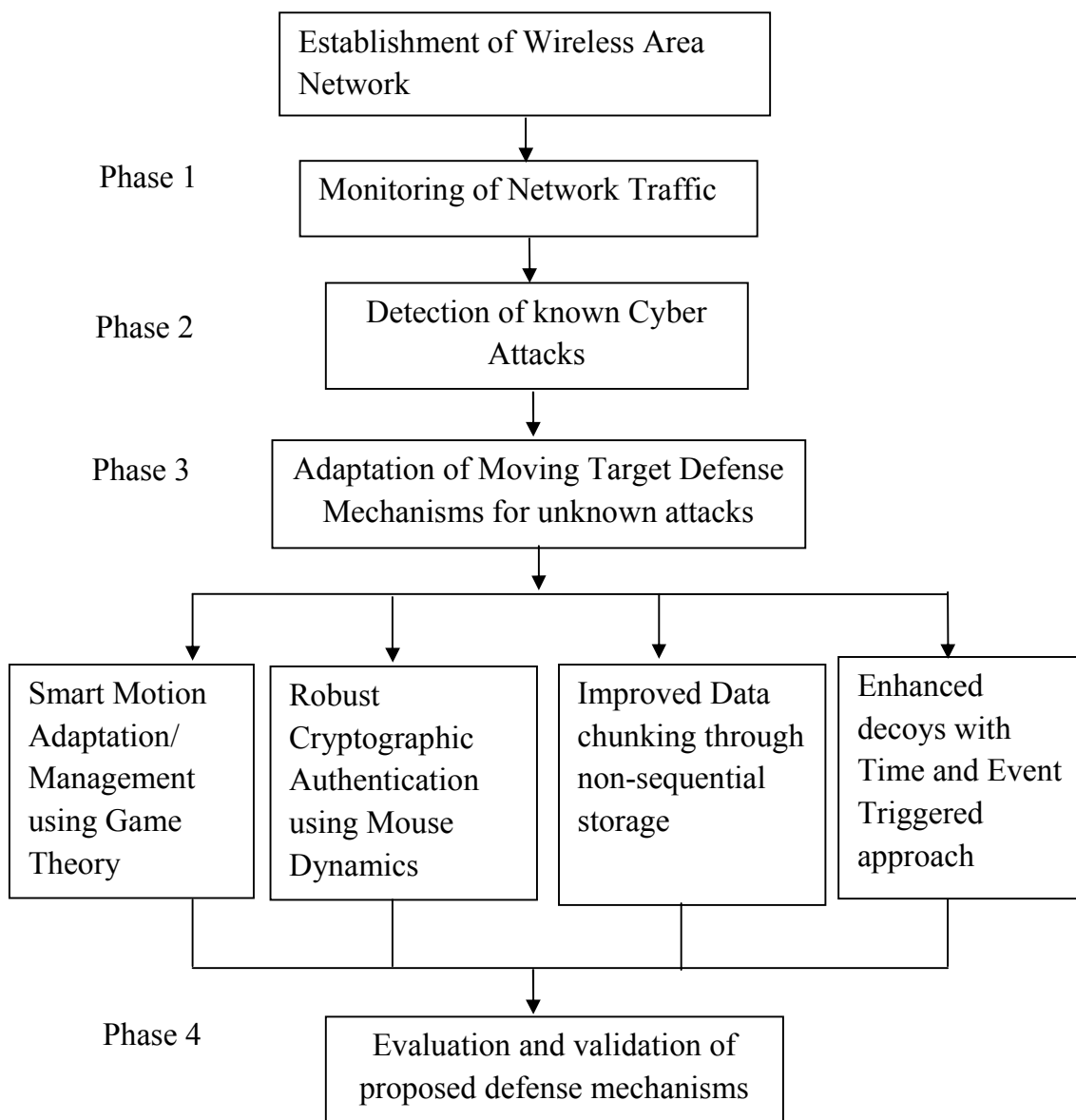


Figure.3.1. Outline of the Research Design

The consolidated view of the proposed methods with techniques applied and outcomes are given in figure.3.2.

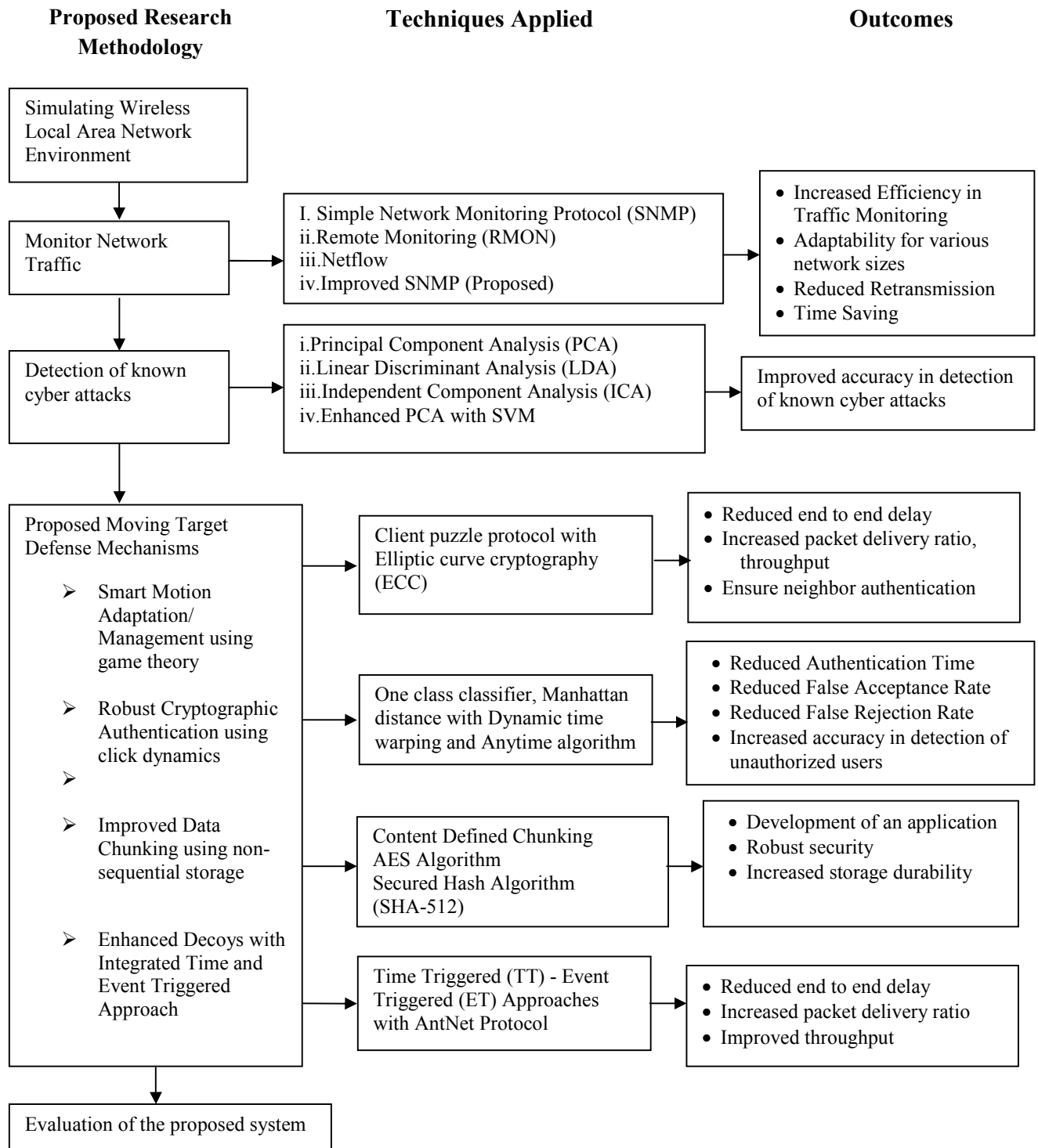


Figure.3.2. Consolidated view of the Proposed Methodology

To meet the objectives of the thesis, a methodology is devised based on the following techniques.

- i. Improved Network Traffic Monitoring Technique
- ii. Enhanced Dimensionality Reduction Technique
- iii. Smart Motion Adaptation/Management using Game Theory
- iv. Robust Cryptographic Authentication using Mouse Dynamics
- v. Improved Data Chunking through Non-Sequential Storage
- vi. Enhanced Decoys with Integrated Time and Event Triggered Approach

A wireless LAN (WLAN) is initially set up using network simulator.

Step – 1: Network Traffic Monitoring

The traffic through the WLAN is monitored using the following methods:

- i. Simple Network Monitoring Protocol (SNMP)
- ii. Remote Monitoring (RMON)
- iii. Netflow
- iv. Improved SNMP (Proposed)

Step – 2: Detection of known Cyber attacks

The detection of known cyber attacks is done using dimensionality reduction techniques. They are

- i. Principal Component Analysis (PCA)
- ii. Linear Discriminant Analysis (LDA)
- iii. Independent Component Analysis (ICA)
- iv. Enhanced Principal Component Analysis

Step – 3: Proposed Moving Target Defense Mechanisms

The moving target defense mechanisms are implemented and they are

- i. Improved Data chunking through non-sequential storage
- ii. Enhanced Decoys with Integrated Time and Event Triggered approach

- iii. Robust Cryptographic Authentication using Click Dynamics
- iv. Smart Motion Adaptation/Management using Game Theory

Step - 4: Evaluation of the Proposed Methods

The proposed methods are evaluated based on the accuracy in detecting the cyber attacks.

3.2. Contributions in each phase

The above discussed moving target defense mechanisms are enhanced to achieve the objectives of the thesis. The conceptual view of the Improved Moving Target Defense Mechanisms is shown in figure.3.3.

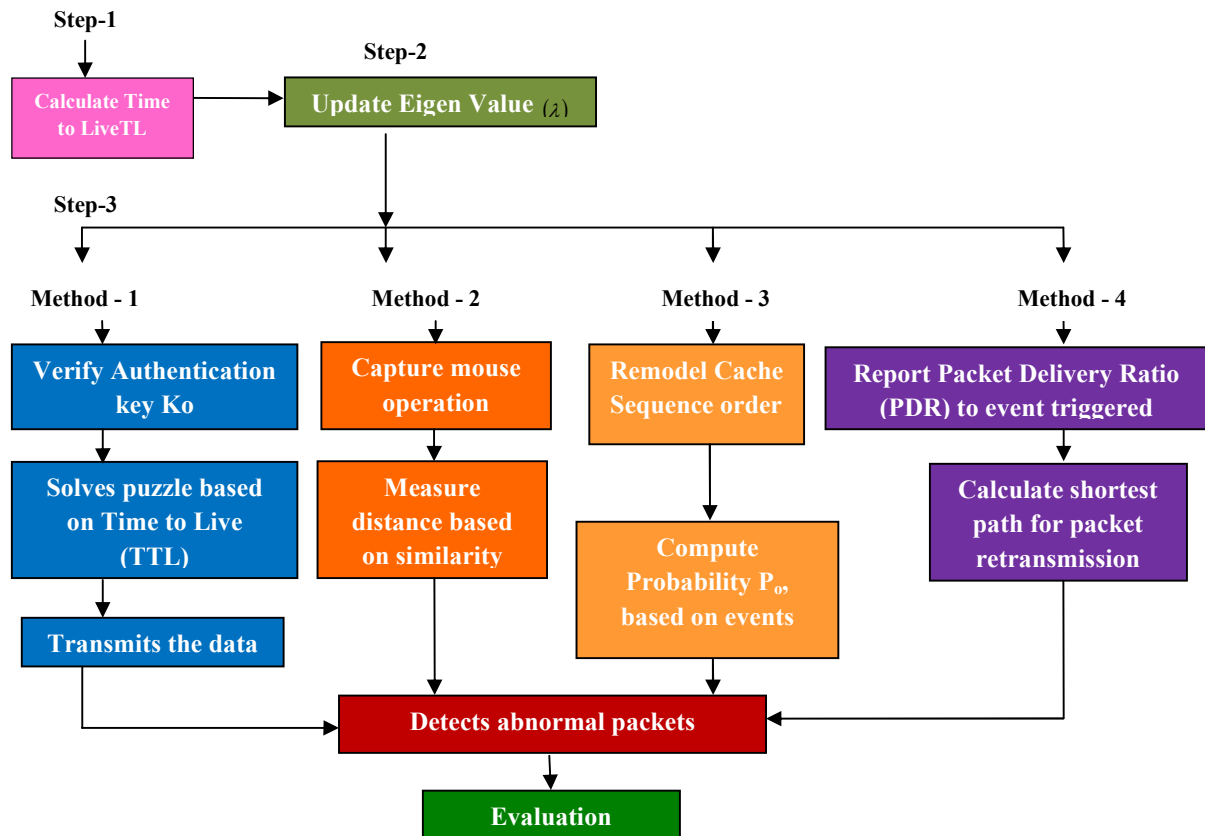


Figure3.3. Conceptual view of the Improved Moving Target Defense Mechanisms

3.3. Chapter Summary

This chapter discusses the various phases of the research design. The consolidated view of the proposed methodology with techniques applied and outcomes are discussed in this section. The proposed methodology consists of six steps. In Step, network traffic monitoring technique is enhanced with an added feature and evaluated with Quality of Service (QoS) parameters. In the second step, enhance linear dimensionality reduction techniques is used to detect the known cyber attacks and accuracy is improved. In the next step, four moving target defense mechanism is implemented and improvement is done. The four moving target defense mechanisms are evaluated for efficiency in detecting the unknown cyber attacks.

In the next coming chapters demonstrate all the four steps of the research designs and its consequences are discussed in detail.