**Paper:** [**On Limitations of Friendly Jamming for Confidentiality**](https://ieeexplore.ieee.org/document/6547108)

**Summary:**

The paper speaks on debunking the idea that friendly jamming achieves proper confidentiality and access control. The confidentiality is said to be achieved by exposing the attacker to friendly jamming such that only the attacker’s channel is degraded to an extent that successful decoding of messages becomes infeasible for that channel. This paper analyses friendly jamming in scenarios where the jammer and message source are both physically very close and the attacker has 2 receiving antennas. It uses a new attack type that is based on multiple input multiple outputs. This allows the attacker to retrieve messages from distances feasible for an actual attack. This attack can be performed from various different locations even if the distance between jammer and shield is less than wavelength/2. In such cases it shows that the recovered signal for attacker has no attenuation. Authors of the paper conclude by saying friendly jamming cannot provide security guarantees in all settings.

**Strengths:**

1. The claim on limitations of friendly jamming is bolstered by the attack being performed when source and jammer is static as well as mobile since information can be recovered intermittently, sufficient to violate confidentiality.
2. This paper also experimentally highlights the fact that even if a high bit error rate is seen, just recovering a fragment of message is sufficient to retrieve the entire message, hence debunking the inefficiency of the method.
3. Various factors such as antenna placements, bit errors and multiple friendly jammers have been considered in raising the limitations of jammings
4. Another strong point portrayed is the fact that the experiments done didn’t restrict the type of jamming signal that the friendly jammer generated as the attack was helping in eliminating the jamming signal regardless of its type.

**Weaknesses:**

1. The optimal simulation used in the Line of Sight, using formation of isosceles trapezoid between the entities might be difficult to achieve in reality since the signal on the attackers end do have some phase shift which may be difficult to monitor closely when it comes to mobile targets. In a perfect/static environment scenario it would be success.
2. It also depends on the antenna placements of the attacker and more detailed knowledge of the channel conditions is required for the attacker so that the placements can be done accordingly.
3. The proposed attack demonstrates limitations of friendly jamming schemes using only the slow jammer approach. This suggests that the results of the setups and experiments in case of the fast jammer approach may vary.
4. Hashing is a popular form of checking if the original message was tampered, although medical devices require quick and very efficient way to check for confidentiality, other areas using friendly jamming could make use of hashes an an additional counter measure for securing the method.