Autonomous Vehicle (AV) Cyber-Attack: LiDAR Spoofing

Ramadida Rai Pahlevi

STEI, Institut Teknologi Bandung, Bandung, Jawa Barat, Indonesia,
18217008@std.stei.itb.ac.id

ABSTRAKSI

Autonomous vehicle saat ini sudah bukan merupakan hal yang *untouchable*. Pada era industri 4.0, iterasi terhadap inovasi teknologi terus berkembang begitu juga pada transportasi. Saat ini, kehidupan serba otomatis sudah sangat dekat dengan manusia. Berbelanja tanpa perlu pergi, robot asisten rumah tangga, dan dalam konteks ini, *autonomous vehicle*. Sistem AV merupakan sebuah sistem cerdas berbasis komputer yang para komponen komputer dan kendaraan saling berkomunikasi untuk melakukan sebuah task driving untuk menggantikan pengemudi. Sebuah sistem AV memiliki sebuah persepsi terhadap lingkungan transportasi. Untuk mengidentifikasi ekosistem tersebut biasa digunakan teknologi LiDAR. Sensor LiDAR mengidentifikasi sebuah objek berdasarkan banyak faktor. Teknologi ini dipakai oleh AV agar komputer dapat mengenal dan familiar terhadap objek-objek pada lingkungan transportasi untuk mengemudi dengan aman. Salah satu attack yang dapat terjadi pada AV adalah LiDAR *spoofing*. *Spoofing* terhadap sensor LiDAR dapat mengganggu perilaku AV, sehingga dapat berisiko terhadap keamanan berkendara. Tulisan ini mengkaji dua studi kasus yang berhubungan dengan *cyber-attack: spoofing* pada sensor LiDAR dan menjelaskan bagaimana proses *spoofing* LiDAR pada *autonomous vehicle*.

KATA KUNCI

Sensor attack, Autonomous driving, LiDAR, *Spoofing*

1 Latar Belakang

Teknologi autonomous vehicle (AV) sudah menjadi bagian dalam hidup kita. Beberapa mobil otomatis sudah terlihat di ramai jalan raya Jakarta. Teknologi ini merubah dan mengembangkan potensi sistem transportasi dan memberi dampak terhadap keamanan penumpang. Teknologi ini memiliki 5 level otomatisasi, dimana *level 0: no automation, level 1: function specific automation, level 2: combined-function automation, level 3: limited self-driving automation,* dan *level 4 full self-driving automation* [1]. Salah satu

konsep penting dalam sistem AV adalah *perception*, yaitu pemahaman sistem AV terhadap lingkungan sekitar. Layaknya pengendara manusia, sistem AV juga harus memiliki persepsi yang menyerupai. Untuk memfasilitasi *perception skill*, sistem AV dilengkapi sensor seperti kamera dan LiDAR (Light Detection and Ranging). Fungsi dari sensor-sensor ini memberikan dampak langsung kepada reaksi AV terhadap keadaan di lapangan. LiDAR berfungsi sebagai proyeksi peta 3D disekitar AV dengan mengkalkulasi jarak antara sensor dan sebuah objek berdasarkan pantulan cahaya. LiDAR menembak laser infrared terhadap suatu objek, dan gambar sebuah objek akan muncul dengan perhitungan yang melibatkan jarak dan waktu tempuh dari cahaya tersebut. LiDAR mampu memberikan pandangan 360 derajat terhadap keadaan sekitar dengan metode ini. Sensor LiDAR dianggap lebih penting dari sensor lainnya untuk persoalan keamanan sistem AV. Setiap tembakan yang menyentuh suatu objek akan diidentifikasi sebagai *point cloud*. Sebuah sensor LiDAR dapat memproduksi jutaan *point cloud* yang menjadi sebuah data yang akan diproses selanjutnya. Sensor LiDAR memiliki akurasi hingga radius 200 meter. Perilaku sebuah sistem AV sangat dipengaruhi oleh LiDAR. Seluruh objek yang dapat diidentifikasi oleh sensor ini akan mempengaruhi perilaku berkendara dari AV.

Dikarenakan fungsinya yang sangat penting pada sistem AV, beberapa ilmuwan telah melakukan sebuah riset terhadap kapabilitas LiDAR dalam menangani sebuah masalah. Eksperimen yang dilakukan oleh Cao et al. [2] tentang *adversarial sensor attack* pada sistem AV menunjukkan sebuah skenario penyerangan terhadap sensor LiDAR yang akan menjadi salah satu bahasan pada tulisan ini. Selain itu, Petit et al. [3] juga melakukan sebuah eksperimen terhadap penyerangan sensor LiDAR. Dua eksperimen ini meneliti tentang *spoofed attack* yang menyerang sensor LiDAR pada sistem AV. *Spoofing* pada sensor LiDAR dapat dideskripsikan sebagai proses injeksi sinyal palsu yang bertujuan untuk mengelabui kinerja sistem. Sistem tidak dapat mendeteksi sinyal palsu dan akan tetap memproses sinyal tersebut. Maka dari itu *spoofing attack* dipertimbangkan sebagai sebuah *cyber-attack* yang berbahaya pada sistem AV karena dapat mempengaruhi fungsi dan perilaku AV dan dapat membahayakan penumpang dan lingkungan sekitar. Salah satu contoh kasus adalah penempatan objek palsu didepan kendaraan dengan sensor LiDAR. Hal ini dapat mengakibatkan kendaraan melakukan rem mendadak atau *freeze* apabila dalam kondisi diam dan dapat membahayakan kendaraan dan orang-orang sekitar. Pada

tulisan ini, penulis akan mengkaji hasil riset dari dua kelompok ilmuwan [2, 3] yang telah melakukan eksperimen terkait *cyber-attack* dengan jenis spoofing yang menyerang sensor LiDAR. Kajian ini dilakukan untuk mengetahui bagaimana proses menyerang dengan teknik *spoofing* mempengaruhi sistem AV secara komprehensif. Diharapkan setelah membaca tulisan ini, pembaca mendapat pengetahuan terkait penyerangan spoofing pada sistem AV, dan apabila salah satu dari pembaca merupakan pengembang teknologi AV, mendapatkan sebuah informasi yang berguna untuk proses pengembangan teknologi.

1.1 Adversarial Sensor Attack on LiDAR by Cao et al.

Pada penelitian yang dilakukan oleh Cao et al. [2], dilakukan studi untuk mengeksplorasi kemampuan keamanan dari sensor LiDAR pada sistem AV. Eksperimen ini dilakukan dengan menggunakan implementasi LiDAR oleh Baidu Apollo, sebuah sistem AV *open-source* yang telah bekerja sama dengan brand-brand otomotif terkenal seperti Volvo dan Ford. Eksperimen ini dilakukan dengan injeksi sinyal palsu yang akan mempengaruhi point cloud yang akan diterima oleh LiDAR. Tujuan akhir penyerangannya adalah menempatkan sebuah objek palsu didekat kendaraan AV dengan teknik *spoofing* hingga sistem AV merubah perilaku berkendara. Untuk mendapatkan hasil yang maksimal, studi kasus ini dilakukan dengan mengontrol variabel *spoofed point* untuk mengelabui sistem deteksi objek. Pada umumnya, pemodelan deteksi objek pada LiDAR menggunakan model *machine-learning.* Eksperimen pada studi kasus ini akan mengontrol *spoofed point* dan membuat sebuah model transformasi yang merubah input *spoofed point* menjadi sebuah model spasial yang akan dideteksi sebagai sebuah objek. Cakupan yang dikaji pada tulisan ini terhadap eksperimen hanya sebatas proses melakukan penyerangan *spoofing.* Skenario yang akan dilakukan pada eksperimen ini untuk mendapatkan pemahaman yang logis terhadap dampak penyerangan adalah (1) *emergency brake attack* dan (2) *AV freezing attack.* Dengan teknologi dan data yang didapatkan oleh Baidu Apollo, eksperimen ini dapat mensimulasikan penyerangan dan dampaknya terhadap sistem AV dengan baik. Pengkajian lebih detil akan dideskripsikan pada bagian pembahasan studi kasus.

1.2 Remote Attack on AV Sensors by Petit et al.

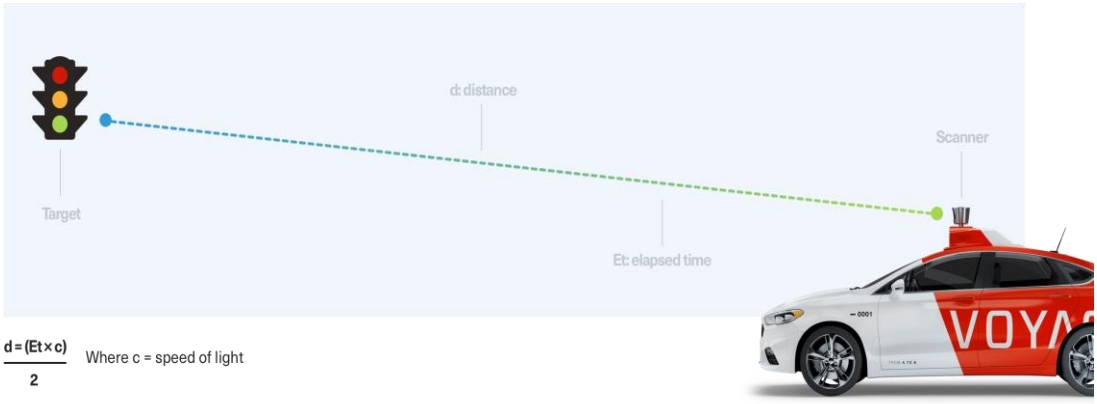
Berbeda dengan penelitian Cao et al., Eksperimen yang dilakukan oleh Petit et al. Merupakan eksperiman dengan domain yang sama namun dengan skala yang lebih kecil.

Petit et al. melakukan eksperimen penyerangan *remote* terhadap sistem LiDAR dan kamera pada AV. Pada tulisan ini cakupan yang dikaji hanya penyerangan terhadap sistem LiDAR. Pada eksperimen ini, Petit et al. menggunakan material yang cukup murah untuk mempertimbangkan *feasibility* dari eksperimen ini. Secara umum studi kasus ini cukup mirip dengan studi kasus pertama. Studi kasus ini hanya mengkaji elemen sinyal dan model 3D sehingga perbedaannya eksperimen ini mengkaji secara *view-level* dan *physical-level*, bagaimana penyerangan *spoofing* pada LiDAR bekerja sedangkan studi kasus pertama lebih mengkaji *logical-level* dari penyerangan *spoofing*.

2 Teori Dasar

2.1 LiDAR Pada Sistem AV

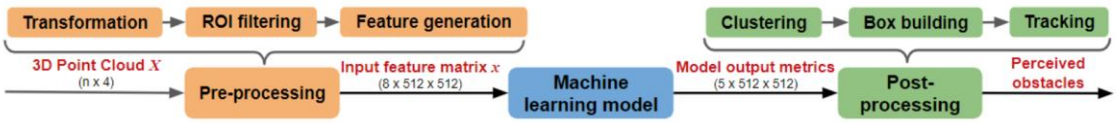
LiDAR adalah sebuah sensor yang dapat mengetahui sebuah nilai jarak berdasarkan pantulan cahaya. LiDAR memiliki sudut pandang 360° dan memiliki jarak radius maksimal 200-meter sehingga kemampuan LiDAR untuk mendeteksi sebuah objek merupakan salah satu faktor mengapa LiDAR sangat penting untuk diimplementasikan pada sistem AV. Perhatikan gambar 1, cara bekerja sensor LiDAR adalah dengan menembakan sebuah laser cahaya dan mengukur jarak berdasarkan waktu pantulan cahaya kembali ke sensor. Kemampuan LiDAR untuk menembakan berjuta-juta laser menghasilkan jutaan data point yang akan diolah dan diproses menjadi model spasial.



Gambar 1: Ilustrasi cara kerja sensor LiDAR pada AV [4]

LiDAR adalah teknologi berbasis gelombang. LiDAR dapat membuat sebuah model peta 3D dengan mentransformasi data-data yang didapatkan dengan menembakan laser.

Berdasarkan sistem Baidu Apollo [2], LiDAR memroses data dalam *pipeline* dengan tiga proses utama yaitu, *pre-processing*, *modelling*, dan *post-processing*. Pada proses *pre-processing input* sensor LiDAR menerima sejumlah *data point* dan setiap *data point* diproyeksikan dalam vektor 4 dimensi dengan koordinat 3D **Wx, Wy, Wz** dan intensitas dari *data point*. Setelah itu *data point* ini di filter dan di *mapping* ke sebuah matriks berukuran 8 X 512 X 512 untuk di-*input* ke model yang telah dibuat. Proses *modelling* akan menerima input matriks dan berdasarkan parameter yang telah dibuat akan menilai input dan menghasilkan *output metrics* yang menjadi dasar untuk proses selanjutnya. Proses berikutnya adalah post-processing. Pada proses ini *output metrics* yang telah dihasilkan pada *modelling* akan melalu proses *clustering* yang akan menyaring dan mengelompokkan *data point* menjadi sebuah kandidat objek yang akan di persepsikan menjadi sebuah objek dalam model 3D berdasarkan informasi yang dimilikinya. Dengan informasi yang dimiliki pada sebuah kandidat objek, sistem kemudian akan menerima informasi objek dan merespon dengan perilaku AV.



Gambar 2: Data pipeline pada sistem LiDAR Baidu Apollo [2]

Gambar 3: Ilustrasi objek model 3D pada Google car [4]

2.2 Serangan Spoofing Pada LiDAR

Sistem AV memerlukan data yang sangat akurat untuk fungsionalitas yang baik. Maka dari itu dibutuhkan sensor-sensor yang menginput data-data yang diperlukan untuk keberlangsungan kinerja sistem AV. Seperti deskripsi diatas, LiDAR merupakan sensor yang mengetahui jarak dari pantulan cahaya. Sensor LiDAR sangat mengandalkan waktu tempuh dari cahaya pantul. Kecepatan cahaya diudara konstan dengan nilai aproksimasi $3x10^8$ m/s. Waktu yang diperlukan untuk memantulkan suatu cahaya pada suatu titik akan menentukan jarak antara sensor dengan titik tersebut. Setiap titik disimpan sebagai data dan data tersebut digunakan untuk sistem keputusan AV. Serangan *spoofing* dilakukan dengan mengirimkan sinyal pantulan palsu tanpa mengganggu proses transmisi sensor. Serangan ini sangat sulit untuk diidentifikasi karena tidak melibatkan serangan fisik pada sensor [2]. Serangan ini dapat mengelabui data input sensor dengan data palsu dan mengakibatkan sistem AV bertindak tidak ideal. Berdasarkan penelitian Petit et al. [3], serangan ini tergolong serangan yang mudah dilakukan dan dapat berdampak serius, dikarenakan serangan dapat dilakukan secara remote dengan merubah sinyal-sinyal palsu sehingga sistem AV mengidentifikasi rintangan dengan jarak yang berbeda-beda. Hal ini dapat berakibat fatal pada penumpang.

2.3 Model Serangan

Tujuan dari serangan ini adalah untuk menipu sensor LiDAR untuk mempersepsikan sebuah objek disekitarnya untuk memaksakan sebuah keputusan yang dapat membahayakan penumpang. Penipuan pada sensor ini melibatkan kualitas data pada sistem. Terdapat tiga model serangan yang dapat mendisrupsi fungsi dari AV. Terdapat *front/rear/side attack,* jenis ini mengimplementasi alat untuk menyerang pada mobil penyerang. Penyerangan ini dapat dilakukan pada sisi depan, belakang, dan samping mobil *target* sesuai dengan posisi mobil penyerang. Serangan dapat dilakukan berkali-kali selama mobil penyerang masih pada posisi paralel dengan mobil *target*. Model kedua adalah *roadside attack* yaitu penyerangan yang dilakukan dengan pemasangan alat *spoofing* pada pinggiran jalanan. Alat-alat dapat dipasang dengan jumlah tidak terbatas dan saling berhubungan sehingga kualitas serangan dapat ditingkatkan namun jarak serangan akan terbatas. Model terakhir menurut Petit et al. [3] adalah *Evil mechanic attack* yang merupakan serangan dengan akses fisik. Serangan ini dilakukan apabila kendaraan sedang tidak diawasi dan dalam keadaan diam dengan melakukan *jamming* pada kendaraan *target.* Model serangan yang lebih spesifik akan dideskripsikan pada setiap studi kasus setelah ini.

3 Pembahasan

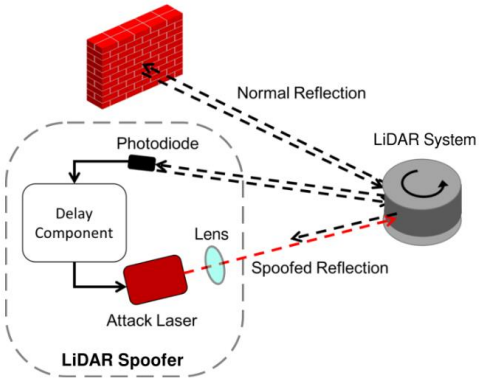
Pada tahap ini akan dijelaskan secara komprehensif penelitian yang dilakukan berdasarkan dua kasus. Kasus 1 adalah eksperimen yang dilakukan oleh Cao et al. [2] dan kasus 2 adalah eksperimen yang dilakukan oleh Petit et al. [3]. Cakupan pembahasan dari kedua studi kasus ini membahas proses *spoofing* pada *physical-level* dan *view-level.* Hal ini berpengaruh khususnya pada kasus 1, eksperimen meliputi percobaan pada level fisik, dan level *logic.*

3.1 Studi Kasus 1

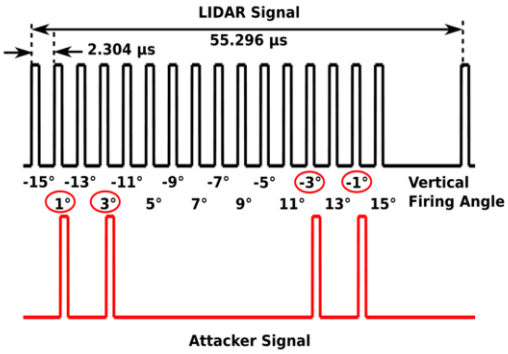
3.1.1 Pengaturan Awal

Spoofing attack yang akan dilakukan pada studi kasus ini dilandaskan salah satu eksperimen terdahulu oleh Shin et al. [5]. Komponen yang digunakan berdasarkan eksperimen tersebut terdiri dari tiga komponen yaitu *photodiode*, komponen *delay*, dan *attack laser*. *Photodiode* digunakan untuk menerima sinyal cahaya yang ditembakan sensor LiDAR, sedangkan komponen *delay* akan mentrigger *attack laser* untuk menembak

kembali sebuah sinyal *spoofed* setelah sinyal *input* melewati suatu fungsi waktu tertentu untuk memalsukan data objek. Pengaturan komponen dapat dilihat pada gambar 4.



Gambar 4: Ilustrasi pengaturan serangan spoofing [2].



Gambar 5: Ilustrasi penembakan sinyal spoofed pada sudut 1, 3, -1, dan -3 [2].

Pada eksperimen ini [2], Cao et al. menggunakan VLP-16 PUCK LiDAR dari Velodyne. LiDAR ini memiliki 16 laser vertikal yang mencakup *range* 30 derajat, dari –15 derajat hingga +15 derajat. Secara horizontal LiDAR ini mampu berputar 360 derajat dengan azimuth antara 0.1 derajat hingga 0.4 derajat. LiDAR ini menembakan gelombang laser setiap 55.296 µs, memiliki periode 2.304 µs, dan jarak waktu penerimaan sinyal balik sekitar 667 ns. Ilustrasi penembakan sinyal *spoofed* dapat dilihat pada gambar 5. Pada ilustrasi tersebut dapat dilihat bahwa LiDAR menembakan sinyal secara konstan dalam kurun waktu tertentu. Penembakan sinyal *spoofed* dapat diatur berdasarkan pelaku penyerangan seperti contoh diatas.

Komponen p*hotodiode* pada eksperimen ini menggunakan OSRAM SFH 213 FA. Sedangkan komponen *delay* menggunakan Tektronix AFG3251 *function generator*. Komponen *attack laser* terbagi menjadi dua komponen. Pemicu laser menggunakan modul PCO-7114 yang akan menstimulasi *attack laser diode* OSRAM SPL PL90. Modul PCO-7114 dapat mengeluarkan laser dengan periode yang sama dengan VLP-16 sehingga kompatibel untuk eksperimen ini. Bentuk gelombang akan dibuat dengan perangkat lunak

Tektronix dan perangkat lunak Velodyne digunakan untuk analisis dan ekstraksi *data point.*

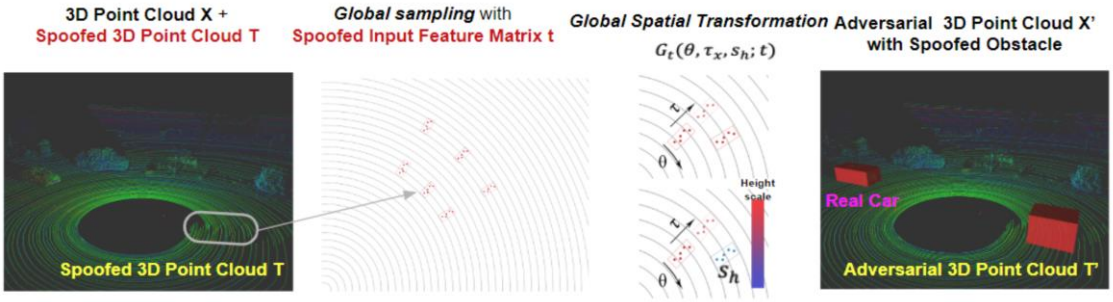
3.1.2 ADV-LiDAR

Eksperimen ini dilakukan berdasarkan pengaturan awal. Eksperimen yang akan dikaji pada tahapan ini adalah metode ADV-LiDAR. Pada penelitiannya, Cao et al. melakukan eksperimen terdahulu dengan secara random menembakan sinyal *spoofed* pada LiDAR yang mampu menghasilkan *spoofed data point.* Namun pada proses *post-processing data point* tersebut tidak dapat diidentifikasi menjadi sebuah rintangan dikarenakan kemampuan serangan yang belum memadai. Cao et al., mengembangkan metode baru ADV-LiDAR yang mempertimbangkan *logic-level* dari sistem LiDAR dengan mempelajari model *machine learning*. *Data point* melewati *pre-processing* sebelum menjadi input pada model *machine learning*. Metode ADV-LiDAR memodifikasi variabel kontrol *spoofed point* agar pada *pre-processing*, input data akan kompatibel dengan model *machine learning*. Proses ini akan dijelaskan pada paragraf berikutnya tentang *spoofing attack capability*. Metode ini juga menganalisis *post-processing* dan mengembangkan fungsi *global spatial transformation* untuk mengidentifikasi sebuah rintangan.

Spoofing attack capability mengkaji *spoofed point* yang akan ditembak pada saat penyerangan. Pada eksperimen ini, *spoofed point* yang akan ditembakkan berkisar 60 titik. Terdapat 3 faktor penting yang dipertimbangkan untuk membuat sebuah *spoofed point*. (1) Memodifikasi jarak *spoofed point* dengan LiDAR dengan mengatur komponen delay. (2) Memodifikasi ketinggian dari *spoofed point* dengan mengatur komponen delay dalam kurun periode 2.304 μs. (3) Memodifikasi *azimuth* dengan mengatur komponen delay dalam kurun waktu 55.296 μs. Setelah menganalisis kapabilitas spoofing attact, Cao et al. Membuat sebuah input matriks yang akan mentransformasi *input spoofed point* menjadi matriks yang akan masuk ke model *machine learning.*

3.1.3 Hasil Eksperimen

Gambar 6 menggambarkan simulasi dari eksperimen ADV-LiDAR. Pada gambar 6, dapat dilihat bahwa terdapat *spoofed point* pada sebuah model 3D. Lalu spoofed point akan dilakukan sampling menggunakan input matriks yang telah dibuat s. Setelah itu, output dari model *machine learning* akan ditransformasi oleh fungsi *global spatial transformation* yang akan menghasilkan 3D *spoofed point.*



Gambar 6: Ilustrasi simulasi serangan spoofing [2].

Untuk membuktikan bahwa serangan ini berpengaruh terhadap *decision system* AV, dilakukan simulasi *sim-control* yang disediakan oleh Baidu Apollo. Pada proses simulasi digunakan data input 3D *point cloud* dengan *spoofed object.* Terdapat dua skenario pada eskperimen ini. (1) *Emergency brake attack* dan (2) AV *freezing attack.* Pada serangan *emergency attack*, di injeksikan 3D *point cloud* pada AV yang sedang berjalan. Setelah mengidentifikasi objek, AV kemudian melakukan rem mendadak yang dapat membahayakan penumpang. Pada *freezing attack,* diinjeksikan 3D *point cloud* pada AV dalam kondisi diam pada lampu merah. Setelah mengidentifikasi objek, sistem AV tetap dalam kondisi statik walaupun kondisi lampu merah sudah hijau. Hal ini dapat mengakibatkan kemacetan dan gangguan pada jalanan. [1]

3.1.4 Kesimpulan Penelitian

Pada eksperimen ini, dilakukan eksplorasi sekuritas sistem AV dengan melakukan *spoofing attack* pada sensor LiDAR. LiDAR adalah sensor yang dapat mengidentifikasi sebuah objek pada lingkungan dan mempengaruhi perilaku sistem AV. Eksperimen ini menganalisis model *machine learning* yang mempengaruhi pemrosesan data dari LiDAR. Cakupan kajian hanya meliputi *physical level* dan *view level* dari proses *spoofing*. Setelah analisis dilakukan, Cao et al. memodifikasi model *pre-processing* dan *post-processing* dan mengoptimasi model tersebut sehingga sesuai dengan model *machine learning*. Setelah dilakukan optimasi, injeksi *spoofed point* yang dikontrol akan disampling menggunakan matriks yang kompatibel dengan model *machine learning*. *Output* dari model *machine*

[1] Video demo dapat ditemukan pada tautan berikut ini https://sites.google.com/umich.edu/advlidar/ [2].

learning kemudian akan ditransformasi dan menghasilkan 3D *point cloud* yang akan diidentifikasi sebagai suatu objek berdasarkan *metrics* yang sudah ada.

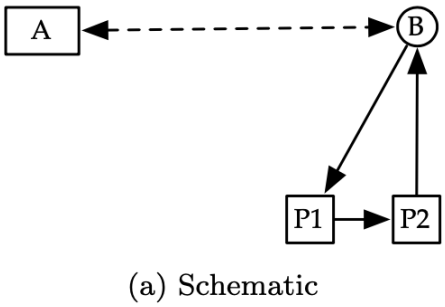
3.2 Studi Kasus 2

3.2.1 Pengaturan Awal

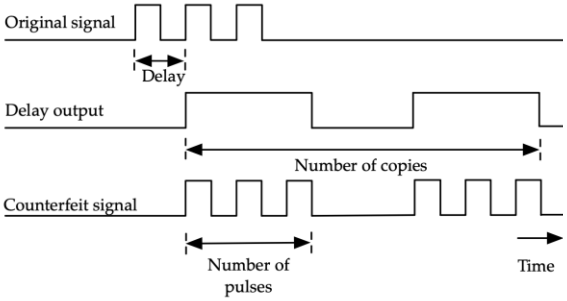
Petit et al. [3] menggunakan LiDAR: ibeo LUX 3 untuk digunakan pada eksperimen ini. LiDAR ini dapat menangkap 800 titik per meter persegi dan terbukti sangat efisien. Ibeo LUX 3 adalah LiDAR 4 lapis yang memiliki sudut horizontal hingga 110 derajat. LiDAR ini tidak memberikan model spasial 3D, dan hanya mengandalkan 4 lapis model 2D. Radius maksimal yang dicakup Ibeo LUX 3 adalah 200 meter. LiDAR ibeo LUX 3 sudah dilengkapi *object tracking system* yang menggunakan Kalman filter untuk mengidentifikasi objek-objek berikut: (1) Mobil, (2) truk, (3) sepeda, (4) pejalan kaki, (5) *unknown small*, (6) *unknown big.* Setiap objek akan diidentifikasi untuk keperluan *tracking* dan maksimal *object tracking* adalah 65. Selain LiDAR, eksperimen ini menggunakan alat penerima sinyal yaitu photodetector Osram SFH-213. Terdapat dua komponen lainnya yang berfungsi sebagai *control logic*. HP 8011A pulse generator yang berfungsi sebagai komponen delay, dan Phillips PM 5715 yang berfungsi untuk membuat sinyal *spoofed* apabila distimulus oleh komponen delay.

3.2.2 Spoofing the Signal

Eksperimen ini [3] bertujuan untuk menginjeksi objek palsu pada sistem LiDAR. Kecepatan cahaya pada udara bersifat konstan $3x10^8$ m/s atau berjalan 1-meter setiap 3.33 ns. Dengan batas radius 200 meter, ibeo LUX 3 memiliki waktu tempuh sinyal maksimal selama 1.33 μs. *Time window* tersebut menjadi acuan penembakan sinyal harus berada pada kurun waktu tersebut. Pengaturan kedekatan suatu objek dapat diatur berdasarkan waktu penembakan sinyal *spoofed.* Semakin kecil waktu *delay* maka objek akan dianggap semakin dekat.



Gambar 7: Ilustrasi pengaturan komponen [3].

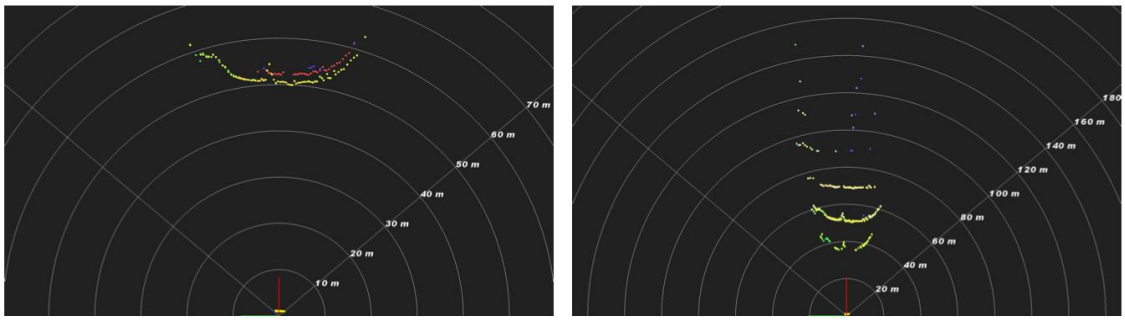


Gambar 8: Ilustrasi sinyal pada serangan spoofing [3].

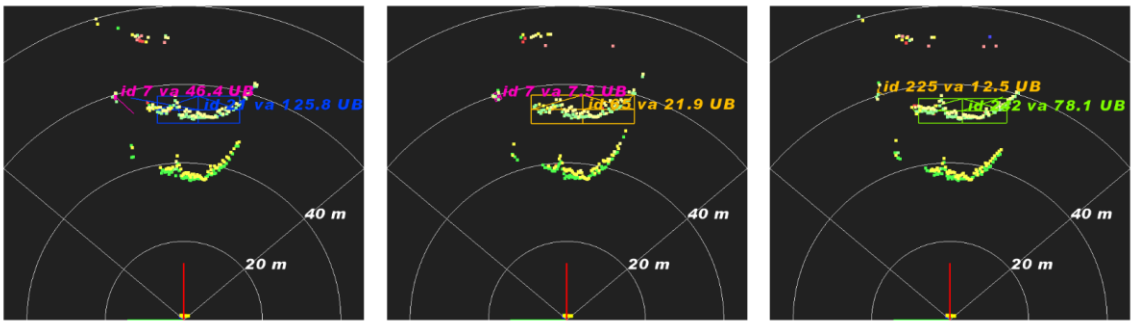
Pada gambar 7, dapat dilihat pengaturan alat untuk eksperimen ini. Asumsikan A adalah ibeo LUX 3, B adalah *photodetector*, P1 adalah komponen *delay*, dan P2 adalah *pulse generator*. LiDAR A akan menembakan sebuah sinyal dan akan diterima oleh *photodetector* B. *Output* dari B akan memberikan *trigger* kepada komponen *delay.* P1 akan mengeluarkan sinyal yang telah melewati fungsi *delay* dan akan menjadi input P2. Kemudian setelah terjadi *trigger* pada P2, *pulse generator* akan membuat sebuah sinyal *spoofed* yang akan ditembakan kembali ke LiDAR. Pada eksperimen ini, fungsi *delay* dan *pulse form* merupakan variabel kontrol. Dapat dilihat pada gambar 8, bagaimana *delay output* dan *number of copies* dapat mempengaruhi sinyal *spoofed (counterfeit).*

3.2.3 Hasil Eksperimen

Gamber 9 menunjukan *spoofing point* yang berhasil ditembakan pada LiDAR. Dapat dilihat bahwa terdapat salinan dari sebuah objek tembok sejauh 50-meter yang dihasilkan dari *echo* pertama sinyal *spoofed.* Setelah itu, salinan menjadi semakin banyak pada jarak 40, 50, dan 70-meter dengan memodifikasi *echo* sinyal *spoofed* selama masih dalam jendela waktu 1.33 μs. Ibeo LUX 3 memiliki fungsi *tracking object* yang akan mengidentifikasi suatu objek dari kumpulan data. Pada gambar 10, fungsi ini dinyalakan dan disimulasikan lagi penembakan sinyal *spoofed.* Ibeo LUX 3 mengidentifikasi objek salinan pertama ini sebagai *unknown big*, dan dalam kurun waktu tertentu sinyal yang hanya memodifikasi *echo* dapat diidentifikasi sebagai 3 objek *unknown big* berbeda pada LiDAR.



Gambar 9: Ilustrasi spoofed point pada LiDAR [3].



Gambar 10: Ilustrasi tracking object pada LiDAR [3].

3.2.4 Kesimpulan Penelitian

Pada eksperimen ini, dilakukan serangan *spoofing* sinyal pada LiDAR: ibeo LUX 3. *Spoofing* menggunakan komponen *photodetector*, komponen *delay*, dan *pulse generator*. Injeksi sinyal *spoofed* dihasilkan dengan menyalin sinyal datang dengan suatu delay tertentu sehingga akan mengakibatkan sinyal *spoofed* yang diterima terlihat seakan-akan sinyal pantul objek. Teknik *spoofing* juga dapat digunakan untuk menciptakan beberapa objek dengan memodifikasi *echo* dari salinan sinyal yang akan ditembak kembali ke LiDAR. Fungsi *tracking object* akan mengidentifikasi setiap *echo* pada sinyal *spoofed* sebagai sebuah objek baru dan akan mengakibatkan perubahan perilaku sistem AV.

4 Kesimpulan

Pada tulisan ini, penulis mengkaji dua eksperimen yang saling berhubungan. Kedua eksperimen ini dilakukan oleh Cao et al. [2] dan Petit et al. [3]. Berdasarkan kajian ini, terdapat beberapa hal yang dapat disimpulkan. *Spoofing* dapat dilakukan dengan menembakan sebuah sinyal palsu yang menyalin sinyal asli dengan suatu delay waktu yang disesuaikan dengan *time window* dari LiDAR. Sinyal yang berhasil ditangkap kembali oleh LiDAR akan menjadi *spoofed point* yang akan di transformasi menjadi suatu objek. Proses

pre-processing spoofed point merupakan proses yang membutuhkan analisis terhadap model *machine learning* LiDAR. Setiap LiDAR memiliki model *machine learning* yang berbeda-beda. Setelah analisis, fungsi transformasi data akan disesuaikan dengan model *machine learning* sehingga *input* akan kompatibel dengan model. Output dari model akan ditransformasi menjadi sebuah model 3D yang akan diidentifikasi menjadi sebuah objek sesuai kemampuan LiDAR. Setelah *spoofed point* diidentifikasi menjadi sebuah objek, simulasi dilakukan untuk mengetahui apakah rintangan palsu yang dihasilkan dapat mempengaruhi perilaku dari sistem AV. Penyerangan *spoofing* pada sistem AV terbilang cukup mungkin dilakukan dengan alat-alat yang tidak terlalu mahal. Pemahaman terhadap pemodelan dalam sistem LiDAR diperlukan untuk melakukan penyerangan yang efektif. Pada tulisan ini, telah dideskripsikan melalu dua studi kasus bagaimana penyerangan *spoofing* pada sistem LiDAR dilakukan. Kedepannya, diharapkan tulisan ini dapat memberikan pandangan untuk pengembangan mitigasi dari *cyber-attack* ini.

REFERENCES

[1] Anderson, James M., Nidhi Kalra, Karlyn D. Stanley, Paul Sorensen, Constantine Samaras, and Tobi A. Oluwatola, Autonomous Vehicle Technology: A Guide for Policymakers. Santa Monica, CA: RAND Corporation, 2016.

[2] Y. Cao, C. Xiao, B. Cyr, Y. Zhou, W. Park, S. Rampazzi, Q. A. Chen, K. Fu, and Z. M. Mao, "Adversarial Sensor Attack on LiDAR-based Perception in Autonomous Driving," Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, 2019.

[3] Jonathan Petit, Bas Stottelaar, Michael Feiri, and Frank Kargl. Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR. Black Hat Europe. 2015.

[4] An Introduction to LIDAR: The Key Self-Driving Car Sensor. https://news.voyage.auto/an-introduction-to-lidar-the-key-self-driving-car-sensor-a7e405590cff. 2017.

[5] Shin H., Kim D., Kwon Y., Kim Y. Illusion and Dazzle: Adversarial Optical Channel Exploits Against Lidars for Automotive Applications. In: Fischer W., Homma N. (eds) Cryptographic Hardware and Embedded Systems – CHES 2017. CHES 2017. Lecture Notes in Computer Science, vol 10529. Springer, Cham. 2017.