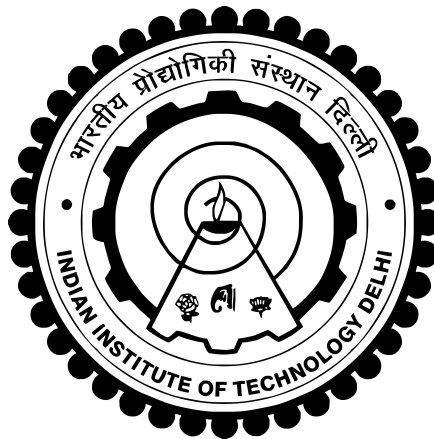


INVERSE STOCHASTIC FILTERING FOR INVERSE COGNITION IN COUNTER-ADVERSARIAL SYSTEMS

HIMALI SINGH



DEPARTMENT OF ELECTRICAL ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY DELHI
FEBRUARY 2025

©Indian Institute of Technology Delhi (IITD), New Delhi, 2025

Inverse Stochastic Filtering for Inverse Cognition in counter-adversarial systems

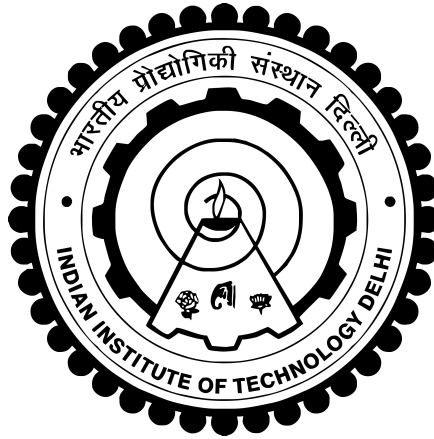
by

HIMALI SINGH

DEPARTMENT OF ELECTRICAL ENGINEERING

Submitted

in fulfillment of the requirements of the degree of Doctor of Philosophy
to the



INDIAN INSTITUTE OF TECHNOLOGY DELHI
FEBRUARY 2025

Dedicated to

The One who has been and will always be there

ℰ

The One whose selflessness made everything possible

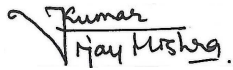
Certificate

This is to certify that the work presented in this thesis entitled "**Inverse Stochastic Filtering for Inverse Cognition in counter-adversarial systems**" being submitted by **Ms. Himali Singh** to Department of Electrical Engineering, **Indian Institute of Technology Delhi**, for the award of the degree of **Doctor of Philosophy** is the record of the bona-fide research work carried out by her under our supervision. In our opinion, the thesis has reached the standards fulfilling the requirements of the regulations relating to the degree.

The results contained in this thesis have not been submitted either in part or in full to any other university or institute for the award of any degree or diploma.



(Dr. Arpan Chattopadhyay)
Assistant Professor
Department of Electrical Engineering
Indian Institute of Technology Delhi



(Dr. Kumar Vijay Mishra)
United States DEVCOM Army Research Laboratory
Adelphi, MD 20783 USA.

Acknowledgements

Firstly, I wish to express my heartfelt gratitude to my thesis supervisors, **Dr. Arpan Chattopadhyay** and **Dr. Kumar Vijay Mishra**, for their exceptional guidance and support throughout this journey. Their proactive supervision, enlightening discussions, and unwavering support have been crucial to my work. Dr. Chattopadhyay's passion for knowledge has been a great source of inspiration. The courses he offered on 'Detection & Estimation Theory' and 'Stochastic Control & Reinforcement Learning' were invaluable learning experiences, and his rigorous mathematical approach laid the groundwork for my research. Dr. Mishra's constant encouragement, positive outlook, and insightful advice greatly motivated me to enhance my work and realize my full potential. His expertise was a significant asset to my research.

I am also deeply grateful to my SRC members, Prof. Lalan Kumar, Prof. Sandeep Kumar, Prof. Prabhu Babu, and the PMRF Annual Review committee for their constructive feedback and suggestions throughout my research.

My deepest thanks go to my family—my mother, Mrs. Seema Singh; my father, Dr. Yashvir Singh; and my brother, Mr. Yugal Deep Singh—for their unwavering support, understanding, and encouragement. Their sacrifices and belief in me, especially my mother's, have been pivotal to my achievements.

Lastly, I would like to acknowledge my friends and colleagues for their support and for making my time at I.I.T. Delhi both enjoyable and memorable. I am also grateful to the Almighty for guiding me through this journey and making the completion of my Ph.D. possible.



Himali Singh

Abstract

Recent advances in cognitive and counter-adversarial systems with the ability to infer their adversary’s beliefs have garnered significant research interest in inverse filtering from a Bayesian perspective. Such counter-adversarial systems have potential applications where an autonomous system interacts with its environment, learns relevant information about it, and then adapts itself to achieve its goals optimally. An important example is the *inverse cognition* problem in cognitive radar-target dynamics. A cognitive radar adapts its waveform, beam pattern, and other parameters in real-time to accurately localize its target. An intelligent target can employ these inverse filtering results to evade detection and even deceive the adversarial radar. In this setting, a cognitive adversary or ‘attacker’ tracks its target of interest using a stochastic framework such as a Kalman filter (KF). The target or ‘defender’ then employs another *inverse* stochastic filter to infer the forward filter’s estimates of the defender’s state computed by the attacker. For instance, recently, *inverse KF* (I-KF) has been developed to predict the attacker’s future steps by estimating its (forward) KF’s estimates. Existing works on inverse stochastic filtering and inverse cognition consider either linear Gaussian or finite state-space models, which limits their applicability in many practical engineering problems. Hence, in this dissertation, we study inverse filtering in the general non-linear non-Gaussian system framework. However, the non-linear Bayesian filtering is an intractable problem that necessitates sub-optimal approximation techniques. In our work, we develop inverse non-linear filters using different sub-optimal filtering approaches. We further study the theoretical performance guarantees for the developed filters. Finally, several numerical experiments demonstrate the estimation performance of our methods using the recursive Cramér-Rao lower bound and non-credibility index (NCI) as benchmarks.

In the inverse non-linear filtering context, we first investigate the extended KF (EKF), which uses Taylor series expansion to extend the standard KF to non-linear dynamics. To this end, we develop inverse EKF (I-EKF) for non-linear systems with and without unknown exogenous inputs. We then provide theoretical stability guarantees for I-EKF in the exponential-mean-squared-boundedness sense using both bounded non-linearity and unknown matrix approaches. In particular, the inverse filter is stable under mild system-level conditions, provided that the forward filter is stable. Additionally, we prove that I-EKF is a conservative estimator, i.e., I-EKF’s estimated error covariance upper bounds its true value. In the process, we also obtain I-KF for linear systems with unknown inputs and provide sufficient conditions for its asymptotic stability. Our I-EKF can be further modified using the maximum correntropy criterion (MCC) to tackle non-Gaussian noises. However, the standard EKF technique has several disadvantages. The EKF, and hence I-EKF, performs poorly when the dynamic system is highly non-linear, is sensitive to initialization, and may even fail completely. These drawbacks of EKF have led to the development of several advanced variants to enhance estimation accuracy, stability, and practical feasibility. Hence, we generalize our I-EKF formulation to highly non-linear models and develop inverse second-order EKF (I-SOEKF), inverse Gaussian-sum EKF (I-GS-

EKF), and inverse dithered EKF (I-DEKF). These advanced I-EKF variants overcome some of I-EKF's limitations and provide improved performance, depending on the system. Finally, we derive I-SOEKF's theoretical stability guarantees using the bounded non-linearity approach. Our numerical experiments further suggest that an advanced inverse filter may provide better performance at the cost of computational efforts, even when assuming an incorrect forward filter employed by the attacker.

Despite its simplicity, EKF suffers from linearization errors in highly non-linear applications, which can be efficiently handled with derivative-free sigma-point KFs (SPKFs). In contrast to EKF, SPKFs use function evaluation at a deterministic set of sigma points to approximate the statistics of a random variable under non-linear transformation. In light of this, we explore the unscented transform method or, equivalently, statistical linearization technique and develop inverse unscented KF (I-UKF). However, practical systems often involve continuous-time state evolution or complex-valued states and observations. Hence, we generalize our I-UKF theory to obtain continuous-discrete and complex I-UKFs for inverse filtering applications. We also investigate enhanced SPKFs based on efficient numerical integration techniques and develop inverse cubature KF (I-CKF), inverse quadrature KF (I-QKF), and inverse cubature-quadrature KF (I-CQKF). Finally, we derive sufficient conditions for the stochastic stability of the aforementioned inverse SPKFs using the unknown matrix approach. In the process, we also obtain hitherto unreported general stability results for forward UKF and CKF. Inverse SPKFs, like I-EKFs, have been shown to be conservative estimators.

Our inverse EKFs and SPKFs adopt the inverse filtering framework of I-KF and assume that both the attacker and defender agents have perfect knowledge of the system model. However, in practice, agents employing stochastic filters often lack prior system model information. In this context, we address the unknown system model case by developing reproducing kernel Hilbert space (RKHS)-based EKF and UKF to learn system parameters and estimate the state simultaneously. Our RKHS-based filters can be employed by both the attacker and defender to estimate the defender's state and the attacker's state estimate, respectively. While both RKHS-based filters adopt an online approximate Expectation Maximization (EM) algorithm to learn the system parameters, the expectations under non-linear transformations in RKHS-EKF and RKHS-UKF are computed using Taylor series-based linearization and the unscented transform, respectively. Our numerical experiments further demonstrate that RKHS-UKF outperforms RKHS-EKF in terms of estimation accuracy. Finally, we provide theoretical stability guarantees for the developed RKHS-based filters using the unknown matrix approach. In our RKHS-based KFs, the recursive Bayesian state estimation framework is extended to unknown systems by coupling an additional EM-based parameter update step with the EKF/UKF recursions. As a result, we are able to examine their stochastic stability, which is not possible with other kernel-based methods reported in the literature.

The sub-optimal non-linear filtering approaches discussed so far assume additive Gaussian system models and/or locally approximate the non-linear dynamics at the state estimates. Consequently, these methods are difficult to implement in many practical scenarios. Hence, we also consider the global but computationally expensive sequential Monte Carlo (SMC) filtering approach to develop inverse filters for general non-linear and non-Gaussian systems. In this context,

we first develop an inverse particle filter (I-PF) that assumes perfect system model information. Unlike EKF and SPKFs, which assume a Gaussian posterior density, the PF framework uses MC methods to approximate arbitrary posterior distributions. However, the particles in PFs are not statistically independent, and standard convergence results for MC methods based on central limit theorems are not applicable. In this work, we study the convergence of the developed I-PF in the L^4 -sense and show that under mild system-level conditions, our I-PF’s estimates converge to the optimal inverse filter’s estimates. Despite the fact that the Gaussianity assumption restricts practical applications, it frequently presents a trade-off between accuracy and ease of implementation. Hence, we next explore the application of SMC techniques to Gaussian systems and develop inverse Gaussian PF (I-GPF) and inverse ensemble KF (I-EnKF). GPFs employ sequential importance sampling (SIS) to approximate the mean and covariance of a Gaussian posterior density. The EnKF, on the other hand, is an MC approximation of the standard KF but has been successfully applied to a wide range of extremely high-dimensional and non-linear problems. Our I-GPF and I-EnKF can further efficiently handle non-Gaussian noises with suitable modifications. Finally, we introduce the differentiable I-PF, differentiable I-EnKF, and RKHS-EnKF methods, leveraging SMC techniques to tackle situations where the defender lacks knowledge of the system information.

सारांश

हाल ही में, संज्ञानात्मक और प्रतिकूल परिस्थितियों का सामना करने वाले सिस्टम, जो अपने विरोधी की मान्यताओं का अनुमान लगाने में सक्षम हैं, ने बेयसियन परिप्रेक्ष्य से व्युत्क्रम निस्पंदन (इनवर्स फिल्टरिंग) में महत्वपूर्ण शोध रुचि प्राप्त की है। ऐसे प्रतिकूल परिस्थितियों का सामना करने वाले सिस्टम उन अनुप्रयोगों में महत्वपूर्ण भूमिका निभा सकते हैं, जहाँ एक स्वायत्त प्रणाली अपने परिवेश के साथ बातचीत करती है, प्रासंगिक जानकारी सीखती है और फिर अपने लक्ष्यों को सर्वोत्तम रूप से प्राप्त करने के लिए स्वयं को अनुकूलित करती है। इसका एक महत्वपूर्ण उदाहरण संज्ञानात्मक रडार-लक्ष्य गतिकी में व्युत्क्रम संज्ञान (इनवर्स कॉग्निशन) समस्या है। एक संज्ञानात्मक रडार अपने लक्ष्य को सटीक रूप से स्थानीयकृत करने के लिए अपने वेवफॉर्म, बीम पैटर्न और अन्य मापदंडों को वास्तविक समय में समायोजित करता है। एक बुद्धिमान लक्ष्य इन व्युत्क्रम निस्पंदन परिणामों का उपयोग करके पहचान से बच सकता है और यहां तक कि प्रतिकूल रडार को धोखा भी दे सकता है। इस परिप्रेक्ष्य में, एक संज्ञानात्मक प्रतिद्वंद्वी या 'हमलावर' कलमैन फिल्टर (KF) जैसे स्तोकास्टिक फ्रेमवर्क का उपयोग करके अपने लक्षित उद्देश्य को ट्रैक करता है। इसके उत्तर में, लक्ष्य या 'रक्षक' एक अन्य व्युत्क्रम स्तोकास्टिक फिल्टर का उपयोग करता है, जिससे वह हमलावर द्वारा अपने अवस्था का अनुमान लगाने वाले फॉरवर्ड फिल्टर के अनुमानों को समझ सकता है। उदाहरण के लिए, हाल ही में इनवर्स KF (I-KF) विकसित किया गया है, जो हमलावर के भविष्य के कदमों की भविष्यवाणी करने के लिए उसके (फॉरवर्ड) KF के अनुमानों का अनुमान लगाता है। अब तक के अधिकांश शोध कार्य केवल रैखिक गॉसियन (लाइनियर-गॉसियन) या सीमित स्थिति-अंतराल (फिनाइट स्टेट-स्पेस) मॉडल तक सीमित रहे हैं, जिससे उनकी व्यावहारिक इंजीनियरिंग समस्याओं में उपयोगिता सीमित हो जाती है। इसीलिए, इस शोध में, हम सामान्य गैर-रेखीय (नॉन-लाइनियर) और गैर-गॉसियन प्रणाली संरचना में व्युत्क्रम निस्पंदन का अध्ययन करते हैं। हालाँकि, गैर-रेखीय बेयसियन निस्पंदन गणनात्मक रूप से जटिल समस्या है, जिसके लिए उप-इष्टतम (सब-ऑप्टिमल) सन्निकटन तकनीकों की आवश्यकता होती है। इस शोध में, हम विभिन्न उप-इष्टतम निस्पंदन विधियों का उपयोग करके व्युत्क्रम गैर-रेखीय फिल्टर विकसित करते हैं। साथ ही, विकसित फिल्टरों के सैद्धांतिक प्रदर्शन गारंटी का अध्ययन करते हैं। इसके अलावा, कई संख्यात्मक प्रयोगों के माध्यम से हमारी विधियों के अनुमान प्रदर्शन का मूल्यांकन किया जाता है, जिसमें पुनरावृत्त क्रैमर-राव निचली सीमा (Cramér-Rao Lower Bound) और गैर-विश्वसनीयता सूचकांक (Non-Credibility Index, NCI) जैसे मापदंडों का उपयोग किया जाता है।

व्युत्क्रम गैर-रेखीय निस्पंदन के संदर्भ में, सबसे पहले हम विस्तारित कलमैन फिल्टर (EKF) की जांच करते हैं, जो टेलर श्रृंखला विस्तार का उपयोग करके मानक KF को गैर-रेखीय गतिकी तक विस्तारित करता है। इस कार्य में, हम अज्ञात वाह्य इनपुट्स के साथ और बिना, गैर-रेखीय प्रणालियों के लिए इनवर्स EKF (I-EKF) विकसित करते हैं। इसके अलावा, हम I-EKF की स्थिरता की सैद्धांतिक गारंटी प्रदान करते हैं और यह दर्शाते हैं कि यदि फॉरवर्ड फिल्टर स्थिर है, तो व्युत्क्रम फिल्टर भी स्थिर रहेगा। इसके अतिरिक्त, हम यह सिद्ध करते हैं कि I-EKF एक संरक्षित (conservative) अनुकरणक है, अर्थात् I-EKF द्वारा अनुमानित त्रुटि सह-सांयोजन (error covariance) इसकी वास्तविक मान से अधिकतम सीमा तक बंधित रहता है। इस प्रक्रिया में, हम अज्ञात इनपुट वाले रैखिक प्रणालियों के लिए I-KF भी प्राप्त करते हैं और इसकी दीर्घकालिक (asymptotic) स्थिरता के लिए पर्याप्त शर्तें प्रदान करते

हैं। हमारे I-EKF को अधिकतम कोर्रेंट्रोपी मापदंड (MCC) का उपयोग करके संशोधित किया जा सकता है, जिससे यह गैर-गॉसियन शोर (non-Gaussian noises) को प्रभावी रूप से संभाल सके। EKF की कुछ सीमाओं को दूर करने के लिए, हम I-EKF को अधिक उन्नत गैर-रेखीय मॉडल तक सामान्यीकृत करते हैं और इनवर्स सेकंड-ऑर्डर EKF (I-SOEKF), इनवर्स गॉसियन-सम EKF (I-GSEKF), और इनवर्स डिथर्ड EKF (I-DEKF) विकसित करते हैं। ये उन्नत I-EKF प्रकार I-EKF की कुछ सीमाओं को दूर करते हैं और प्रणाली के आधार पर बेहतर प्रदर्शन प्रदान करते हैं। अंततः, हम सीमित गैर-रेखीयता (bounded non-linearity) दृष्टिकोण का उपयोग करके I-SOEKF की सैद्धांतिक स्थिरता गारंटी प्राप्त करते हैं। हमारे संख्यात्मक प्रयोग यह भी संकेत देते हैं कि एक उन्नत व्युत्क्रम फ़िल्टर, भले ही हमलावर द्वारा उपयोग किए गए फ़ॉरवर्ड फ़िल्टर की धारणा गलत हो, फिर भी अतिरिक्त गणनात्मक प्रयासों की कीमत पर बेहतर प्रदर्शन प्रदान कर सकता है।

हालांकि EKF सरल है, यह अत्यधिक गैर-रेखीय अनुप्रयोगों में रैखिकीकरण (लिनियराइज़ेशन) त्रुटियों के कारण प्रभावित हो सकता है। इस समस्या को सुलझाने के लिए, हम सिग्मा-पॉइंट कलमैन फ़िल्टर (SPKF) दृष्टिकोण अपनाते हैं, जो यादृच्छिक चर (रैंडम वैरिएबल) के सांख्यिकीय अनुमान को बेहतर ढंग से संभालता है। इस आधार पर, हम इनवर्स अनसैटेड KF (I-UKF) विकसित करते हैं और इसे सतत-विच्छिन्न (Continuous-Discrete) और जटिल-मान (Complex-Valued) प्रणालियों तक विस्तारित करते हैं। इसके अलावा, हम कुबेटर KF (I-CKF), क्वाड्रेटर KF (I-QKF) और कुबेटर-क्वाड्रेटर KF (I-CQKF) विकसित करते हैं और इनके स्थिरता गुणों का विश्लेषण करते हैं। अंततः, हम अज्ञात मैट्रिक्स दृष्टिकोण का उपयोग करके उपर्युक्त व्युत्क्रम SPKF की स्तोकास्टिक स्थिरता के लिए पर्याप्त शर्तें प्राप्त करते हैं। इस प्रक्रिया में, हम अब तक अप्रकाशित फ़ॉरवर्ड UKF और CKF के सामान्य स्थिरता परिणाम भी प्राप्त करते हैं। I-EKF की तरह, व्युत्क्रम SPKF भी संरक्षित (conservative) अनुकरणक सिद्ध हुए हैं।

हमारे इनवर्स EKF और SPKF फ़िल्टर इस धारणा पर आधारित हैं कि हमलावर और रक्षक दोनों के पास प्रणाली मॉडल की पूरी जानकारी होती है। हालांकि, व्यावहारिक परिस्थितियों में, एजेंटों को अक्सर पूर्ण प्रणाली मॉडल की जानकारी नहीं होती। इस समस्या के समाधान के लिए, हम रिप्रोड्यूसिंग कर्नेल हिल्बर्ट स्पेस (RKHS) आधारित EKF और UKF विकसित करते हैं, जो प्रणाली के पैरामीटर सीखने और स्थिति का अनुमान लगाने में सक्षम हैं। इस संदर्भ में, हम ऑनलाइन अनुमानित अपेक्षा-अधिकतमकरण (EM) एल्गोरिदम का उपयोग करते हैं, जो प्रणाली के पैरामीटर को अद्यतन करने के लिए EKF/UKF पुनरावृत्तियों (रिकर्सन) के साथ जोड़ा जाता है। हमारे RKHS-आधारित फ़िल्टर का उपयोग हमलावर और रक्षक दोनों द्वारा किया जा सकता है, जहां रक्षक की स्थिति का अनुमान हमलावर द्वारा और हमलावर की स्थिति का अनुमान रक्षक द्वारा लगाया जाता है। दोनों RKHS-आधारित फ़िल्टर सिस्टम के पैरामीटर सीखने के लिए एक ऑनलाइन अनुमानित एक्सपेक्टेड मैक्सिमाइज़ेशन (EM) एल्गोरिदम अपनाते हैं। हालांकि, RKHS-EKF और RKHS-UKF में गैर-रेखीय रूपांतरणों के अंतर्गत अपेक्षाएं क्रमशः टेलर श्रृंखला-आधारित रैखिकीकरण और अनसैटेड ट्रांसफॉर्म का उपयोग करके गणना की जाती हैं। हमारे प्रयोगों से पता चलता है कि RKHS-UKF, RKHS-EKF की तुलना में बेहतर अनुमान सटीकता प्रदान करता है। अंततः, हम विकसित किए गए RKHS-आधारित फ़िल्टरों के लिए अज्ञात मैट्रिक्स दृष्टिकोण का उपयोग करके सैद्धांतिक स्थिरता गारंटी प्रदान करते हैं। हमारे RKHS-आधारित केएफ़ (KFs) में, पुनरावृत्त बायेसियन अवस्था अनुमान ढांचे को अज्ञात प्रणालियों तक विस्तारित किया जाता है, जिसमें EKF/UKF पुनरावृत्तियों के साथ एक अतिरिक्त

EM-आधारित पैरामीटर अपडेट चरण जोड़ा जाता है। परिणामस्वरूप, हम उनकी स्तोकास्टिक स्थिरता की जांच करने में सक्षम होते हैं, जो साहित्य में रिपोर्ट की गई अन्य कर्नेल-आधारित विधियों के साथ संभव नहीं है।

अब तक चर्चा किए गए उप-इष्टतम गैर-रेखीय निस्पंदन दृष्टिकोण आमतौर पर अतिरिक्त गॉसियन मॉडल मानते हैं या स्थानीय रूप से गैर-रेखीय गतिकी को अनुमानित करते हैं, जिससे उनकी व्यावहारिकता सीमित हो जाती है। इसलिए, हम अनुक्रमिक मॉंटे-कार्लो (SMC) निस्पंदन तकनीकों का उपयोग करके व्युत्क्रम फ़िल्टर विकसित करते हैं, जो अधिक सामान्य गैर-रेखीय और गैर-गॉसियन प्रणालियों पर लागू किए जा सकते हैं। इस दृष्टिकोण में, हम पहले इनवर्स पार्टिकल फ़िल्टर (I-PF) विकसित करते हैं, जो संपूर्ण प्रणाली मॉडल की जानकारी मानता है। EKF और SPKF के विपरीत, जो गॉसियन पश्च घनत्व (Gaussian posterior density) को मानते हैं, PF फ्रेमवर्क मनमाने पश्च वितरणों (arbitrary posterior distributions) के सन्निकटन के लिए MC विधियों का उपयोग करता है। हालांकि, PF में कण (particles) सांख्यिकीय रूप से स्वतंत्र नहीं होते हैं, और केंद्रीय सीमा प्रमेय (central limit theorem) पर आधारित MC विधियों के मानक अभिसरण (convergence) परिणाम लागू नहीं होते। इस कार्य में, हम विकसित किए गए I-PF के L4-सेंस में अभिसरण का अध्ययन करते हैं और दिखाते हैं कि हल्की प्रणाली-स्तरीय (system-level) शर्तों के तहत, हमारे I-PF के अनुमान इष्टतम व्युत्क्रम फ़िल्टर (optimal inverse filter) के अनुमानों से मेल खाते हैं। हालांकि गॉसियनता (Gaussianity) की धारणा व्यावहारिक अनुप्रयोगों को सीमित करती है, यह अक्सर सटीकता और कार्यान्वयन में आसानी के बीच एक समझौता प्रस्तुत करती है। इसलिए, हम अगला कदम बढ़ाते हुए गॉसियन प्रणालियों पर SMC तकनीकों के अनुप्रयोग का अध्ययन करते हैं और इनवर्स गॉसियन PF (I-GPF) तथा इनवर्स एंसेंबल KF (I-EnKF) विकसित करते हैं। GPFs अनुक्रमिक महत्व सैंपलिंग (SIS) का उपयोग करके गॉसियन पश्च घनत्व (Gaussian posterior density) के माध्य और सह-सांयोजन (covariance) का सन्निकटन करते हैं। दूसरी ओर, EnKF एक मानक KF का MC सन्निकटन है, लेकिन इसे अत्यधिक उच्च-आयामी और गैर-रेखीय समस्याओं की एक विस्तृत श्रृंखला में सफलतापूर्वक लागू किया गया है। हमारा I-GPF और I-EnKF, उपयुक्त संशोधनों के साथ, गैर-गॉसियन शोर (non-Gaussian noises) को भी प्रभावी ढंग से संभाल सकता है। अंततः, हम विभेदनीय (differentiable) I-PF, विभेदनीय I-EnKF, और RKHS-EnKF विधियों को प्रस्तुत करते हैं, जो SMC तकनीकों का उपयोग करके उन परिस्थितियों से निपटने में सक्षम होते हैं जहां रक्षक (defender) के पास प्रणाली संबंधी जानकारी का अभाव होता है।

Table of Contents

Certificate	i
Acknowledgements	ii
Abstract	iii
List of Figures	ix
List of Tables	x
Abbreviations	xi
Notations	xii
1 Introduction	1
1.1 Inverse filtering and Inverse Cognition	2
1.2 Non-linear filtering	3
1.2.1 Extended KF and its variants	4
1.2.2 Sigma-point KFs	4
1.2.3 Sequential Monte-Carlo filters	5
1.2.4 Unknown system dynamics	6
1.3 Motivation and Contributions	7
1.4 Organization of the thesis	11
2 System model and Optimal inverse filter	13
2.1 System model	13
2.1.1 Systems with additive Gaussian noises	14
2.2 Optimal inverse filter	15
3 Inverse EKF and its variants	18
3.1 Inverse EKF	18
3.1.1 Filter formulation	18
3.1.2 Performance analyses	20
3.2 Inverse SOEKF	26
3.2.1 Filter formulation	26
3.2.2 Stability guarantees	28
3.3 Inverse Gaussian sum and dithered EKEs	30
3.3.1 Inverse GS-EKF	30
3.3.2 Inverse DEKF	32
3.4 Numerical experiments	32
3.4.1 FM demodulation with I-EKF, I-SOEKF and I-GS-EKF	34
3.4.2 Coordinate estimation with I-DEKF	36
3.5 Concluding remarks	37
4 Inverse filters for systems with unknown inputs	38
4.1 Inverse EKF with unknown input	39

4.1.1	I-EKF-without-DF	39
4.1.2	I-EKF-with-DF	41
4.2	Inverse KFs with unknown input	42
4.2.1	I-KF-without-DF	42
4.2.2	I-KF-with-DF	43
4.2.3	Stability analysis	45
4.3	Numerical experiments	45
4.3.1	I-KFs with unknown inputs	45
4.3.2	I-EKFs with unknown inputs	46
4.4	Concluding remarks	47
5	Inverse SPKFs	48
5.1	Inverse UKF	48
5.1.1	Filter formulation	48
5.1.2	Performance analyses	53
5.2	Inverse Cubature and Quadrature KFs	56
5.2.1	Inverse CKF	56
5.2.2	Inverse QKF	59
5.2.3	Inverse CQKF	60
5.3	Numerical experiments	61
5.3.1	FM demodulation with I-UKF, I-CKF and I-QKF	61
5.3.2	Vehicle reentry with I-UKF	63
5.3.3	Target tracking with I-CKF	64
5.3.4	Lorenz system with I-QKF and I-CQKF	65
5.4	Concluding remarks	67
6	RKHS-based KFs for unknown system dynamics	68
6.1	Filter formulations	68
6.1.1	Online approximate EM	69
6.1.2	RKHS-EKF	71
6.1.3	RKHS-UKF	73
6.2	Stability guarantees	76
6.3	Numerical experiments	79
6.3.1	FM demodulation with RKHS-EKF and RKHS-UKF	79
6.3.2	Lorenz system with RKHS-UKF	80
6.4	Concluding remarks	81
7	Inverse Particle and Ensemble Kalman filters	82
7.1	Inverse PF	82
7.1.1	Filter formulation	82
7.1.2	Convergence guarantees	86
7.2	Inverse Gaussian PF and Ensemble KF	88
7.2.1	Inverse GPF	88
7.2.2	Inverse EnKF	89
7.2.3	Non-Gaussian systems	91
7.3	Unknown system dynamics	93
7.3.1	Differentiable I-PF	93
7.3.2	Differentiable I-EnKF and RKHS-EnKF	95
7.4	Numerical experiments	96
7.4.1	1-D non-linear system with I-PF, I-GPF and I-EnKF	96
7.4.2	Bearing only tracking with I-PF and I-GPF	97

7.4.3	Van der Pol oscillator with I-EnKF	99
7.4.4	One-dimensional heat conduction with I-EnKF	99
7.5	Concluding remarks	101
8	Conclusions and Future scope	102
8.1	Conclusions	102
8.2	Future scope of work	104
References		105
A	Proofs for I-EKF's and I-SOEKF's performance guarantees	119
A.1	Proof of Theorem 3.1	119
A.2	Proof of Theorem 3.2	120
A.3	Proof of Theorem 3.4	121
A.4	Proof of Theorem 3.5	121
A.5	Proof of Theorem 3.6	122
A.5.1	Preliminaries	122
A.5.2	Proof of the theorem	125
A.6	Proof of Theorem 3.7	125
B	Proofs for forward and inverse unknown-input filters	127
B.1	Proof of forward EKF-without-DF recursions	127
B.1.1	Recursive solutions for extended state	128
B.1.2	Forward EKF-without-DF recursions	129
B.2	Proof of Theorem 4.1	133
C	Proof for I-UKF's stability	134
C.1	Proof of Theorem 5.2	134
C.1.1	Stochastic stability of augmented state UKF	134
C.1.2	Preliminaries	135
C.1.3	Proof of the theorem	136
C.1.4	Proofs of claims	137
D	Proof for RKHS-UKF's stability	140
D.1	Proof of Theorem 6.1	140
E	Proofs for I-PF's formulation and convergence	142
E.1	Proof of eqs. (7.2) and (7.3)	142
E.2	Proof of Theorem 7.1	142
E.2.1	Preliminaries	143
E.2.2	Proof of the theorem	147
List of Publications		152
Brief Bio-data of Author		153

List of Figures

2.1	Graphical representation of the defender-attacker interaction.	14
3.1	AMSE and RCRLB for forward and inverse filters: (a) EKF and SOEKF; (b) EKF and GS-EKF (I-GS-EKF-2 and I-GS-EKF-5, respectively, for $\bar{l} = 2$ and 5); mismatched (c) I-EKF and I-SOEKF; and (d) I-EKF and I-GS-EKF. The assumptions of different inverse filters are detailed in Table 3.1.	34
3.2	Absolute error and RCRLB for forward and inverse EKF as well as DEKF. I-DEKF-1 is the I-DEKF without considering the modified dithered function in the inverse filter formulation, while I-DEKF-2 considers the modified function. . .	36
4.1	Graphical representation of I-EKF-without-DF recursion at k -th time step. . .	40
4.2	Graphical representation of I-EKF-with-DF recursion at k -th time step. . . .	42
4.3	RMSE, AMSE, and RCRLB for forward and inverse filters (a) KF-without-DF; (b) KF-with-DF; and (c) AMSE for forward and inverse EKF with and without DF.	46
5.1	(a) Time-averaged RMSE and RCRLB, and (b) NCI for forward and inverse UKF for FM demodulator system.	62
5.2	Time-averaged RMSE for (a) forward filters, (b) I-UKFs, (c) I-CKFs, and (d) I-QKFs for FM demodulator system.	63
5.3	(a) Time-averaged estimation error and RCRLB, and (b) NCI for forward and inverse UKF for vehicle reentry system averaged over 100 runs.	64
5.4	Time-averaged estimation error and RCRLB of forward and inverse (a) CKFs for target tracking system (averaged over 250 runs); (b) UKFs, (c) QKFs, and (d) CQKFs for Lorenz system (averaged over 50 runs).	65
6.1	(a) Time-averaged RMSE, and (b) NCI for forward and inverse RKHS-EKF and UKF for FM demodulator system, compared with forward and inverse EKF. .	80
6.2	(a) Time-averaged RMSE, and (b) Time-averaged NCI for forward and inverse RKHS-UKF for Lorenz system, compared with forward and inverse UKF. . . .	81
7.1	Graphical representation of transformation of posterior distributions in I-PF. .	85
7.2	Time-averaged RMSE for (a) forward filters ($\mathbf{x}_k$ estimation), (b) forward EKF's $\hat{\mathbf{x}}_k$ estimation, (c) forward PF's $\hat{\mathbf{x}}_k$ estimation, (d) forward GPF's $\hat{\mathbf{x}}_k$ estimation, and (e) forward EnKF's $\hat{\mathbf{x}}_k$ estimation; and (f) NCI (for forward and inverse filters) for non-linear system example, compared with inverse EKF.	97
7.3	Relative error for (a) forward filters and forward EKF's $\hat{\mathbf{x}}_k$ estimation, and (b) forward PF's and forward GPF's $\hat{\mathbf{x}}_k$ estimation for bearing-only tracking system. .	98
7.4	Time-averaged RMSE for forward and inverse EnKF for (a) Van der Pol oscillator, compared with forward and inverse EKF; and (b) One-dimensional heat conduction system, compared with forward and inverse KF.	99

List of Tables

3.1	Summary of forward-inverse filters in Fig. 3.1(c)-(d)	35
5.1	Run time (in seconds) of different filters for target tracking system.	65
5.2	Run time (in seconds) of different filters for Lorenz system.	66
7.1	Summary of I-PF, I-GPF, and I-EnKF.	93
7.2	Run time (in seconds) of different filters for bearing-only tracking system.	98
7.3	Run time (in seconds) of different filters for Van der Pol oscillator system.	100
7.4	Run time (in seconds) of different filters for heat conduction example.	100

Abbreviations

ADF	Assumed density filtering
ALD	Approximate linear dependence
CKF/ I-CKF	Cubature Kalman filter/ Inverse CKF
CQKF/ I-CQKF	Cubature quadrature Kalman filter/ Inverse CQKF
DEKF/ I-DEKF	Dithered Extended Kalman Filter/ Inverse DEKF
DF	Direct feed-through
DPF	Differentiable Particle filter
EKF/ I-EKF	Extended Kalman filter/ Inverse EKF
EM	Expectation Maximization
EnKF/ I-EnKF	Ensemble Kalman filter/ Inverse EnKF
FM	Frequency modulation
GM/ GS	Gaussian Mixture/ Gaussian sum
GPF/ I-GPF	Gaussian Particle filter/ Inverse GPF
GS-EKF/ I-GS-EKF	Gaussian-sum EKF/ Inverse GS-EKF
GSPF/ I-GSPF	Gaussian-sum PF/ Inverse GSPF
HMMs	Hidden Markov Models
KF/ I-KF	Kalman filter/ Inverse KF
KKF	Kernel Kalman filter
KRLS/ Ex-KRLS	Kernel recursive least squares/ Extended KRLS
MC/ MCMC	Monte Carlo/ Markov chain MC
MCC	Maximum Correntropy criterion
ML	Machine learning
MSE/ MMSE	Mean-squared error/ Minimum MSE
NCI	Non-credibility index
NN/ RNN	Neural Network/ Recurrent NN
PF/ I-PF	Particle filter/ Inverse PF
P-MCMC	Particle MCMC
QKF/ I-QKF	Quadrature Kalman filter/ Inverse QKF
RCRLB	Recursive Cramer-Rao lower bound
RKHS	Reproducing kernel Hilbert space
RKHS-EKF/UKF/EnKF	RKHS-based EKF/UKF/EnKF
RL/ IRL	Reinforcement learning/ Inverse RL
RMSE/ AMSE	Root mean-squared error/ Time-averaged RMSE
SIS	Sequential Importance sampling
SLT	Statistical Linearization technique
SMC	Sequential Monte Carlo
SOEKF/ I-SOEKF	Second-order EKF/ Inverse SOEKF
SPKF	Sigma-point Kalman filter
UKF/ I-UKF	Unscented Kalman filter/ Inverse UKF

Notations

Parameter/ Function	Definition
k	Discrete-time index
$\mathbf{x}_k$	Defender's true state (n_x -dimensional vector) at k -th time instant
$\mathbf{u}_k$	Unknown exogenous control input (n_u -dimensional vector) at k -th time instant
$\mathbf{y}_k$	Attacker's observation (n_y -dimensional vector) of $\mathbf{x}_k$ at k -th time instant
$\hat{\mathbf{x}}_k$	Attacker's estimate of $\mathbf{x}_k$ given observations $\{\mathbf{y}_j\}_{1 \leq j \leq k}$ computed via a forward filter
$\hat{\mathbf{u}}_k$	Attacker's estimate of the unknown input via forward filter
Σ_k	Forward filter's estimate of error covariance for estimate $\hat{\mathbf{x}}_k$
$\mathbf{a}_k$	Defender's observation (n_a -dimensional vector) of $\hat{\mathbf{x}}_k$ at k -th time instant
$\hat{\hat{\mathbf{x}}}_k$	Defender's estimate of $\hat{\mathbf{x}}_k$ given observations $\{\mathbf{a}_j\}_{1 \leq j \leq k}$ and true states
$\hat{\hat{\mathbf{u}}}_k$	Defender's estimate of $\hat{\mathbf{u}}_k$ via inverse filter
$\bar{\Sigma}_k$	Inverse filter's estimate of error covariance for estimate $\hat{\hat{\mathbf{x}}}_k$
$[\mathbf{a}]_i / [\mathbf{A}]_{i,j}$	The i -th component of vector $\mathbf{a}$ / (i, j) -th component of matrix $\mathbf{A}$
$[\mathbf{A}]_{(i_1:i_2, j_1:j_2)}$	The sub-matrix of $\mathbf{A}$ consisting of rows i_1 to i_2 and columns j_1 to j_2
$[\mathbf{A}]_{(i,:)} / [\mathbf{A}]_{(:,j)}$	The i -th row / j -th column of matrix $\mathbf{A}$
$(\cdot)^{T/H}$	Transpose / Hermitian operation
$\ \cdot\ _2 / \ \cdot\ _{\mathbf{A}}$	l_2 norm / norm with respect to matrix $\mathbf{A}$ of a vector, i.e., $\mathbf{x}^T \mathbf{A} \mathbf{x}$
$\ \mathbf{x}\ _{\infty}$	l_{∞} norm of vector $\mathbf{x}$
$\text{Tr}/\text{det}/\text{rank}(\mathbf{A})$	Trace / Determinant / Rank of matrix $\mathbf{A}$
$\text{diag}(a_1, a_2, \dots, a_l)$	A ' $l \times l$ ' diagonal matrix with diagonal elements $a_1, a_2, \dots, a_l$
$\ \mathbf{A}\ / \ \mathbf{A}\ _{\infty}$	Spectral / maximum row sum norm of matrix $\mathbf{A}$
$\mathbf{A} \preceq \mathbf{B}$	The matrix $\mathbf{B} - \mathbf{A}$ is a positive semidefinite (p.s.d.) matrix
$\sqrt{\mathbf{A}}$	Square-root of matrix $\mathbf{A}$ such that $\mathbf{A} = \sqrt{\mathbf{A}} \sqrt{\mathbf{A}}^T$
$\nabla f / \frac{\partial f}{\partial \mathbf{x}}$	The $\mathbb{R}^{m \times n}$ Jacobian matrix for a function $f : \mathbb{R}^n \rightarrow \mathbb{R}^m$ or $\mathbb{R}^{n \times 1}$ gradient vector for $f : \mathbb{R}^n \rightarrow \mathbb{R}$
$\nabla^2 f / \frac{\partial^2 f}{\partial \mathbf{x}^2}$	The $\mathbb{R}^{n \times n}$ Hessian matrix for a function $f : \mathbb{R}^n \rightarrow \mathbb{R}$.
$\ f\ _{\infty}$	The supremum norm of the real-valued function $f(\cdot)$
$\delta(x - x_0)$	The Dirac-delta function in variable x centered at x_0
$\mathbf{I}_n / \mathbf{0}_{n \times m}$	$n \times n$ identity matrix / $n \times m$ all zero matrix
$\mathbf{I} / \mathbf{0}$	Identity matrix / all zero matrix of appropriate size
i.i.d.	Independent and identically distributed
p.d. / p.s.d.	Positive definite / positive semi-definite
$\mathbb{E}[\cdot]$	Expectation operation
$\mathcal{N}(\boldsymbol{\mu}, \mathbf{Q}) / \mathcal{N}(\mathbf{x}; \boldsymbol{\mu}, \mathbf{Q})$	Gaussian distribution with mean $\boldsymbol{\mu}$ and covariance matrix $\mathbf{Q}$
$\mathcal{U}[u_l, u_u]$	The uniform distribution over interval $[u_l, u_u]$
$\text{Cov}(\mathbf{x}) / \text{Cov}(\mathbf{x}, \mathbf{y})$	Covariance / cross-covariance matrix for random variables $\mathbf{x}$ and $\mathbf{y}$