

**Phase Detection based Two-way Ranging
in Sub-GHz Band
for Remote Keyless Entry Systems**

August 2022

Ichiro Seto

主 論 文 要 旨

No.1

報告番号	甲 乙 第	号	氏 名	瀬戸 一郎
主 論 文 題 名 : Phase Detection based Two-way Ranging in Sub-GHz Band for Remote Keyless Entry Systems (リモートキーレスエントリシステム向けサブギガヘルツ帯における位相検波を用いた双方向型測距方式)				
(内容の要旨) 市場に浸透しているリモートキーレスエントリ (RKE) システムは、近傍磁界結合を活用し、所有者が車両の所定距離以下に近寄ると、キー FOB に触れる必要なく、ドアロックを解除する。近傍磁界は盗聴の脆弱性があり、車両盗難等の被害が増える社会問題となっている。リレーアタックと呼ばれる攻撃は、磁界を傍受し、離れたキー FOB に無線中継し、キー FOB からの応答も車両に向け無線中継する。車両はキー FOB が近寄ったと騙され、ドアロックを解除してしまう。この攻撃への対策は急務であり、無線測距方式の導入が期待されている。例えば、車両がキー FOB までの距離を認識し、3m 以内にある時のみドアロック解除することで、車両盗難を防げる。RKE システムでは、測距性能に加え、グローバル無線規定、カバレッジ、低消費電力によるバッテリー動作等の必要条件がある。様々な測距方式のなかで、サブギガヘルツ帯の位相検波方式が注目される。 本論文では、RKE システム向けサブギガヘルツ帯における位相検波を用いた双方向型測距方式を提案する。時間検波で研究されてきた双方向型の概念を位相検波に拡張し、新たに適用する 8 シーケンスの通信により、送受デバイス間の非同期クロックオフセットによる時間及び位相ずれへの耐性を高め、高精度の距離測定を提供する。さらに、狭帯域条件下で、マルチパスの無線伝搬の影響を軽減する世界初の補償方式を提案する。 本論文では、まず、RKE システム及びリレーアタックの概要、無線仕様、測距方式比較を紹介し、提案するシーケンス及びマルチパス補償方式の動作原理を述べる。続けて、クロックオフセット、マルチパスに対する理論的な性能限界、無線機雑音による性能ばらつきを導く。無線機プロトを用いて、車両傍ら 6m x 6m エリアのマルチパス環境下でフィールド評価を実施し、提案する測距方式の有効性を確認する。理論性能限界及び実測性能は、平均絶対誤差にて 0.65 m 及び 1.13 m、誤差 3 m 以下のカバレッジ率にて 99% 及び 94.7% であった。提案方式は、キー FOB までの測距機能を有し、グローバル無線規定への準拠、10 m のカバレッジ、低消費電力の条件を満足する。リレーアタック対策を備えた RKE システムに適す唯一の無線測距と結論付けられる。				

Thesis Abstract

No. _____

Registration Number	☒ "KOU" ☐ "OTSU" No. _____ *Office use only	Name	Ichiro Seto
Thesis Title Phase Detection based Two-way Ranging in Sub-GHz Band for Remote Keyless Entry Systems			
Thesis Summary Passive remote keyless entry systems have penetrated the vehicular market due to their convenience. However, its vulnerability against relay attacks exploiting the wireless channel is a serious threat. One of the prominent countermeasures is to estimate the distance between the key fob and the vehicle. Taking into account considerations such as ranging performance, radio regulations, usability, and power consumption for battery operation, we need to devise a suitable approach to achieve these practical specifications. We propose a novel two-way ranging based on phase detection in the sub-GHz band utilizing narrow bandwidth. We extend the concept of two-way ranging studied in time-of-flight into phase detection. Applying eight sequences for two-way ranging, the ranging can provide sufficient accuracy for distance estimation with high tolerance to asynchronous clock offset between a pair of transceiver devices. Under the condition of ranging with narrow bandwidth, we also propose a novel compensation scheme to mitigate multipath effects on distance estimation. We present the operation principle and theoretical performance analysis under a two-path model of radio propagation and additive white Gaussian noise. In field experiments of 6 m x 6 m spaces with prototyping transceiver devices, we validate the ranging accuracy in the distance estimation. In the theoretical analysis and the field experiment, the Mean Absolute Errors (MAE) were 0.65 meter and 1.13 meters; the coverage area within 3-meters error was 99.0 percent and 94.7 percent, respectively. The proposed ranging produces performance in confirming if the key fob is within 3 meters of the vehicle, which can offer a countermeasure to relay attacks. To the best of our knowledge, the proposed solution is the first to meet sufficient ranging performance while suiting the required conditions of remote keyless entry systems which are global radio regulations, comfortable usability with 10-meters coverage, and low power consumption for practical coin-battery operations.			