Abstrak

Paradigma *Internet of Things* bergantung pada partisipasi antar objek yang saling terhubung pada suatu jaringan untuk mengamati dan bereaksi terhadap perubahan disekitarnya secara otonom. Partisipasi antar objek IoT terancam oleh serangan berbasis *trust* berupa *bad-mouthing*. Serangan ini dapat memperburuk kepercayaan kinerja objek-objek IoT terhadap suatu objek IoT yang terkena serangan. Hilangnya kepercayaan antar objek-objek IoT berakibat pada hasil yang ingin dicapai dari penerapan IoT menjadi tidak maksimal. Untuk itu, dibuat suatu manajemen *trust* yang menggunakan penghitungan *trust* secara menyeluruh yang menggabungkan penghitungan *trust* subjektif objek dengan penghitungan *broker* berupa *feedback*. Penghitungan *trust* pada *broker* menggunakan teori entropi informasi yang memiliki bobot nilai objektif. Kemudian, nilai *trust* diagregasi secara dinamis oleh objek untuk mendapatkan nilai *trust* terhadap objek lain yang lebih dapat dipercaya. Manajemen *trust* juga mendeteksi serangan dengan menggunakan standar deviasi, untuk mengetahui mana *feedback* normal dengan *feedback* serangan. Manajemen *trust* dapat mendeteksi serangan *bad-mouthing*, rata-rata waktu yang dibutuhkan *broker* dan *node-node* dalam penghitungan *trust* adalah 1.349768 milidetik dan 1011.086426 milidetik.

Kata kunci : internet of things, penghitungan trust, manajemen trust, feedback multi-sumber, teori entropi Informasi.