Detection and Localization of Multiple Spoofing

Attackers in Wireless Networks…

FAQ’s

**Detection** : is the extraction of particular information from a larger stream of information without specific cooperation from or synchronization with the sender.

**Localization:**

[Localization (algebra)](http://en.wikipedia.org/wiki/Localization_%28algebra%29), a formal way to introduce the "denominators" to a given ring or a module

[Localization of a category](http://en.wikipedia.org/wiki/Localization_of_a_category), adding to a category inverse morphisms for some collection of morphisms, constraining them to become isomorphisms

[Localization of a module](http://en.wikipedia.org/wiki/Localization_of_a_module), a construction to introduce denominators in a module M for a ring R

[Localization of a ring](http://en.wikipedia.org/wiki/Localization_of_a_ring), in abstract algebra, a systematic method of adding multiplicative inverses to a ring

[Localization of a topological space](http://en.wikipedia.org/wiki/Localization_of_a_topological_space), the localization of topological spaces at primes

[Localization theorem](http://en.wikipedia.org/wiki/Localization_theorem), theorem to infer the nullity of a function given only information about its continuity and the value of its integral.

[GSM localization](http://en.wikipedia.org/wiki/GSM_localization), a technique for determining the location of an active cell phone or wireless transceiver

[Robot localization](http://en.wikipedia.org/wiki/Robot_localization), figuring out robot's position in an environment .

[Sound localization](http://en.wikipedia.org/wiki/Sound_localization), a listener's ability to identify the location or origin of a detected sound.

**spoofing attack:** is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.

**Cryptographic Authentication:** A PKI ([Public Key Infrastructure](http://hitachi-id.com/concepts/public_key_infrastructure.html)) allows principals to authenticate one another using asymmetric encryption. A client (C) claiming to be a principal (P) authenticates to a server (S) as follows:

* S sends C a random number R.
* C encrypts R with his private key, and sends the result to S.
* S decrypts the result with P's public key.
* If the result matches R, then S knows that C must possess P's private key, and so C is assumed to be P.

**Conventional security:**

Attack Methods:differential cryptanalysis,linear cryptanalysis.

Security Analysis:Non-linearity.

SecurityStrengthening:indistinguishability,dedicated construction,decorrelation.

**spatial correlation**: the performance of wireless communication systems can be improved by having [multiple antennas](http://en.wikipedia.org/wiki/MIMO) at the transmitter and the receiver. The idea is that if the [propagation channels](http://en.wikipedia.org/wiki/Channel_%28communications%29) between each pair of transmit and receive antennas are [statistically independent](http://en.wikipedia.org/wiki/Independence_%28probability_theory%29) and [identically distributed](http://en.wikipedia.org/wiki/Identically_distributed), then multiple independent channels with identical characteristics can be created by [precoding](http://en.wikipedia.org/wiki/Precoding) and be used for either transmitting [multiple data streams](http://en.wikipedia.org/wiki/Spatial_multiplexing) or increasing the [reliability](http://en.wikipedia.org/wiki/Diversity_combining) (in terms of [bit error rate](http://en.wikipedia.org/wiki/Bit_error_rate)). In practice, the channels between different antennas are often correlated and therefore the potential multi antenna gains may not always be obtainable. This is called **spatial correlation.**