1. **Hypothesis and Methodology.**

The term authentication describes the process of verifying user identification based on something the user knows, something the user has, something the user is or something the user does. By analyzing recent trends in Self Propagating Codes, we need to get ready for Self Propagating Codes with a variety of destructive characteristics including multi-platform, multi-exploit, zero-payload, fast spreading, polymorphic, metamorphic, truly nasty Self Propagating Codes. The detection of Self Propagating Codes transmitted over mobile networks has been researched intensively in recent years. One type of abundant Self Propagating Codes is worms, which proactively propagate across networks while exploiting vulnerabilities in operating systems or in installed programs. Other types of malcode include computer viruses, Trojan horses, spyware, and adware. In this thesis we focus on Polymorphic and Metamorphic Self Propagating Codes.

We defined are research questions accordingly:

Q1: In the detection of known Self Propagating Codes, based on a computer's measurements, using Artificial Neural Network techniques, what is the achievable level of accuracy?

Q2: Is it possible to reduce the amount of false-positive features to known benchmark, while maintaining a high level of accuracy (compared to the full set of features). Which feature consolidation approach (unified versus averaged) and feature selection method is superior?

Q3: How can we have effective and reliable authentication process implemented?

Q4: Will the mobile platform configuration and the mobile computing activity, from which the training sets are taken, have a significant influence on the detection accuracy?

Q5: Is the detection of fraudulence transaction by unknown Self Propagating Codes possible, based on a training set of known Self Propagating Codes?

2. **Scope of Study.**

Fraud correlation is an important technique for managing of different pattern of malicious packets that are raised by heterogeneous Multi Agent Systems (MAS). The recent trend of research in this area is towards extracting attack strategies from Self Propagating Codes (SPC). It is generally believed that pure Multi Agent Systems no longer can satisfy the security need of organizations. Attack response and prevention are now becoming crucially important for protecting the network and minimizing damage. Knowing the real security situation of a network and the strategies used by the fraudsters enables Network and Security
Operations to launch appropriate response to stop online fraud and prevent them from escalating. Some techniques for extracting fraud strategies have been proposed in recent years, but they normally require defining a larger number of rules.

This research focuses on developing a Fraud Packets Correlation Technique (FPCT) that can help to automatically extract fraud strategies, without specific knowledge about unknown attack packets. The proposed approach is based on two different neural network approaches, namely, Supervised Learning and Un-supervised Learning. The probabilistic output of these two methods issued to determine with which previous attack packets, these current attack packets should be correlated. This suggests the causal relationship of attack packets, which is helpful for constructing fraud scenarios. One of the distinguishing features of the proposed technique is that a Fraud Packets Correlation Matrix (FPCM) is used to store correlation strengths of any types of attack packets. FPCM is updated in the training process, and the information (correlation strength) is then used for extracting high level attack strategies.

3. Utility of the Study.

The defeat of two-factor authentication that uses physical devices is a significant breakthrough for the fraudsters. Financial institutions must take the risk seriously, especially considering that the technique used can be expanded for other forms of physical security devices. Artificial Neural Networks are widely used in many fields. One of the applications of Artificial Neural Networks in the field of the information security is classification of raw packets into malicious and benign. Detecting unknown Self Propagating Codes is a challenging task. Extant solutions, such as anti-virus tools, rely mainly on prior explicit knowledge of specific Self Propagating Codes signatures. Anti viruses consisting on signature-based methods are helpless against new (unknown) Self Propagating Codes. As a result, after the appearance of a new Self Propagating Code on the Web there is a significant delay until an update carrying the Self Propagating Code’s signature is distributed to anti-virus tools. During this time interval a new Self Propagating Codes can infect many computers and cause significant damage. This thesis propose an innovative technique for detecting and analyzing the presence of an unknown Self Propagating Codes, not necessarily by recognizing specific instances of the Self Propagating Codes, but rather based on the computer measurements. This thesis focuses on the feasibility of accurately detecting unknown Self Propagating Codes activity in individual computers and networks while minimizing the required set of features collected from the monitored network equipments.

4. Time Schedule.
Phase I
- Implement and evaluate the proposed authentication frameworks and the algorithms using different real-world datasets.

Phase II
- Profiling the Self Propagating Codes behavior to capture the static or dynamic events.

Phase III
- Examining and recording each of those activities from mobile devices.
- Creating statistics based on all applicable findings.

Phase IV
- Generating new functional or non-functional design requirements for securing Mobile Computing infrastructure.