CHAPTER 1 : INTRODUCTION

1.1 Background

Vehicular Ad-Hoc Network or VANET, which is a subclass of Mobile Ad Hoc Network (MANET) is an on-demand network of vehicles that holds the features such as self organization, auto configuration, and self healing. VANET topology can be varies and it is depends on the traffic condition from very dense (e.g. traffic jams, rush hour, etc.) to very sparse (e.g. late night, rural area etc.). In the condition of a dense network topologies, it is very easy to provide an end-to-end multi-hop communication between the sources and the destinations between the vehicles, it is because the presence of vehicles along the path during the communication between vehicles. Meanwhile, similar communications performance between the vehicles could not be achieved in sparse network condition because of the intermittent nature of intermediate links due to limited number of vehicles along the path.

In VANET, each of vehicle is equipped with short range radios and computing resources, it can be able to communicate with the infrastructure (V2I) or other nearby vehicles (V2V). However, due to the high movement of vehicles, the connectivity in VANET is highly unstable and links may change or break soon after they have been established.

The communications between vehicles in VANET are achieved by using the Store-Carry-and-Forward (SCF) communication mechanism which is the foundation of Delay Tolerant Network (DTN). This type of vehicular network paradigm is called Vehicular Delay Tolerant Network (VDTN). In a simple way, a packet will be sent over the existing link and buffered at the next hop until a connection to a suitable next hop is established. The idea behind SCF is very simple, the message (bundle) will be stored in the buffer of an intermediate or each node/vehicle when the next hop is not available, until it finds the opportunity to forwarding the packets to another node/vehicle.

The SCF mechanism process will continues until the bundle reaches the destination or its Time To Live (TTL) has expired and the message will be dropped. In the VDTN network the message are not only stored in each node/vehicle but it is also replicated by multiple other nodes/vehicles before reaching the destination. In real world implementation, several VDTN projects are using cars, buses, trucks, motorcycles or even bicycles.

Because of vehicle density (sparse and dense) and also the traffic variations, highly dynamic topology, short contact durations, limited transmission ranges, radio obstacles, and interferences, VDTN are prone to intermittent connectivity, and significant loss rates. As the consequences, routing in vehicular networks presents a particularly challenging problem due to the unique characteristics of the networks.

Typically VDTN assume cooperation and no malicious behavior from participating vehicular nodes. However, vehicles are individual entities that can make independent decisions regarding the forwarding or deletion of messages. It is highly possible that some of the vehicular nodes may be malicious, trying their best to destroy or disrupt the network. Hence, security considerations are clearly a highly important issue in order to achieve reliable VDTN network.

Annu et al.[19] has classified different attack on VDTN network, one of the attack classification is the attack on the availability of the network which is consist of DOS, Spamming, Black hole, Malware, Greedy Driver. Black hole characteristic is instead of forwarding data to destination it simply drops the packets. Hence, the destination vehicle will never be received the packets.

Security is a fundamental issue for promising applications in such networks, VDTN are prone to some specific attacks such as the malicious nodes (black hole attack) [18]. The proposed scheme is based on Intrusion Detection System (IDS), this scheme facilitates a method to defense against malicious nodes attacks (blackhole) to achieve reliable VDTN network with 3 performance metrics will be the key indicators (Throughput, Packet Loss, End to End Delay and Normalized Routing Load (NRL))

1.2 Problem Formulation

Based on above description, formulation of the problem can be made as follows:

1. VDTN are prone to specific attacks such as malicious node (blackhole)
2. How to make a reliable VDTN to defense against blackhole by improving Throughput, Packet Loss, End to End Delay and NRL.

1.3 Objective

1. Implementing Intrusion Detection System (IDS) on VDTN to achieve desirable QoS (Throughput, Packet Loss, End to End Delay and NRL)
2. Evaluating Intrusion Detection System (IDS) performance on VDTN to defense against blackhole attack.

1.4 Hypotheses

By implementing Intrusion Detection System (IDS) on VDTN will improve the QoS performance which consist of Throughput, Packet Loss, End to End Delay and NRL.

1.5 Scope of Work

The research will focus in the QoS performances that consist of Throughput, Packet Loss, End to End Delay and NRL. The steps and mechanisms which are influencing the research will be described as follow :

1. Implementation of Intrusion Detection System (IDS) on VDTN to defense against specific attack, the communication will be specific on Vehicle to Vehicle (V2V)
2. Blackhole attack will be implemented on the simulation, blackhole will either drops the packet or simply not forwarding the packet.
3. IDS and Blackhole simulation will be implemented on NS2 due to limitation of ONE Sim
4. Simulation tools on this research will be using ONE Sim and Network Simulator (NS2).

1.6 Research Methodology

The method used in this study are as follows :

1. Place and Time
   The study was conducted at the PT Telekomunikasi Indonesia International, Jakarta and at Switching laboratory of Telkom University, Bandung over a period of 6 months from December 2015 until May 2016
2. Study literature
   To learn the basic theory of literature related to Data Communication and Routing Protocols
3. System Design
   Network Configuration with real condition parameters including real geographical map, mobility model, clustering design and network specifications, blackhole attack and IDS implementation.
4. Preparation and Testing System
   This is the stage of the manufacturing system and then conduct tests on the system to see the accuracy of the system that has been designed
5. Analysis the result of data which have been simulated through generated specific attacks and after implementing Intrusion Detection System (IDS).
6. Making conclusions about the simulation results.