



Defense and Security



Contents

Defense and Security · 6 inventions

ODTÜ-87	Accountable Subgroup Multi-signature Scheme with Verifiable Group Setup	3
ODTÜ-89	Doppler Shift Based Distributed Drone Detection System	4
ODTÜ-133	Gunshot Detection From High Noise Multichannel Acoustic Data on Unmanned Aerial Vehicles	5
ODTÜ-145	System For Detection Of Non-Organic Object Transition In Shallow Waters Using Muons	6
ODTÜ-146	Naval Task Group Defense Planning Algorithm	7
ODTÜ-95	Quantum-Resistant Lattice-Based Accountable Subgroup Multi-Signature Scheme	8

Accountable Subgroup Multi-signature Scheme with Verifiable Group Setup

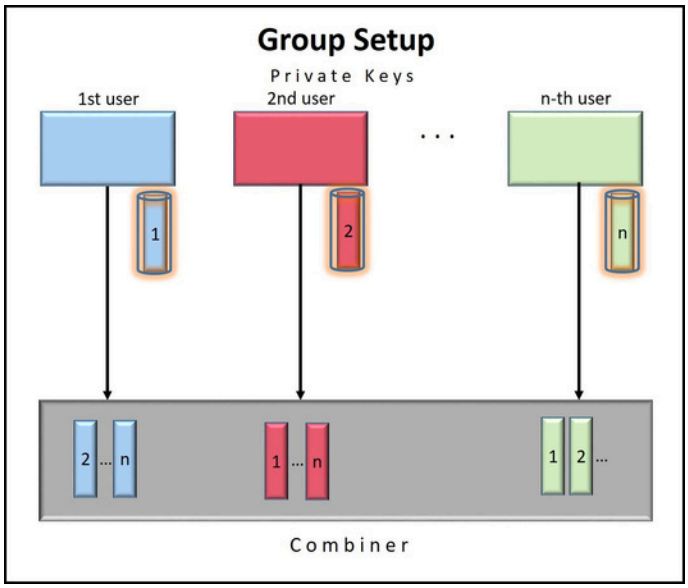
tto.metu.edu.tr
tto@metu.edu.tr

H2CI-3: Fast & Accountable Multi-Signature-3

Thanks to its unique group setup, the invention has the fastest signing and verification and the smallest signature size among known pairing-based ASM schemes.

Advantages

Fast signing: Requires 1 elliptic curve scalar multiplication.
Fast verification: Requires 2 elliptic curves pairing and n elliptic curve scalar multiplication operations.
Accountability: Signatures are computationally binding, hence they cannot be repudiated.
Constant signature size: Consists of only 1 elliptic curve group element, independent of the number of signers.
Flexible number of signers: The number of signers can be 1 to n.
(*) n: number of potential signers



The generated signature can be verified with public keys and identities of the signers.

Potential signers, authorized on behalf of an organization, can sign in a fast, secure and accountable fashion with the membership key they obtained following the group setup that they performed jointly with their private keys. This signature can be verified very quickly by anyone given signers' public identities.
Each potential signer in the organization signs the others' public identities individually with their private key and sends them to the combiner. She stores her own identity signature. Later, when she wants to sign a message, she signs it with her private key and add the identity signature she has recorded. She sends it to the combiner. The combiner aggregates the signatures he receives. Then, he combines the previously recorded identity signatures of the signers and aggregates it to the signature he has already created.

Doppler Shift Based Distributed Drone Detection System

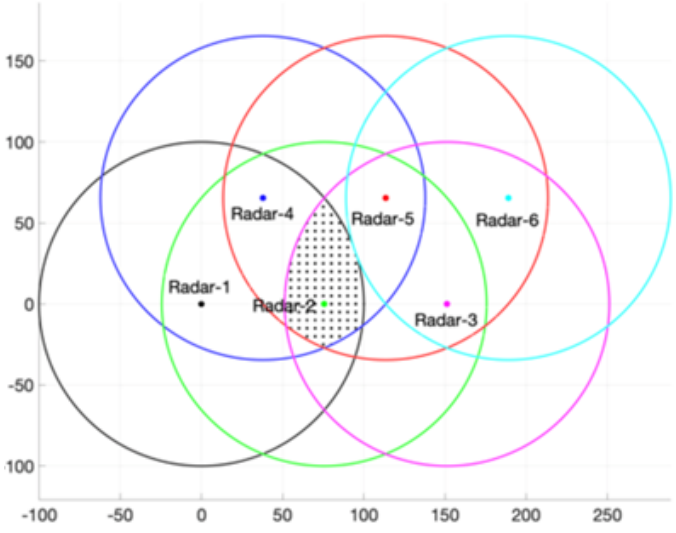
tto.metu.edu.tr
tto@metu.edu.tr

Distributed Drone Detection System

This invention focuses on a new method to detect drones in target dense environments. This method is based on using the Micro-Doppler signals caused by the motion of the propellers of the drones to detect drones and filtering other targets.

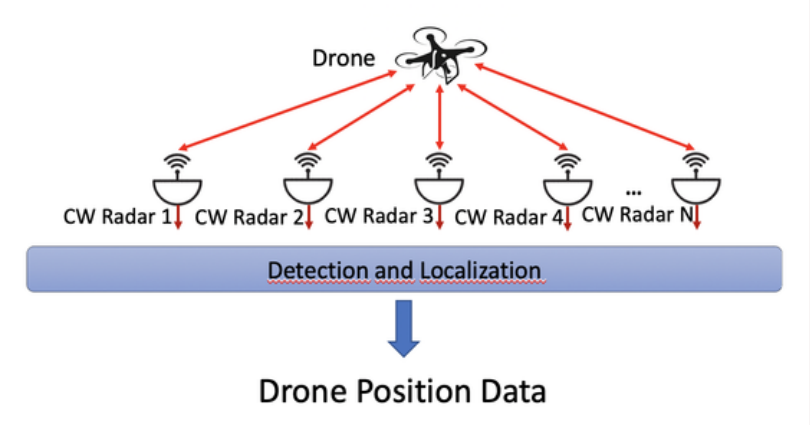
Advantages

Cost effective: Cost effective in radar coverage limited regions
Scalable: System architecture can be scaled according to the surveillance region
Graceful degradation: High reliability due to the usage of multiple distributed radars
Easy deployment: Easy deployment of multiple small radar systems compared to single conventional radar system
Operation in target dense environment: Operate in target dense environment using drone specific filtering.



Radar drone detection in radar-coverage limited and target dense environments like urban areas.

It is a challenging task both in terms of cost and performance for conventional radar systems to detect drones in radar-coverage limited and target dense environments. This invention defines a distributed, low power and cost effective radar drone detection solution. With this method, fusion of the data generated by distributed radar systems is used to detect and localize drones. With this distributed structure, radar blind zones can be prevented using proper deployment of radars.



ODTÜ-89

Gunshot Detection From High Noise Multichannel Acoustic Data on Unmanned Aerial Vehicles

tto.metu.edu.tr
tto@metu.edu.tr

Noise resistant gunshot detection on a drone

Advantages

Emphasizing the distant gunshot sounds instead of the noise close to the microphone array

Adaptive to different firearm types and nonstationary ego-noise without apriori information

Precise resolution in time and frequency, ability to tune / focus different signal characteristics

Support for different microphone array sizes and geometries

Low computational complexity for real-time processing.

Robustness even if some microphones in the array mulfunction.

Adaptive detection and imrovement of different muzzle blast and shock waves despite varying drone noise for gunshot localization.

Detecting impulsive event / gunshot in an adaptive way, taking advantage of multi-channel's coherence so as to improve SNR performance.

The offered Array Corelation Map (ACM) uses cross-correlations of array signals. The adaptivity feature is achieved by a specific selection method of the known CWT's scales.

System For Detection Of Non-Organic Object Transition In Shallow Waters Using Muons

tto.metu.edu.tr
tto@metu.edu.tr

Emins

Unlike its counterparts, It does not see organic objects with low false alarm rate.

Advantages

Detection with a low error margin.

Organic objects (for example, a pod of dolphins) cannot be seen by EMINS.

Being a passive system.

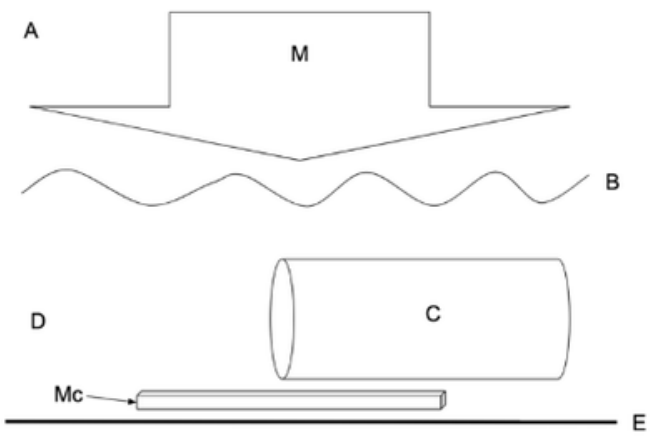
Measurement of parameters such as length, diameter and speed of the object that may be required for the identification of the object.

The system can be installed up to 70 meters sea depth.

It can be used as a warning system for secret submarine passages, especially in shallow waters such as the Straits.

The invention relates to a muon flux measuring device placed on the bottom or on a platform underwater for the detection of the passage and/or presence of non-organic objects (e.g. submarines) standing or moving underwater or on the water surface in shallow waters, and to a system that will give a live alarm as a result of a decrease in the instantaneous muon flux caused by the presence of the object.

It is possible to detect a decrease in the number of high-energy cosmic muons that can enter water, due to the high stopping power of steel.



A. Atmosphere

B. Surface of the sea, ocean, strait, river or natural or artificial lake

C. Non-organic object, e.g. submarine

D. The sea, ocean, strait, river or natural or artificial lake

E. Bottom of the sea, ocean, strait, river or natural or artificial lake

M. Atmospheric muon flux

Mc. Muon flux measuring device

ODTÜ-145

Naval Task Group Defense Planning Algorithm

tto.metu.edu.tr
tto@metu.edu.tr

NADP Algorithm

The invention is an algorithm that can produce an effective solution in a short time so that it can be used in real time.

Advantages

Real-time and effective (near-optimal) solutions can be obtained

Increasing the survival probability of platforms

Efficient use of defense resources

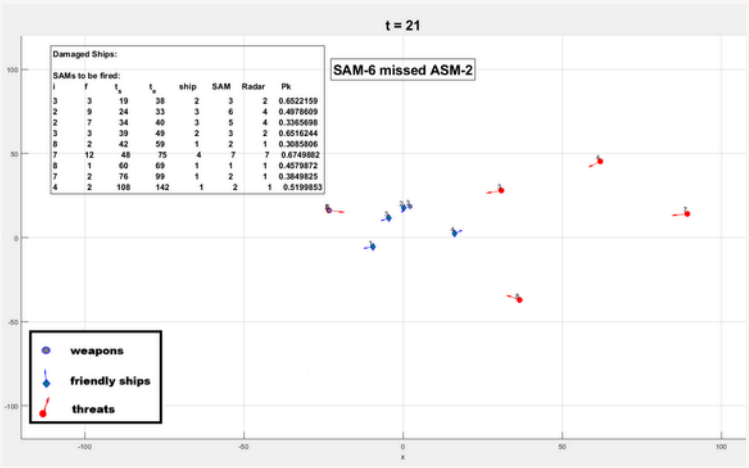
Scalability of the solution approach

Easy implementation

Providing engagement scheduling and ship routing decisions within the scope of naval task group air defense planning

The invention, Naval Air Defense Planning (NADP) Algorithm, comprises a solution approach developed for use in combat management systems to effectively protect naval task group platforms from air threats.

The NADP algorithm is an algorithm that optimizes and automates naval air defense planning. The algorithm covers the planning of defense resources in a very short time, including maneuver decisions of ships, assignment and timing of weapons and sensors against threats.



ODTÜ-146

Quantum-Resistant Lattice-Based Accountable Subgroup Multi-Signature Scheme

tto.metu.edu.tr
tto@metu.edu.tr

Quantum-Resistant ASM Scheme (vMS2)

The first quantum-resistant Accountable Subgroup Multi-Signature (ASM) scheme in the literature, securing signatures against quantum computers with a lattice-based design.

Advantages

Quantum resistance: Provides quantum-computer security that no existing ASM scheme offers.
Accountability: The identity of every signing subgroup member can be verified.
Flexible number of signers: No fixed threshold; any subgroup can sign together.
Wide application: Usable in finance, authentication, e-voting, blockchain and military systems.
Standards-compatible basis: Built on MS2, an extension of NIST PQC finalist Dilithium.

The first ASM solution to bring digital signatures to a quantum-resistant platform.

Existing classical ASM schemes (DLP/DHP-based) are vulnerable to quantum computers. vMS2 extends the MS2 multi-signature scheme with Verifiable Secret Sharing (VSS) and the Rejection Sampling protocol.
During group setup, each user selects a random polynomial based on their secret key, and membership keys are shared via VSS. Accountability is ensured by using the membership key in signature generation. Security relies on the Module-LWE and Module-SIS assumptions.