デジタルツインのための LiDAR データ比較によるデータ改ざん検出

Data Tampering Detection by LiDAR Data Comparison for Digital Twin

高橋悠理　長坂新　中川雅史
Yuri Takahashi, Arata Nagasaka, Masafumi Nakagawa
芝浦工業大学
Shibaura Institute of Technology

1.　はじめに

デジタルツインは，現実空間をセンシングし，デジタル空間に現実空間を複製するとともに，デジタル空間での最適化結果を現実空間にフィードバックするというデータサイクルを実行するものである．近年，デジタルツインを都市空間に適用することで都市全体の最適化を図り，高度な社会課題の解決に貢献する動きが活発になっている．そして，都市のデジタルツイン実現のためのセンシングとして，スマートフォンや IoT デバイス，監視センサ等が用いられる．しかしながら，民間企業や自治体など多様な主体がそれらの所有者となることで，一元的なセキュリティ管理が難しくなることが想定される．さらに，システムへの攻撃やデータ改ざんへの対応の不十分さも想定され，セキュリティ管理の難しさが懸念される．近年ではオープンデータの利活用も進められているが，オープンデータは改ざんがないことを保証するものではないため，信頼性の高いシミュレーション結果を得ることを困難にする可能性もある．したがって，GNSS 測位と同様に，画像センシングや 3D センシングなどでも完全性に関する議論が必要となる．そこで本研究では，都市のデジタルツインにおける複数スキャナ間での LiDAR のセキュリティについて議論する．

2.　手法

図 1 に手法フローを示す．まず，2 つの定点スキャナから点群を取得する．そのうちの 1 つを基準とする「基準点群」，もう 1 つを基準と照らし合わせて調べる「照査対象点群」とする．この「基準点群」を基準として，点群のレジストレーションと時刻同期を行う．その後，時刻同期まで行った 2 つの点群に対して Root Mean Square Error(RMSE)を用いて残差を算出する．この残差が小さいほど，2 つのスキャナでそれぞれ取得した点群による空間が一致しているものと考える．

また，点群の生成 AI である Point-E を用いて点群を生成し，これを照査対象点群に挿入することで，悪意を持った処理が行われた(攻撃された)ケースを想定した実験を行う．この生成点群を時系列の途中で挿入する実験では，攻撃前と攻撃後の残差を比較し，空間一致度を検証する．

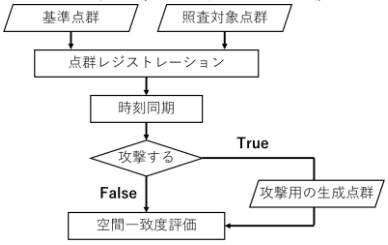

図 1．手法フロー

3.　実験・処理

実験は大型トランポリン遊具とそれの利用者を対象として行った．実験機材は定点スキャナ 2 台を用い，反復走査型 LiDAR スキャナ(VLP-32C, Velodyne)及び，非反復走査型 LiDAR スキャナ(AVIA, Livox)を利用した．

この実験で得られた点群に対して時刻同期を行った後，スケール調整を行ったうえで Point-E を用いて生成した点群を挿入した(図 2)．点群生成のプロンプトは「A tree」とした．照査対象点群は時系列データであり，その途中から点群を挿入した．

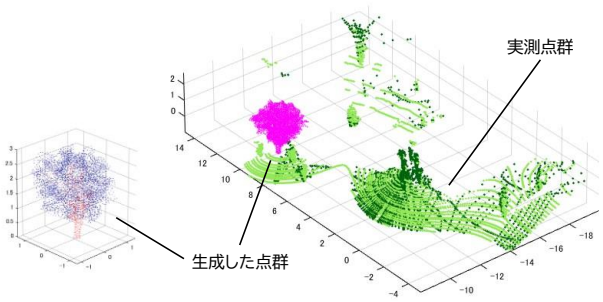

図 2．挿入した点群

4.　結果および考察

図 3 は，攻撃前と攻撃後の残差の比較であり，攻撃された場合は空間一致度が低下(残差が増加)することを示している．攻撃の検知を行うためには，残差に閾値を設定しその値を超えた際には攻撃されているとみなすことで可能であると考えられる．例として，図 3 では 0.5 を閾値と設定することで，0.5 以下のときは攻撃されていない正常な点群，0.5 以上のときは攻撃下にある点群とみなすことができる．さらに，その閾値を超えたタイミングを計測した際には，そのタイミングで攻撃されたことが検知できると考えられる．

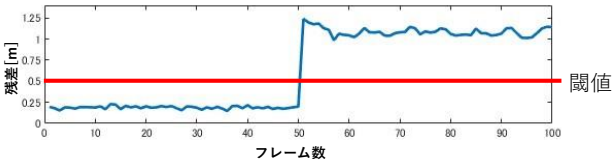

図 3．LiDAR 攻撃時の空間一致度の変化

5.　まとめ

本研究では，デジタルツインに構築における LiDAR への攻撃および検知に関する議論を行った．今後の展望として，より巧妙な攻撃に対しての検知への議論が挙げられる．