Reaktiver Schutz
vor Drohnen

Das Schützen von sicherheitskritischen Infrastrukturen vor sich ständig ändernden Bedrohungen ist im Zeitalter der Technik extrem wichtig. Der aufkommende Hype der Drohnen mit UHD-Kameras und intelligenter Flugunterstützung stellt für gewisse sensible Bereiche ein neues Risiko dar.

Das Thema Sicherheit hat in jüngster Zeit an Aktualität und Relevanz gewonnen. Durch potenzielle Gefahren im öffentlichen Raum ist das Sicherheitsgefühl zunehmend beeinträchtigt. Der Schutz von sicherheitskritischen Infrastrukturen, z. B. Atomkraftwerken, Flughäfen oder Gefängnissen, ist deshalb von grosser Bedeutung. Eine mögliche Bedrohung sind Quadcopter oder Multicopter – besser bekannt als Drohnen –, welche sich heutzutage enormer Beliebtheit erfreuen. Eine Drohne wie etwa die Phantom 4 von DJI kann über zwei Kilometer ferngesteuert werden und verfügt über eine UHD-Kamera, deren Aufnahmen der Pilot live anschauen kann. Somit ist es ein Leichtes, unbemerkt in sensible Areale einzudringen, um Schaden zu verursachen oder Drogen, Waffen und Handys in ein Gefängnis zu schmuggeln.

In Zusammenarbeit mit dem Berner Unternehmen COMLAB AG entwickeln wir am Institut für Risiko- und Extremwertanalyse i-REX der Berner Fachhochschule deshalb ein System zur reaktiven Drohnenabwehr.

Gezieltes Stören der Drohnensignale

Das Ziel ist es, die Kommunikation zwischen Drohne und Pilot so zu unterbinden, dass das Flugobjekt nicht in ein geschütztes Areal eindringen kann. Unser System basiert daher auf einer Detektion und einem gezielten Stören (Jamming) der Kommunikationssignale. Jamming ist ein Verfahren, welches die Kommunikation so stört, dass kein Informationsaustausch zwischen Sender und Empfänger mehr möglich ist. Verliert eine Drohne die Verbindung zum Piloten, kehrt sie entweder zu diesem zurück oder landet an Ort und Stelle.

Drohnen – ein wachsendes Sicherheitsrisiko

In einem ersten Schritt trennen morphologische Filter im Frequenzbereich die Kommunikationssignale der Drohne von den übrigen, unerwünschten Signalen. In einem zweiten Schritt werden die Drohnensignale, welche von mehreren Antennen gleichzeitig empfangen werden, mittels moderner Beamforming-Techniken ausgewertet. Diese geben Aufschluss über die Richtung, aus der ein Signal auf die Antennen trifft. Im Endeffekt kann so die Anflugrichtung einer Drohne geschätzt werden.

Die isolierten Drohnensignale und die bekannte Anflugrichtung ermöglichen es schliesslich, ein Störsignal in Richtung der Drohne zu senden. Somit werden gezielt nur Drohnensignale gestört, während andere Geräte in der Umgebung unbehindert bleiben.

Aktueller Projektstand und Ausblick

Die Detektion, die Schätzung der Anflugrichtung und das Jamming wurden in verschiedenen Projekten in Zusammenarbeit mit der Firma COMLAB AG erarbeitet, umgesetzt und validiert. Die Projekte werden durch die Inventus Bern Stiftung und die Kommission für Technologie und Innovation (KTI) finanziert. Aktuell können Drohnen vom Typ Phantom 3 und 4 von DJI auf drei Kilometer detektiert werden. Erste Tests zeigen, dass auch die Anflugrichtung korrekt geschätzt werden kann. Zudem funktioniert das Jamming der Kommunikation für die Drohnenmodelle der Hersteller DJI, 3D Robotics und Parrot.

Zurzeit sind wir daran, die Detektionsalgorithmen auf andere Drohnentypen auszubauen und die einzelnen Teilsysteme zu einem kompletten Funktionsmuster zusammenzufügen.

Autoren
– Jonas Schild, MSc in Elektrotechnik
– Bernhard Nyffenegger, BSc in Elektrotechnik
– Matthias Witschi, BSc in Elektrotechnik
Alle drei: Wissenschaftliche Mitarbeiter BFH

Kontakt
– rolf.vetter@bfh.ch
– irex.bfh.ch

Infos
– irex.bfh.ch