

**CHENNAI – PONDICHERRY**

**Two-hop Distance-Bounding Protocols: Keep your Friends Close**

**Abstract:**

Authentication in wireless communications often depends on the physical proximity to a location. Distance-bounding (DB) protocols are cross-layer authentication protocols that are based on the round-trip-time of challenge-response exchanges and can be employed to guarantee physical proximity and combat relay attacks. However, traditional DB protocols rely on the assumption that the prover (e.g., user) is in the communication range of the verifier (e.g., access point); something that might not be the case in multiple access control scenarios in ubiquitous computing environments as well as when we need to verify the proximity of our two-hop neighbour in an ad-hoc network. In this paper, we extend traditional DB protocols to a two-hop setting i.e. when the prover is out of the communication range of the verifier and thus, they both need to rely on an untrusted in-between entity in order to verify proximity. We present a formal framework that captures the most representative classes of existing DB protocols and provide a general method to extend traditional DB protocols to the two-hop case (three participants). We analyse the security of two-hop DB protocols and identify connections with the security issues of the corresponding one-hop case. Finally, we demonstrate the correctness of our security analysis and the efficiency of our model by transforming five existing DB protocols to the two-hop setting and we evaluate their performance with simulated experiments.

**Existing System:**

Furthermore, wireless communications often rely on the cooperation of one-hop and two-hop neighbours (e.g., routing in wireless ad-hoc networks). Verifying the location of our neighbours and our proximity to an access point is usually performed by employing a secure neighbour discovery (SND) method. Distance-bounding (DB) protocol is an important method for reliable SND, which is based on the round-triptime of carefully designed challenge-response messages to provide an upper bound on the physical distance between two nodes.

Although DB protocols provide a cryptographic proof of proximity for one-hop neighbours they cannot be employed when the prover is outside the communication range of the verifier.

**Proposed System:**

We shall focus on DB protocols that are registerbased, as these constitute the overwhelming majority of the proposals presented in the literature. We need to note though that non-register based DB protocols could easily be extended to a two-hop setting. However, the employed generalisation and notation does not capture the description of non-register based protocols, since they have more complicated structures (e.g., a tree-based response function). Henceforth, when referring to DB protocols we shall consider register-based DB protocols.

We have recently introduced the concept of two-hop distance-bounding that extends traditional DB protocols to a two-hop setting and proposed an approach on how some of the existing DB protocols could be modified to verify the proximity of both next-hop and two-hop neighbours. In this paper, we go beyond this and introduce a general model that covers most of the existing DB protocols and analyse its security for internal and external adversaries. Furthermore, we provide instantiations for the transformation of five existing DB protocols to a two-hop setting. To verify our theoretical analysis, we evaluate the five chosen protocols and provide an analysis of the success probability of the different types of attacks for a varying number of rounds. Finally, we provide simulated experiments that validate our theoretical results.