WRife: A Wireless Epidemic Data Collection and Tracking Protocol Suitable for Medical Monitoring

Somdev Chatterjee, Manuel Corona, Eric A. Freudenthal, Virgilio Gonzalez, Luc Longpré, and Avranil Tah

The University of Texas at El Paso

{efreudenthal, longpre, vgonzalez3}@utep.edu; {schatterjee, atah, mcorona2}@miners.utep.edu

Abstract

Collection of patients' health related data is one of the major time consuming activities for health-care personnel in modern health care systems. Manual data collection is monotonous, error-prone, and well suited for electronic support. Wired links provide high reliability and bandwidth but at high cost of installation, and ill-suited for monitoring mobile assets and patients. Radio communication channels can potentially reduce cost of installation and enable mobile data collection. However, the selection of transmission power and communication protocol exposes a range of scalability, privacy, integrity, and safety concerns. We propose the integration of a novel composition of cryptographic and epidemic data collection techniques with suitable properties for this problem.

Risk of interference with sensitive devices including safety risks due to induced current and power availability dictate the use of low-power short range devices. There exists epidemic routing protocol in partially connected ad-hoc networks with primary emphasis on maximum message delivery, minimum latency, and minimal resource consumption. This implementation addresses absence of a connected path between source and destination, and presence of network partitions.

We propose the use of epidemic communication protocol for low-bandwidth data collection from medical sensors in non-critical-care contexts. The fixed and mobile radio devices are responsible for disseminating information from medical sensors to server. The incorporation of mobile devices worn by patients and staff permits their opportunistic use as "data-mules" to transport samples beyond the limited communication radius of short-range devices.

Epidemic communication leaves copies of samples simultaneously on multiple devices and results into waste of bandwidth and power. Time-stamping of data is not enough to deal with this situation as it is not obvious that the collected information gets uploaded to the central storage before the expiration of the timestamp. Our protocol uses anti-entropy mechanism to erase copies of samples after they are uploaded to the servers. The samples are disseminated in an ascending monotonic sequence. Servers maintain the database in the form of monotonic sequences of health related data. Deletion of unnecessary samples is simplified by maintaining the monotonic order of samples during exchange of data within devices

We employ distinct cryptographic ciphers for the protocol and sensor data to guard against information poisoning and to protect the integrity of the system. We use encryption at two levels through dual symmetric keys, a sensor key unique to each sensor and a protocol key unique to the protocol. These keys may be revoked as needed using appropriate key distribution technique. The concept of digital signature could also be used to guard the system against masquerading. We propose alarms be used to trigger manual intervention when needed in the process of reliably uploading critical samples in a timely fashion.

Hospital management may want to keep track of inter-personnel rendezvous among patients, visitors, and health personnel for identifying possible transmission of contagious agent during the outbreak of an

infectious disease. WRife automates the process of tracking the inter-personnel rendezvous within a hospital and it fulfills the requirements of portability, low-power consumption, a reasonable communication range and ultimately to transfer the tracking information to the central storage device.