Kurzfassung

Verteilte Mess- und Fusionsalgorithmen sind in öffentlichen Computernetzen immer häufiger anzutreffen und haben zu einer natürlichen Sorge um die Datensicherheit in diesen Umgebungen geführt. Ziel dieser Arbeit ist es, verallgemeinerbare Datenfusionsalgorithmen vorzustellen, die gleichzeitig strenge kryptographische Garantien für die Vertraulichkeit der Benutzerdaten bieten. Zwar gibt es bereits Fusionsalgorithmen, die ein gewisses Maß an Sicherheitsgarantien bieten, doch gehen diese in der Regel entweder auf Kosten der Allgemeinheit der Lösung oder es fehlen formale Sicherheitsbeweise. In dieser Arbeit werden neuartige kryptographische Konstrukte und modernste Verschlüsselungsverfahren verwendet, um formale Sicherheitsgarantien für neue und verallgemeinerte Datenfusionsalgorithmen zu entwickeln. Standard Kalman-Filter-Derivate werden modifiziert und bestehende Schemata abstrahiert, so dass neuartige kryptographische Begriffe, die die erforderliche Kommunikation erfassen, formalisiert werden können, während Simulationen eine Analyse der Praktikabilität liefern. Aufgrund der Allgemeingültigkeit der vorgestellten Lösungen wird eine Vielzahl von Anwendungen unterstützt, darunter autonome Fahrzeugkommunikation, intelligente Sensornetzwerke und verteilte Lokalisierung.