# Chapter 6
# Dynamic Intelligence-Driven Engineering Flooding Attack Prediction Using Ensemble Learning

**R. Angeline**
*SRM Institute of Science and Technology, Ramapuram, India*

**S. Aarthi**
*SRM Institute of Science and Technology, Ramapuram, India*

**R. Regin**
*SRM Institute of Science and Technology, Ramapuram, India*

**S. Suman Rajest**
https://orcid.org/0000-0001-8315-3747
*Dhaanish Ahmed College of Engineering, India*

## ABSTRACT

*The rapid evolution of the Internet and communication technologies has fueled the proliferation of wireless sensor network (WSN) technology, which is increasingly important in today's interconnected world. For a broad variety of industries and applications, an enormous number of sensing devices continuously create and/or gather copious amounts of sensory data. However, it has been shown that WSN is susceptible to security flaws. These networks' abrasive and unmanaged deployment, along with their limited resources and the amount of data produced, raise serious security issues. The development of trustworthy solutions that include quick and continuous processes for live data stream analysis allowing the identification of flooding assaults is crucial since WSN applications are of the utmost importance. To put it in plain words: The assault is carried out by repeatedly sending pointless requests to the target computer in an effort to overwhelm it, cause the systems to fail, and prevent people from accessing the network or machine.*

DOI: 10.4018/979-8-3693-1301-5.ch006

## 1. INTRODUCTION

The field of cybersecurity is of paramount importance in today's digital world, where malicious attacks on computer networks and systems can cause significant damage to individuals and organizations (Taherkhani & Pierre, 2015). One such attack is the flooding attack, which floods a network or system with a large volume of traffic, causing it to crash or become unresponsive (Greff et al., 2017). To address this problem, researchers have developed various techniques for detecting and preventing flooding attacks (Józefowicz et al., 2015). In this chapter, we propose a novel approach to predicting flooding attacks using ensemble learning, which is a machine learning technique that combines the outputs of multiple models to improve prediction accuracy (Sun et al., 2020). Our proposed approach, called Dynamic Intelligent Driven Engineering Flooding Attack Prediction (DIDE-FAP), is based on a dynamic feature selection and intelligent feature engineering process that improves the performance of the machine learning models used for prediction. also use several popular machine learning algorithms, including K-Nearest Neighbor (KNN), Random Forest (RF), Decision Tree (DT), and Support Vector Machine (SVM), to predict the flooding attacks with high accuracy (Rashi & Madamala, 2022).

The proposed dynamic intelligent-driven engineering flood attack prediction the ensemble learning approach leverages the power of ensemble learning and incorporates dynamic feature selection and intelligent feature engineering to enhance the accuracy of the prediction models (Tiwari, et al., 2018). To prevent flooding attacks, it is important to develop effective prediction models that can identify and respond to potential attacks before they occur (Sinha et al., 2021). This is where machine learning techniques, such as ensemble learning, can play a vital role (Singh et al., 2022). Ensemble learning involves combining multiple models to improve the accuracy and robustness of predictions, making it a promising approach for predicting flooding attacks (Surve et al., 2022). This approach involves developing dynamic and intelligent models that can adapt to changes in network traffic and improve their accuracy over time.

By using ensemble learning to predict flooding attacks, organisations can better protect their networks and prevent the disruption and financial losses that can result from such attacks (Pandit, 2023). This chapter makes a significant contribution to the field of cybersecurity by proposing an effective approach for predicting flooding attacks. Our proposed approach can be used by security analysts and network administrators to improve the security of their systems by detecting and preventing flooding attacks before they occur. Predicting how much traffic will increase or decrease is a big challenge for today's transportation networks (Sepasgozar & Pierre, 2022). It might help with traffic reduction, better route planning, and better route selection. Predicting when and where traffic congestion will occur is one approach to managing transportation (Wu et al., 2018).

Network traffic would grow if there were more cars on the road, since more cars would mean more packets being sent. In the literature study, we looked at previous studies that separately examined network traffic and traffic on the roads (UmaMaheswaran, et al., 2022). Most of these studies addressed either road or network congestion individually; this one seeks to bridge that gap by analysing the correlation between these two types of traffic measurements. Intelligent approaches employing machine learning (ML) methods are the best solutions to handle traffic prediction problems with the aim of anticipating traffic flow. Bayesian modelling, fuzzy logic, hybrid modelling, neural networks (NN), and statistical modelling are only a few of the available computer methodologies. Most of these techniques, and NN in particular, have the potential to improve prediction accuracy in data flow (Yang, et al., 2017).

The accuracy of prediction is a key factor in all of these considerations. Three categories of ML approaches are distinguished: Unsupervised learning (in which training is based on unlabeled data),