**INDIAN INSTITUTE OF TECHNOLOGY GUWAHATI**
**SHORT ABSTRACT OF THESIS**

| | | |
|---|---|---|
| Name of the Student | : | BASANT SUBBA |
| Roll Number | : | 126101003 |
| Programme of Study | : | PhD |

Thesis Title: On improving the efficiency of intrusion detection systems using game theoretic approaches

| | | |
|---|---|---|
| Name of Thesis Supervisor(s) | : | Dr. Sushanta karmakar & Dr. Santosh Biswas |
| Thesis Submitted to the Department/ Center | : | Computer Science & Engineering |
| Date of completion of Thesis Viva-Voce Exam | : | 28th June 2018 |
| Key words for description of Thesis Work | : | Game Theory, Intrusion Detection Systems, Network Security |

**SHORT ABSTRACT**

The thesis consists of three distinct contributions. As the first contribution, a novel game theory-based false alarm minimization scheme for signature based IDS is proposed. The proposed framework models the intrusion detection process as a two player non-cooperative game between the IDS and the attacker. It uses various network context information like, IDS's detection rate, criticality levels of the host machines, severity levels of network vulnerabilities, attacking and monitoring costs etc., to devise efficient IDS monitoring strategies
based on the Nash Equilibrium (NE) of the game. The proposed framework is shown to filter out most of the false positive alarms generated by the signature based IDS and thereby, significantly improve the IDS's accuracy, without adversely affecting its detection capabilities.

The second contribution of the thesis proposes a Bayesian game theory-based hybrid intrusion detection framework for resource constrained Mobile Ad-hoc Networks (MANETs). It uses a combination of simple threshold based rules and complex data mining based

association rules to detect various type of attacks in MANETs. In addition, the proposed
intrusion detection framework models the interaction between the IDS and the node being monitored as a two player non-cooperative Bayesian game. Such non-cooperative game theoretic modeling enables the MANET nodes operating the IDS to minimize their overall energy consumption by adopting probabilistic monitoring strategies based on the Bayesian Nash Equilibrium (BNE) of the game, without adversely affecting their detection rate. The framework is also shown to significantly reduce the volume of IDS traffic introduced into the network.

As the final contribution of the thesis, a novel clustering algorithm and a game theory-based multi-layered intrusion detection framework for Vehicular Ad-hoc Networks (VANETs) are proposed. High vehicular mobility of VANETs results in unstable vehicular clusters with intermittent network connectivity among vehicles. Therefore, introduction of high volume of intrusion detection related traffic can cause congestion in VANETs. The proposed clustering algorithm uses various vehicular information like vehicles' velocities, their direction of movements, real-time coordinates etc., to produce stable vehicular clusters, which enhances the overall stability of the vehicular network. The proposed IDS framework uses a combination of specification rules and a neural network based classifier module to detect various type of attacks in VANETs. Additionally, the proposed IDS framework models the intrusion detection process in VANET as a two player non-cooperative game between the IDS and the vehicle being monitored. This enables the IDS to devise efficient monitoring strategy based on the Nash Equilibrium of the game and thereby, significantly reduce the volume of IDS traffic in the vehicular networks.