Việc tích hợp mạng 5G và mạng cảm biến không dây (WSN) là rất quan trọng trong kỷ nguyên mới của Internet vạn vật (IoT), cho một loạt các ứng dụng. Tuy nhiên, bất chấp những lợi thế tiềm năng của sự tích hợp này, có những lo ngại về các mối đe dọa an ninh không lường trước có thể ảnh hưởng đến cuộc sống hàng ngày của chúng ta.

Thỏa thuận khóa xác thực là một tính năng bảo mật thiết yếu để liên lạc an toàn giữa người dùng và thiết bị IoT và để bảo vệ các ứng dụng IoT khỏi các mối đe dọa bảo mật. Một lược đồ xác thực và thỏa thuận khóa dựa trên khái niệm IoT gần đây đã được đề xuất cho các WSN không đồng nhất, tuyên bố cung cấp ẩn danh cho người dùng và xác thực lẫn nhau, cũng như khả năng chống lại một số loại tấn công.

Trong bài viết này, chúng tôi kiểm tra một số điểm yếu bảo mật của sơ đồ nói trên. Tiếp theo, chúng tôi thiết kế kiến ​​trúc mạng phù hợp cho việc tích hợp mạng 5G và WSN. Dựa trên kiến ​​trúc mạng, chúng tôi đề xuất lược đồ xác thực hai yếu tố và thỏa thuận khóa trong các WSN tích hợp 5G cho IoT có thể chống lại các cuộc tấn công khác nhau, bao gồm cả các cuộc tấn công được xác định trước đó và có thể bảo vệ các yêu cầu bảo mật, bao gồm cả khả năng không liên kết.

Cuối cùng, chúng tôi đánh giá tính bảo mật và hiệu suất của chương trình đề xuất và so sánh sơ đồ của chúng tôi với các chương trình liên quan khác.

Internet of Things (IoT) là một công nghệ mới nổi kết nối nhiều loại thiết bị, bao gồm điện thoại thông minh, thiết bị gia dụng, cảm biến và các thiết bị mạng khác. Công nghệ mới này có thể được áp dụng trong nhiều lĩnh vực ứng dụng, như nhà thông minh (ví dụ: an ninh, kiểm soát nhiệt độ và chiếu sáng), thành phố thông minh, chăm sóc sức khỏe (ví dụ: giám sát bệnh nhân từ xa) và sản xuất thông minh (ví dụ: giám sát và kiểm soát từ xa của hệ thống sản xuất).

Để phát triển các ứng dụng IoT, việc thiết lập một ngăn xếp mạng mở, tiêu chuẩn với các giao thức phục vụ cho nhu cầu của các thiết bị bị hạn chế là điều cần thiết. Hơn nữa, vì IoT trải rộng trên nhiều miền ứng dụng như vậy, nên việc triển khai của nó đòi hỏi kết nối mạng không đồng nhất.

Điện thoại thông minh đã đóng một vai trò quan trọng trong các dịch vụ IoT ban đầu, giao tiếp bằng Wi-Fi và các công nghệ mạng di động. Mạng di động được coi là một ứng cử viên tiềm năng để cung cấp kết nối cho các thiết bị IoT, nhờ hỗ trợ di động, độ tin cậy và triển khai phổ biến.

Đặc biệt, các mạng thế hệ thứ năm (5G) hiện đang được phát triển đang hướng tới việc cung cấp tốc độ cao (1 Gbps), công suất thấp và độ trễ thấp (1 ms trở xuống). Do đó, công nghệ 5G sẽ đẩy nhanh việc triển khai nhiều ứng dụng IoT, đòi hỏi sự phổ biến hơn, tính di động cao hơn, hiệu suất và tốc độ tốt hơn và thời gian phản hồi nhanh hơn.

Mạng cảm biến không dây (WSN) bao gồm một số lượng lớn các nút cảm biến nhỏ, bị hạn chế về tài nguyên, được triển khai trong một khu vực quan tâm để theo dõi và thu thập các điều kiện vật lý hoặc môi trường, như ánh sáng, nhiệt độ, bảo đảm, chuyển động, âm thanh, hoặc chất ô nhiễm. WSN đóng vai trò quan trọng trong IoT bằng cách hỗ trợ cảm biến và thu thập thông tin môi trường. Do đó, để cung cấp thành công các ứng dụng IoT, cần phải tích hợp mạng 5G và WSN.

Tuy nhiên, bất chấp tiềm năng của sự tích hợp này, nó cũng khiến chúng ta tiếp tục gặp phải các mối đe dọa an ninh trong cuộc sống hàng ngày.

Do đó, bảo mật và quyền riêng tư là rất quan trọng để bảo vệ các ứng dụng IoT khỏi các cuộc tấn công như vậy. Hơn nữa, tính không đồng nhất của các mạng có thể có ảnh hưởng đáng kể đến bảo mật của các ứng dụng IoT, trong đó các nút cảm biến bị hạn chế tài nguyên phải mở giao tiếp an toàn với các thiết bị mạnh hơn.

Ví dụ, trong một ngôi nhà thông minh, các nút cảm biến gia đình giao tiếp với điện thoại thông minh của người dùng. Để liên lạc an toàn giữa bất kỳ bên nào và để cung cấp các mức bảo mật tương đương cho liên lạc giữa các thiết bị thông thường, thuật toán mã hóa tối ưu là rất cần thiết. Hơn nữa, các thiết bị IoT yêu cầu bảo mật nhẹ tốc độ cao và hiệu quả.