Abstract

The Internet of Things paradigm relies on participation between connected objects on a network to observe and react to the changes of its surroundings autonomously. This participation between IoT objects is threatened by a trust-based attack in the form of bad-mouthing. This attack can worsen the performance trust between IoT objects to certain IoT object that is being attacked. The loss of trust between IoT objects could lead to not optimal expected results from IoT applications. For that problem, trust management is created that uses comprehensive trust computation that combines subjective object trust computation in the feedback form with broker computation. Trust computation in the broker uses information entropy theory which has objective value weight. Then, the object aggregates the trust value dynamically to achieve a more trustable trust value of other objects. Trust management also detects bad-mouthing attacks using standard deviation, to determine which feedback is normal and which feedback is an attack. The trust management can detect bad-mouthing attack, average time needed for broker and nodes for trust computing are 1.349768 milliseconds and 1011.086426 milliseconds.

Keywords: internet of things, trust computation, trust management, multisource feedback, information entropy theory.