MỘT THUẬT TOÁN MÃ KHỐI MỚI TRÊN CƠ SỞ TOÁN TỬ PHỤ THUỘC DỮ LIỆU CHUYỂN ĐỔI ĐƯỢC DÙNG CHO MẠNG DI ĐỘNG.

Nguyễn Hiếu Minh, Đỗ Thị Bắc, Hồ Ngọc Duy

TÓM TẮT:

Có rất nhiều dạng tấn công có thể nhằm vào các mạng cảm biến vô tuyến (WSNs). độ mạnh và phức tạp của các dạng tấn công này không ngừng tăng lên. Các hạn chế về máy tính và năng lượng pin ở các node cảm biến vẫn tồn tại do sự đa dạng của các cơ chế bảo mật. Bài báo này đề cập đến vấn đề sử dụng các toán tử phụ thuộc dữ liệu chuyển đổi được định hướng cho thiết kế các thuật toán mã hóa tốc độ cao phù hợp với các ứng dụng trong các môi trường hạn chế. Trong bài này cũng giới thiệu và đưa ra các đánh giá mã khối mới dựa trên SDDO sử dụng phương pháp trên. Kết quả đánh giá mức độ bảo mật cho thấy mật mã MD-64 khó bị xâm nhập hơn so với các WSN đang được sử dụng phổ biến hiện nay như DES, Camellia, …Hơn nữa kết quả tổng hợp cho việc triển khai trên phần cứng (FPGA) chứng minh được rằng MD-64 mới này có hiệu quả rất cao, đặc biệt là đối với WSN.

Wireless sensor networks (WSNs) are exposed to a variety of attacks. The quality and complexity of attacks are rising day by day. Limitations in computational and battery power in sensor nodes are constraints on the diversity of security mechanisms. This paper concerns the problem of using of the switchable data-dependent operations (SDDOs) oriented to the design of fast cipher suitable to applications in constrained environments. The new SDDO-based block cipher using this approach presented and estimated. The security estimations show that cipher MD-64 is less likely to suffer intrusion of differential cryptanalysis than currently used popular WSN ciphers like DES, Camellia and so on. Moreover, FPGA synthesis result for hardware implementation (FPGA) proves that new cipher MD-64 is very efficient, especially for WSN

Đề xuất giải pháp mật mã khối trên cơ sở toán tử phụ thuộc dữ liệu chuyển đổi được hướng đến ứng dụng trên các thiết bị di động.