How to Protect a Distance Bounding Protocol against a Terrorist Fraud Attack?

Distance bounding protocols are proposed based upon the round trip time measurements of the executed messages to prevent sensor networks against wormhole attack and to safeguard RFID systems against relay attack. In such protocols, the verifier authenticates users as well as establishing an upper bound on its physical distance between the users and itself. Distance bounding protocols are also vulnerable to mafia fraud, distance fraud and terrorist fraud attacks. This talk describes all-or-nothing method employed on distance bounding protocols that can prevent terrorist fraud attack performed over the existing distance bounding protocols. Actually, this method is the only approach which can overcome all the three fraud attacks simultaneously with the lowest success probability of the attacks compared with the well known distance bounding protocols. Besides, this method can be implemented on a low-cost device due to low computational cost and minimum system memory requirements.