# A security mechanism for Enhanced ShockBurst wireless communication protocol using nRF24L01

**Aref Ayati**

Sau đại học Đại học Công nghệ Tiên tiến

**Hamid Reza Naji** ( naji@kgut.ac.ir )

Sau đại học Đại học Công nghệ Tiên tiến

---

**Research Article**

**Keywords:** IoT, WSN, nRF24L01, ShockBurst nâng cao, Bảo mật, Phòng thủ mục tiêu di động

**Posted Date:** 12/12/2023

**DOI:** https://doi.org/10.21203/rs.3.rs-3777984/v1



**Additional Declarations:** Không có lợi ích cạnh tranh nào được báo cáo.

---

# Cơ chế bảo mật cho giao thức truyền thông không dây ShockBurst nâng cao bằng cách sử dụng nRF24L01

Aref Ayati, Hamid Reza Naji*

Khoa Kỹ thuật Máy tính và Công nghệ Thông tin, Đại học Công nghệ Tiên tiến, Kerman, Iran

trừu tượng

Việc sử dụng Internet vạn vật và Mạng cảm biến không dây ngày càng tăng là rất đáng chú ý do tính đa dạng của chúng.
các ứng dụng. Do có nhiều mối đe dọa an ninh mạng cũng như điểm yếu của hệ thống truyền thông trong IoT và WSN
cơ sở hạ tầng, chúng tôi đã tiến hành nghiên cứu để tăng cường tính bảo mật của giao thức "ShockBurst nâng cao", một trong những giao thức không dây
các giao thức mạng được sử dụng rộng rãi trong các lĩnh vực này. Chúng tôi đề xuất một cơ chế bảo mật để nâng cao tính bảo mật của "Tăng cường
ShockBurst" giao thức mạng không dây và bảo vệ các mạng truyền thông trong IoT hoặc WSN sử dụng giao thức này. Cơ chế này là
an toàn hơn và nhanh hơn các cơ chế được đề xuất trước đó và dựa trên CIAA có thể đảm bảo tính bảo mật của tin nhắn,
tính toàn vẹn, tính sẵn sàng và trách nhiệm giải trình. Trong phương pháp này, bằng cách tận dụng thời gian và chức năng để thường xuyên xáo trộn địa chỉ
trong giao thức truyền thông không dây Tăng cường Shock Burst, các điều kiện bảo mật phù hợp hơn đã được triển khai với quy trình không quá phức tạp.
chi phí cao so với các phương pháp khác.

Từ khóa: IoT, WSN, nRF24L01, ShockBurst nâng cao, Bảo mật, Phòng thủ mục tiêu di động

## 1. Giới thiệu

Sự mở rộng của Internet of Things (IoT) và mạng cảm biến không dây (WSN) trong những năm gần đây và sự đa dạng của chúng
các ứng dụng, do hầu hết các nút của chúng được kết nối với nhau thông qua mạng không dây, là một trong những mục tiêu chính của
những kẻ xâm nhập xâm nhập vào các mạng này. Đặc biệt, IoT và WSN đã được ứng dụng trong nhiều lĩnh vực như kinh doanh, tự động hóa, thông minh
thành phố, nông nghiệp, máy bay không người lái, y tế, môi trường và giáo dục. Trong các hệ thống như vậy, thường sử dụng mô-đun giao tiếp có thể
giao tiếp dựa trên giao thức truyền thông, các nút có thể trao đổi thông tin trong mạng [1-4].

Khi công nghệ truyền thông tiến bộ và các thiết bị cũng như hệ thống tính toán trở nên dễ tiếp cận hơn, IoT dự kiến sẽ
mở rộng nhanh chóng. Điều này làm cho bảo mật IoT trở thành một vấn đề quan trọng để bảo vệ phần cứng và mạng trong hệ thống IoT. Tuy nhiên, kể từ
kết nối các thiết bị này là một khái niệm tương đối mới, bảo mật chưa thực sự là ưu tiên hàng đầu trong việc sản xuất các thiết bị này
[5]. Một trong những giao thức mạng có thể giúp chúng tôi kết nối không dây từng nút trong các mạng này với các mạng khác được gọi là "Nâng cao
ShockBurst" (ESB). Ngoài ra, giao thức này được sử dụng bởi dòng chip truyền thông nRF24L01.

Trong những năm gần đây, chúng ta đã thấy việc sử dụng ngày càng nhiều các mô-đun giao tiếp nRF24L01 hoạt động dựa trên giao thức ESB.
Có lẽ lý do quan trọng để sử dụng chúng là giá cả hợp lý, hiệu quả cao và tốc độ truyền dữ liệu cao [6]. Tuy nhiên, một trong những
Nhược điểm của giao thức truyền thông này là tính bảo mật cơ bản của nó. Tuy nhiên, việc sử dụng các mô-đun này đã được quan sát gần đây
trong các ngành công nghiệp khác nhau như sản xuất máy bay không người lái và các thiết bị liên quan đến IoT [7,8]. Nói chung, như đã nêu trong [9], ESB

Cấu trúc liên kết mạng phân tán hiện đã được phát triển mà không cần bất kỳ quy trình bảo mật hoặc mã hóa mặc định nào. Kết quả là, những rủi ro của mạng các cuộc tấn công đe dọa lớn đến thông tin liên lạc dựa trên giao thức này. Vì vậy, giao thức này đòi hỏi nỗ lực để làm cho nó an toàn hơn trong điều kiện đảm bảo an toàn trong tương lai.

Trong bài viết này, chúng tôi sẽ cố gắng trình bày một cơ chế bảo mật nhanh chóng, phần nào hoàn thiện về mọi mặt, dựa trên nghiên cứu trước đó. về bảo mật truyền thông, để trong tương lai, người dùng giao thức truyền thông ESB có thể làm cho thông tin liên lạc của họ an toàn hơn. Bài viết sẽ trình bày một cơ chế bảo mật đảm bảo tính bảo mật, tính toàn vẹn và xác thực người dùng (nút) trong giao tiếp. Cũng, chúng tôi trình bày một phương pháp xáo trộn địa chỉ dựa trên quan hệ toán học để tăng cường và tăng khả năng kiểm soát khả năng truy cập. Các các phương pháp bảo vệ mạng thông thường (ví dụ: mã hóa thông tin, xác thực, quét lỗ hổng và bảo vệ chống vi-rút) có cung cấp một số mức độ bảo mật, nhưng chúng không đủ để bảo vệ chống lại các cuộc tấn công đa dạng và ngày càng phát triển, và những cuộc tấn công này đòi hỏi nhiều hơn kỹ thuật phòng thủ không gian mạng tiên tiến [10,11].

Như chúng ta đã biết trong lĩnh vực mạng máy tính, nếu thực hiện truyền thông thì các chi tiết trong mạng vẫn được giữ nguyên cho đến cuối cùng. của giao tiếp. Trong trường hợp này, kẻ xâm nhập có thể dễ dàng quan sát và nghe lén mạng, phân tích và thực hiện hành động chống lại nó [10]. Ngoài ra, một số cuộc tấn công mạng như Từ chối dịch vụ (DoS) hay SYN Flood, v.v. cũng có khả năng xảy ra ở bất cứ đâu và bất cứ lúc nào trong mạng truyền thống [12]. Đó là lý do tại sao chúng tôi sử dụng phương pháp xáo trộn địa chỉ, một biến thể của phương pháp Phòng thủ mục tiêu di chuyển được gọi là MTD.

Hãy tưởng tượng rằng chúng ta có một nút cảm biến hoặc một nút trong mạng IoT cần gửi tin nhắn đến một nút khác. Chúng ta cần phải thực hiện đảm bảo rằng tin nhắn của chúng tôi an toàn trước mọi hình thức nghe lén, đó là lý do để có cơ chế bảo mật tin nhắn. Ngoài ra, tất cả các tin nhắn phải được gửi một cách toàn vẹn và chúng tôi cũng phải đảm bảo rằng quá trình này không có tin nhắn nào được gửi đi. bị giả mạo và cuối cùng có một xác thực nút đơn giản để bảo vệ chống lại tất cả các loại tấn công mạo danh nhằm giải trình trách nhiệm.

Trong bài viết này trước tiên, chúng tôi sẽ trình bày các công trình khác trong lĩnh vực này dưới dạng các công trình liên quan, tiếp theo chúng tôi sẽ thảo luận về ESB giao thức truyền thông, sau đó chúng tôi đề xuất cơ chế bảo mật của mình. Chúng tôi đã triển khai cơ chế đề xuất của mình trên cơ sở vi điều khiển để hiển thị hiệu suất của nó và so sánh nó với các phương pháp khác. Cuối cùng, chúng tôi có kết luận và các công việc tiếp theo.

## 2. Công trình liên quan

Để làm ví dụ về ứng dụng ESB, chúng ta có thể tham khảo một số nghiên cứu trong lĩnh vực này. Trong [13], trong khi nói rằng ngày nay hầu hết thách thức quan trọng trong ngành nông nghiệp và theo hướng số hóa nông nghiệp là nâng cao năng suất và lợi nhuận, các tác giả đã đề cập đến việc quản lý tưới tiêu và sử dụng IoT theo hướng này. Trong dự án này, mô-đun nRF24l01 được sử dụng để liên lạc vô tuyến giữa các nút đích và các nút khác, nhưng không có bất kỳ cơ chế bảo mật cụ thể nào để bảo mật truyền thông nRF24l01. Mặt khác, trong [14] một lần nữa chúng ta lại thấy thảo luận về việc cung cấp một hệ thống nông nghiệp dựa trên Các mô-đun nRF24L01 dựa trên IoT và ESB được sử dụng, một lần nữa không bao gồm bất kỳ cơ chế bảo mật nào.

Trong nghiên cứu khác [15], IoT đã được sử dụng với mô-đun giao tiếp không dây nRF24L01 trong lĩnh vực dinh dưỡng. Tuy nhiên, không có cơ chế bảo mật để thiết lập liên lạc an toàn.

Trong các trư ờng hợp khác liên quan đến sức khỏe [16], để chăm sóc tốt hơn cho ngư ời già hoặc các nhóm dễ bị tổn thư ơng khác có vấn đề về tâm thần hoặc bệnh Alzheimer, v.v., việc sử dụng IoT với giao tiếp không dây thông qua nRF24L01 đã đư ợc thảo luận như ng họ không cung cấp bất kỳ thông tin nào. cơ chế bảo mật. Trong một số công trình khác, cơ chế bảo mật để thiết lập bảo mật tối thiểu trong truyền thông dựa trên nRF24L01 đã đư ợc thảo luận và chúng tôi sẽ xem xét chúng ở bên dư ới.

Trong bài viết [17], bằng cách sử dụng bộ vi điều khiển MSP430F1611 do Texas Instruments (TI) sản xuất và mô-đun truyền thông nRF24L01 dựa trên ESB, họ đã cố gắng thiết lập liên lạc an toàn bằng bộ vi điều khiển. họ so sánh thiết kế mới của họ với MSP430F1611 về mức tiêu thụ năng lư ợng. Bài viết này, đư ợc trình bày trong lĩnh vực y tế, lư u ý rằng hầu hết các bài báo gần đây năm qua, đặc biệt là trong lĩnh vực WSN, mới chỉ cố gắng trình bày và mô phỏng một phư ơng pháp đư ợc đề xuất sử dụng mã hóa đối xứng, như ng trong thực tế, họ chư a thể triển khai nó trong môi trư ờng thực tế. Chế độ bảo mật CCM, là một trong những loại mã hóa các chế độ với thuật toán AES-128, đư ợc sử dụng để thiết lập tính bảo mật của dữ liệu và cũng đảm bảo tính toàn vẹn của tin nhắn. TRONG phư ơng pháp này, trong năm chế độ làm việc sử dụng phư ơng pháp CCM và mã hóa AES-128, mã xác thực tin nhắn (MAC) là đầu tiên đư ợc áp dụng cho tin nhắn, sau đó tin nhắn kết hợp và MAC đư ợc mã hóa và truyền đi trên phư ơng tiện truyền thông. Năm ngư ời này chế độ làm việc đư ợc chỉ định trong hai loại khung thông báo và ở chế độ thứ nhất và thứ ba, khung thông báo chứa một kết hợp MAC 4 byte với tin nhắn gốc 8 byte trong phần tải trọng của khung tin nhắn. Ở chế độ đầu tiên, tin nhắn xin chào đư ợc gửi từ nút cảm biến đến nút chính để vào mạng và ở chế độ thứ ba, nó đư ợc sử dụng để gửi ACK từ nút cảm biến đến nút cảm biến. nút chủ hoặc ngư ợc lại. Ba chế độ làm việc khác cũng đư ợc sử dụng để truyền các thông điệp thông thư ờng giữa các nút cảm biến và nút chính, trong đó MAC 4 byte kết hợp với 24 byte văn bản tin nhắn gốc đư ợc sử dụng trong phần tải trọng của khung tin nhắn. BẰNG đã đề cập, tất cả các tin nhắn đều đư ợc mã hóa hoàn toàn bằng phư ơng thức AES-128 trư ớc khi đư ợc gửi lên mạng. Trong phư ơng pháp này, không có gì đặc biệt đã đư ợc thực hiện để ngăn chặn tất cả các loại tấn công DoS. Hệ thống do các tác giả này đề xuất nhìn chung dễ bị tấn công bởi tất cả các loại của các cuộc tấn công DoS do thiếu bất kỳ cơ chế phòng vệ nào chống lại nó, mặt khác, do kỹ thuật thiết lập MAC đầu tiên và sau đó mã hóa, nó cũng có thể chống lại các cuộc tấn công giả mạo. Như ng nó dễ bị tổn thư ơng ở một khía cạnh nào đó và nếu kẻ xâm nhập thay đổi nội dung sau khi nghe vào mạng, ngư ời nhận tin nhắn, miễn là anh ta không giải mã tin nhắn, sẽ không biết về sự thay đổi nội dung.
Một điều đáng chú ý khác là việc không có bất kỳ cơ chế xác thực nào, điều này cuối cùng khiến hệ thống này dễ bị xác thực-
các cuộc tấn công dựa trên

Các nhà nghiên cứu của bài báo [18] cũng đã triển khai thuật toán mã hóa bất đối xứng trên giao tiếp giữa hai Các mô-đun nRF24L01 dựa trên giao thức mạng ESB để mã hóa tất cả dữ liệu đư ợc truyền trên mạng. Họ đã sử dụng mã hóa RSA thuật toán đơn giản vì theo nghiên cứu của họ, so với thuật toán RC5 và Skipjack, thuật toán RSA thực hiện tốt hơn, vì nói chung các thuật toán bất đối xứng mang lại tính bảo mật cao hơn như ng chúng không tính đến mức tiêu thụ năng lư ợng. Ngoài ra, họ còn tuyên bố thuật toán này giúp họ an toàn trư ớc các cuộc tấn công nghe lén và họ chỉ thiết lập xác thực và bảo mật với loại này của mã hóa. Có vẻ như trọng tâm của nghiên cứu này là duy trì tính bảo mật của dữ liệu chứ không phải các yếu tố bảo mật khác. Do không có bất kỳ xác thực tin nhắn nào, những kẻ xâm nhập có thể phá vỡ tính toàn vẹn của tin nhắn, dẫn đến các cuộc tấn công giả mạo.

Trong một nghiên cứu khác, các tác giả của bài báo [19], đã cố gắng cung cấp và thực hiện một kế hoạch bảo mật dữ liệu và truyền thông về cơ sở hạ tầng dựa trên đồ chơi thông minh trong lĩnh vực IoT. Họ đã giới thiệu một phương pháp bảo mật thông tin liên lạc dựa trên ESB giao thức. Bằng cách trình bày một số kịch bản, họ dự định cung cấp một cơ chế bảo mật thông tin liên lạc trong cơ sở hạ tầng thông minh. đồ chơi. Họ dự định kết nối một món đồ chơi thông minh với bộ thu thập dữ liệu bằng mô-đun nRF24L01 và truyền thông tin từ đồ chơi này sang người thu thập dữ liệu. Họ chuyển thông tin đến điện thoại di động Android thông qua giao thức truyền thông Wi-Fi và sau đó đến máy chủ có tên GIÁO DỤC sử dụng Internet. Trong phần đầu tiên của giao tiếp, nRF24L01 được sử dụng để kết nối giữa đồ chơi và Collector, các nhà nghiên cứu trong dự án này đã điều tra hai mối đe dọa bảo mật và đưa ra giải pháp khắc phục hai mối đe dọa này. Các Mối đe dọa đầu tiên là nếu người sưu tập giả gửi sai tin nhắn đến đồ chơi thì dịch vụ của đồ chơi sẽ bị ảnh hưởng. Vụ việc này được coi là một cuộc tấn công DoS và đề xuất rằng nếu cơ chế MAC được sử dụng trong văn bản của tin nhắn được truyền đi thì MAC sẽ được kiểm tra mỗi tin nhắn, vấn đề tấn công DoS sẽ không còn xảy ra nữa. Nhưng theo quan điểm của chúng tôi, cơ chế MAC không cung cấp bảo mật chống lại tất cả các loại tấn công DoS và các phương pháp này tạo ra sự bảo mật chống lại các cuộc tấn công như tấn công giả mạo. Ngoài ra, mục tiêu là để ngăn chặn gửi sai tin nhắn, nhưng vì họ đã tạo bản tóm tắt MAC cho tin nhắn ban đầu của mình và sau đó cố gắng mã hóa sự kết hợp của chúng, điều này sẽ khiến phương thức tốn nhiều năng lượng để giải mã và sau đó kiểm tra MAC xem có tin nhắn giả mạo không. Mối đe dọa thứ hai họ đề cập đến việc một kẻ thu thập giả mạo đánh cắp tin nhắn và tạo ra vấn đề về tính bảo mật trên mạng. Họ chưa đề cập đến chính xác họ đang bảo vệ chống lại cuộc tấn công nào, nhưng có vẻ như họ có ý định thiết lập bảo mật chống lại kẻ trung gian (MITM) tấn công và tấn công nghe lén tin nhắn. Để giải quyết vấn đề này, đề xuất của họ là sử dụng thuật toán mã hóa AES-128 cùng với với MAC để đảm bảo tính bảo mật và xác thực tính toàn vẹn của tin nhắn. Tuy nhiên, họ không đề cập cụ thể lý do tại sao họ sử dụng AES-128 và tuyên bố đơn giản rằng do hạn chế về tài nguyên xử lý trong đồ chơi thông minh nên họ đã chuyển sang mã hóa đối xứng này phương pháp này và bỏ qua các phương pháp khác. Điểm chính trong phương pháp được họ sử dụng là cơ chế chuyển khóa phiên trên mạng, trong trường hợp khóa chính bị rò rỉ, điều này cũng có thể do nội bộ độc hại thực hiện. Khóa phiên có thể bị rò rỉ bởi nghe lén thông điệp được truyền trên mạng. Họ đã sử dụng cài đặt MAC với phương pháp SHA-3 và Keccak sử dụng nhiều thao tác XOR trên các biến để tạo khóa và mã hóa bằng AES-128. Phương pháp này dễ bị tấn công DoS, nhưng do sử dụng phiên bản MAC thứ ba của SHA nên nó có thể ngăn chặn các cuộc tấn công giả mạo, nhưng có một cơ chế xác thực cụ thể các nút không được nhìn thấy.

Trong [20], các nhà nghiên cứu đã phát triển một hệ thống đèn đường thông minh sử dụng phần mềm điện thoại di động, đồng thời họ giao phó cho giao tiếp giữa các nút cảm biến với mô-đun nRF24L01 và giải quyết một số vấn đề bảo mật của nó. Nhìn chung, mô hình của họ dựa trên ứng dụng Android trên điện thoại di động được ghép nối với nút chính trong mạng WSN, được đồng bộ hóa với các nút chung khác được ghép nối trên đèn đường. Trong phương pháp được các tác giả này xem xét, phần Tải trọng nằm trong mỗi khung thông báo ESB chỉ chứa bảy byte từ 32 byte và để thiết lập bảo mật, họ chỉ xem xét tính bảo mật và sử dụng thuật toán mã hóa RC4 với độ dài khóa 128 bit, đây là thuật toán mã hóa mật mã luồng chứ không phải một khối mật mã. Tất cả nội dung tin nhắn bảy byte được mã hóa bằng thuật toán mã hóa đối xứng này và được giải mã trên thiết bị đích. Theo các tác giả, lý do sử dụng thuật toán RC4 là tốc độ hoạt động nhanh hơn và tiêu tốn ít bộ nhớ hơn khi truyền phát.

mật mã so với mật mã khối. Tất nhiên, các nhà nghiên cứu trong bài viết này đã đề xuất sử dụng các thuật toán mã hóa như RSA, DES và AES để bảo mật hiệu quả hơn. Cần lưu ý rằng do những điểm yếu cố hữu nên Microsoft đã ngừng hỗ trợ cho thuật toán này trong các trình duyệt web của nó vào năm 2015 và lý do là khả năng của thuật toán này trong việc khôi phục các văn bản được mã hóa [21]. Trong này phương pháp này không có xác thực nút và xác thực tin nhắn, hậu quả của các cuộc tấn công như thay đổi danh tính, mật khẩu đoán cùng với các cuộc tấn công của Sybil, và mặt khác, việc thiếu MAC cũng gây ra lỗ hổng cho việc giả mạo dữ liệu, và điều đó không có bất kỳ cơ chế nào để chống lại các cuộc tấn công DoS.

Hầu như tất cả các công việc liên quan được thảo luận đều không xem xét xác thực nút trong giao thức truyền thông ESB và chúng cũng không xem xét việc xác thực nút trong giao thức truyền thông ESB. có cơ chế bảo vệ khỏi việc đoán mật khẩu, mạo danh và tấn công Sybil dựa trên yêu cầu về trách nhiệm giải trình.

## 3. Giao thức ShockBurst nâng cao

Giao thức này truyền dữ liệu dựa trên khung gói được mô tả trong Hình 1. Giao thức này được phát triển bởi Nordic Semiconductor công ty và có mức tiêu thụ thấp, độ trễ thấp, chi phí thấp, tốc độ truyền tải cao. Mặc dù nó cung cấp thông tin liên lạc hai chiều đáng tin cậy, phù hợp để liên lạc giữa các thiết bị, chẳng hạn như những thiết bị hoạt động dựa trên WSN và cơ sở hạ tầng IoT. Cái này giao thức, giống như một số giao thức mạng không dây khác, có khả năng hỗ trợ cơ chế xác thực, mã hóa và tin nhắn mã xác thực [22-24].

| Lời mở đầu (1 byte) | Địa chỉ (3-5 byte) | Trường điều khiển gói (PCF) (9 bit) | Khối hàng (0-32 byte) | CRC (1-2 byte) |
|---|---|---|---|---|

Hình 1 Khung gói của Giao thức ShockBurst nâng cao.

Mỗi khung gói của giao thức ESB gồm 5 phần chính: 1-Lời mở đầu 2-Địa chỉ 3-Trường điều khiển gói (PCF) 4-Tải trọng và 5-CRC.

Ở đầu khung tin nhắn, chúng ta thấy "Lời mở đầu", là một chuỗi 01010101 hoặc 10101010. "Địa chỉ" phần, chứa địa chỉ của mô-đun ở chế độ máy thu. Địa chỉ của máy thu trong mô-đun thu phát có thể được đặt bằng 3, 4, hoặc 5 byte. Phần tiếp theo trong khung thông báo được gọi là "PCF" như bạn thấy trong Hình 2, chứa ba thành phần. Cái đầu tiên đại diện cho "độ dài của tải trọng" của tin nhắn đã gửi (nội dung). Tiếp theo là "PID" để tìm hiểu xem gói nhận được có đúng không mới hoặc trùng lặp. Việc sử dụng phần này trong gói tin gốc sẽ ngăn không cho dữ liệu trùng lặp được gửi đến gói chính. vi điều khiển trong nút mạng và trên thực tế, nó sẽ có khả năng chống lại các cuộc tấn công lặp lại phần nào. Trong phần sau đây, phần "ACK" được sử dụng để xác nhận việc nhận tin nhắn. Ngoài phần PCF, chúng ta còn đến phần chính của nội dung chính của thông báo “Payload”, có thể chứa tối đa 32 byte và ở cuối, "CRC" được sử dụng làm cơ chế phát hiện lỗi trong toàn bộ gói, tức là 1 hoặc 2 byte và nó được tính toán dựa trên các trường Địa chỉ, PCF và Tải trọng.

| Độ dài tải trọng (6 bit) | PID (2 bit) | Không_ACK (1 bit) |
|---|---|---|

Hình 2 Chi tiết về PCF.

Như có thể thấy trong khung thông báo chung của giao thức này, không có dấu vết nào của cơ chế bảo mật đặc biệt. Trong những điều sau đây, chúng tôi khuyên bạn nên thực hiện các thay đổi về địa chỉ và phần tải trọng để làm cho giao thức này an toàn hơn trước một số cuộc tấn công mạng.

Hiện nay, các kênh liên lạc không đáng tin cậy và các hoạt động không được giám sát đã khiến quá trình bảo vệ an ninh trở nên khó khăn hơn.
phức tạp [25], như đã đề cập trong giao thức ESB, giao thức này cung cấp cho chúng ta một giao tiếp không đáng tin cậy
kênh ở trạng thái cơ bản. Trong bài viết này, chúng tôi đề cập đến một số cuộc tấn công thụ động và chủ động có thể phân tích hoặc nghe trộm thông tin của chúng tôi.
liên lạc hoặc có thể giả mạo hoặc sửa đổi các gói của chúng tôi [26]. Trong phần tiếp theo của bài viết này, chúng tôi sẽ thảo luận về cơ chế được đề xuất để
tạo một kênh an toàn trong liên lạc dựa trên ESB nhằm cung cấp bảo mật chống lại các cuộc tấn công thụ động và chủ động. Kênh an toàn này
sẽ đảm bảo tính bảo mật, xác thực và tính toàn vẹn của thông điệp dựa trên lý thuyết [27] và cũng cố gắng có một giải pháp nhẹ
xác thực để đảm bảo trách nhiệm giải trình.

Dựa trên [5] và [28] hiện tại, một số mối đe dọa đối với IoT hoặc WSN là nghe lén, người đứng giữa, Sybil, mạo danh hoặc
giả mạo danh tính, DoS, đoán mật khẩu, giả mạo và tấn công lũ lụt SYN. Trong bài báo này, chúng tôi đề xuất một cơ chế giải quyết
những vấn đề trên. Giao thức truyền thông ESB hiện đang hoạt động với dòng mô-đun nRF24L01 có thể cung cấp tối đa
Tốc độ truyền dữ liệu 2mbps và liên lạc tầm xa khoảng hơn 1 km nếu bạn sử dụng phiên bản mới của mô-đun nRF có bộ khuếch đại.

## 4. Mặc định của Cơ chế bảo mật được đề xuất

### MỘT. Nguyên tắc bảo mật của cơ chế bảo mật được đề xuất

Chúng tôi xem xét tính bảo mật và hiệu quả trong việc thiết kế hệ thống của mình như sau.

Bảo mật: Việc thiết lập bảo mật trong mạng truyền thông được thực hiện để ngăn chặn sự xuất hiện của các cuộc tấn công chủ động hoặc thụ động. tấn công
dẫn đến việc nghe lén hoặc giám sát mạng hoặc những thứ tương tự được gọi là các cuộc tấn công thụ động, các cuộc tấn công gây giả mạo dữ liệu
hoặc tạo ra một luồng sai, và những thứ như thế còn được gọi là các cuộc tấn công tích cực [26]. Nhìn chung, bốn yếu tố chính để thiết lập an ninh trong
cơ chế được đề xuất của chúng tôi sẽ dựa trên tính bảo mật, tính toàn vẹn, tính sẵn sàng và trách nhiệm giải trình được gọi là các yêu cầu của CIAA [29]. ĐẾN
thiết lập bảo mật trong mạng IoT hoặc WSN, trách nhiệm giải trình và tính bảo mật của tin nhắn của người dùng hoặc nút phải được xem xét và
tin nhắn gửi đi phải được nhận xác thực ở phía người nhận nên chúng ta phải có giải pháp đảm bảo tính toàn vẹn của tin nhắn. Chúng tôi
cũng nên lập kế hoạch để nếu một nút bị đánh cắp hoặc chiếm đoạt khỏi mạng, kẻ xâm nhập không thể truy cập thông tin của nút đó hoặc trích xuất
thông tin từ nút và chúng tôi cũng cần lập kế hoạch chống lại các cuộc tấn công từ chối dịch vụ (DoS).

Hiệu quả: Do hạn chế về tài nguyên của một nút trong IoT hoặc WSN, đặc biệt là hạn chế về tài nguyên năng lượng,
phương pháp được trình bày phải đi kèm với tốc độ tối đa và mức tiêu thụ năng lượng và tài nguyên tối thiểu. Dựa trên
này, chúng tôi sẽ tập trung vào việc lựa chọn các thuật toán tiêu thụ điện năng nhanh và tiêu thụ điện năng thấp.

### B. Điều kiện tiên quyết

Do hệ thống IoT hoặc WSN có thể được xem là hệ thống phân tán nên các thuật toán mã hóa được sử dụng rộng rãi để đảm bảo quyền riêng tư trong
hệ thống phân tán [30]. Do việc xem xét mức tiêu thụ năng lượng và tài nguyên có hạn, đồng thời cũng cung cấp khả năng mã hóa/giải mã
tốc độ của các thuật toán mã hóa đối xứng so với các thuật toán mã hóa bất đối xứng, chúng tôi đề xuất phương pháp dựa trên tính đối xứng [31,32].

Phương pháp mã hóa đối xứng: Phương pháp mã hóa đối xứng được sử dụng do tính dễ sử dụng, đơn giản trong thực hiện, cao
tốc độ thực thi, linh hoạt hơn, tiêu thụ ít bộ nhớ hơn và tiêu thụ ít điện năng hơn. Trong số các thuật toán mã hóa đối xứng,

AES, Blowfish và RC4 hiện có điều kiện tốt về tốc độ thực thi thuật toán trên tin nhắn. Chúng tôi đã chọn AES để hư ởng lợi
khỏi những vấn đề trên cũng như sự chấp nhận và bảo mật cao của công chúng [33,34].

Xác thực ngư ời dùng/nút: Trong xác thực ngư ời dùng/nút, thông thư ờng, cả hai phía của kết nối đều đư ợc xác thực bằng tên ngư ời dùng hoặc
mật khẩu hoặc một giá trị bí mật. Do hạn chế về tài nguyên xử lý và giới hạn về độ dài tải trọng trong giao tiếp ESB
Protocol, chúng tôi không cung cấp phư ơng thức xác thực phức tạp và sử dụng một phư ơng thức rất nhẹ, như ng chúng tôi xem xét
xác thực ngư ời dùng/nút cho mỗi tin nhắn đư ợc trao đổi trong mạng để đảm bảo trách nhiệm giải trình của ngư ời dùng/nút.

Xác thực tin nhắn hoặc Kiểm tra tính toàn vẹn: Xác thực tin nhắn, thư ờng là để xác nhận rằng tin nhắn đã đư ợc gửi bởi ngư ời dự định.
ngư ời gửi, nội dung của nó không thay đổi và nó đư ợc gửi vào một thời điểm cụ thể. Các phư ơng pháp như HMAC, LMAC, v.v. thư ờng đư ợc sử dụng
đư ợc sử dụng cho mục đích này.

Nói chung, trong các phư ơng thức này, một giá trị gọi là MAC đư ợc ngư ời gửi tạo ra bằng thuật toán cụ thể và khóa chung giữa
ngư ời nhận và ngư ời gửi, đư ợc đặt cạnh nội dung tin nhắn và gửi qua mạng. Về phía ngư ời nhận, phần chính của thông điệp
đư ợc tách khỏi phần MAC và MAC đư ợc tạo lại với cùng khóa và thuật toán sử dụng thông báo gốc. Tiếp theo,
Giá trị MAC mới đư ợc so sánh với giá trị MAC do ngư ời gửi gửi và nếu chúng bằng nhau thì tin nhắn sẽ đư ợc chấp nhận trong hệ thống.
Nếu không, điều đó có nghĩa là tin nhắn đã bị giả mạo bởi kẻ thù hoặc kẻ xâm nhập trong quá trình liên lạc [30]. Các
Thông báo MAC đư ợc sử dụng phía sau hoặc phía trư ớc thông báo, đư ợc tạo bằng các thuật toán khác nhau. Hiện tại, MD5 và SHA-1
các thuật toán nói chung đã bị NIST loại bỏ [35], Ngoài ra, các thuật toán MD4, GOST, HAVAL-128 và RIPEMD đã đư ợc loại bỏ.
đư ợc xem xét và loại bỏ một cách khoa học về mặt bảo mật [36].

Hiện nay, họ thuật toán SHA-2 và SHA-3 rất phổ biến và đư ợc sử dụng rộng rãi, như ng đáng tiếc là độ dài của bản tóm tắt
do chúng tạo ra thư ờng rất lớn, ít nhất là 28 byte. Chúng có thể đư ợc sử dụng như ng chúng ta cần sử dụng hàm cắt ngắn để giảm
độ dài của chúng có thể buộc hệ thống thực hiện các quy trình bổ sung.

Trong cơ chế đư ợc đề xuất của chúng tôi, thuật toán SipHash sẽ đư ợc sử dụng để tạo thông báo MAC, có độ dài thông báo ngắn hơn và
tốc độ tính toán rất phù hợp. Thuật toán này đã đư ợc trình bày vào năm 2012 và đầu ra tóm tắt tư ơng đư ơng với 8 byte [36,37].

MTD trong Phư ơng pháp phòng thủ động: Trong những năm qua, các giải pháp phổ biến như kiểm soát truy cập, mã hóa thông tin, xâm nhập
hệ thống phòng ngừa, tư ờng lửa, hệ thống chống virus, v.v. đã đư ợc cung cấp. Chúng cung cấp mức độ bảo mật phù hợp, như ng hầu hết chúng có thể
cung cấp bảo mật chống lại các cuộc tấn công đã đư ợc biết đến [38,12,10].

Sau đây, chúng tôi có một số cuộc thảo luận với tiêu đề phòng thủ năng động, với những thay đổi liên tục trong mạng
điều kiện, cố gắng đánh lừa kẻ tấn công và tăng chi phí của anh ta để tìm ra cách thâm nhập. Ngoài ra, nó buộc kẻ tấn công phải lãng phí rất nhiều
thời gian thâm nhập vào hệ thống. Về vấn đề này, chúng tôi đã chọn một phư ơng pháp phòng thủ năng động dựa trên một kỹ thuật đư ợc gọi là di chuyển
phòng thủ mục tiêu (MTD) để triển khai trong khuôn khổ bảo mật của chúng tôi [39].

Trong kỹ thuật MTD, một nỗ lực đư ợc thực hiện nhằm liên tục thay đổi mức độ tấn công nhằm gây khó khăn hơn cho kẻ thù hoặc kẻ xâm nhập.
nhận ra hệ thống mục tiêu, điều này làm lãng phí thời gian của anh ta và làm tăng độ phức tạp trong công việc của anh ta. Bằng cách sử dụng kỹ thuật này, kẻ thù có thể
khó tìm và sử dụng một phư ơng pháp chính xác để chống lại hệ thống mục tiêu. Trong kỹ thuật MTD, những thay đổi tích cực như địa chỉ mạng

sự thay đổi đư ợc thực hiện liên tục và năng động. Việc sử dụng kỹ thuật này trong các phư ơng pháp thiết lập bảo mật trong ESB giao thức truyền thông cũng có thể là một sự đổi mới khác biệt, hiệu quả và hiệu quả. Trong cơ chế đề xuất của chúng tôi, một trong những phư ơng pháp chúng tôi có xu hư ớng sử dụng là chủ đề thay đổi hoặc xáo trộn mối quan hệ giữa địa chỉ và thiết bị trong mạng truyền thông đư ợc gọi là xáo trộn địa chỉ.

Trong cái gọi là phư ơng pháp xáo trộn địa chỉ, có hai mẫu công việc chính [40] mà chúng tôi giải thích sau đây:

- Kiểu nhảy: Kiểu này chính xác về mặt truyền thông và đồng bộ hóa thời gian và phù hợp với truyền thông hiện đang truyền dữ liệu cơ bản. Phư ơng pháp làm việc dựa trên thực tế là cả hai bên đều ổn nhận thức đư ợc thông tin về kiểu nhảy địa chỉ của họ hoặc một bên của giao tiếp nhận thức rõ về mô hình nhảy của phía bên kia. Cơ chế đồng bộ hóa trong phư ơng pháp này đư ợc thực hiện bằng cách xác định thời gian bằng cách trao đổi mô hình nhảy giữa các bên hoặc bằng cách sử dụng chức năng đặt trư ớc với giá trị đầu vào ban đầu.
- Mẫu đột biến: Trong mẫu này, việc đồng bộ hóa giao tiếp không chính xác về mặt thời gian và thư ờng là đồng bộ hóa đư ợc hỗ trợ bởi các cập nhật định tuyến và yêu cầu/phản hồi DNS hoặc các cơ chế khác của bên thứ ba.

Do việc sử dụng giao thức mạng không dây ESB và tầm quan trọng của việc đồng bộ hóa thời gian chính xác và sự miễn cư ỡng đối với chuyển một địa chỉ mới trên mạng, chúng tôi sẽ sử dụng mô hình nhảy theo phư ơng pháp đư ợc đề xuất trong cơ chế bảo mật của chúng tôi.

## 5. Cơ chế đề xuất

Trong phư ơng pháp đề xuất của chúng tôi, cơ chế xáo trộn địa chỉ liên tục, xác thực ngư ời dùng/nút nhẹ, kiểm tra tính toàn vẹn và tính bảo mật của tin nhắn sẽ đư ợc sử dụng, điều mà chúng tôi sẽ thảo luận riêng bên dư ới:

1) Thiết lập xáo trộn địa chỉ chống tấn công DoS cho giao thức truyền thông ESB

Trong cơ chế bảo mật đư ợc đề xuất nhằm tăng tính bảo mật của giao thức ESB, ư u tiên của chúng tôi là cung cấp phư ơng pháp dựa trên MTD. Để đối phó với các cuộc tấn công do phân tích mạng (như tấn công DoS), các cuộc tấn công này có thể đư ợc ngăn chặn bằng cách xáo trộn liên tục địa chỉ dựa trên mẫu nhảy đã đư ợc đề cập trư ớc đó. Trên thực tế, bằng cách tạo điều kiện cho kẻ tấn công lãng phí thời gian, chúng ta giảm khả năng anh ta khai thác các lỗ hổng trong hệ thống của chúng tôi và thậm chí ở một góc nhìn dài hơn, chúng tôi có thể nghĩ rằng kẻ tấn công sẽ cũng mất khả năng quét các lỗ hổng. Chính xác hơn, với việc xáo trộn địa chỉ liên tục, kẻ tấn công không thể dễ dàng theo dõi địa chỉ mục tiêu và phải quét một không gian địa chỉ lớn hơn để tìm thấy nó. Như đã đề cập trư ớc đó, để thiết lập liên lạc trong mạng bao gồm giao thức ESB, cần phải chỉ định địa chỉ cho ngư ời gửi và ngư ời nhận. Chúng tôi biết độ dài địa chỉ của ESB giao thức nằm trong khoảng từ 3 đến 5 byte. Trong phư ơng pháp đề xuất của chúng tôi, chúng tôi xem xét biến thời gian (tính bằng phút) cùng với địa chỉ ban đầu đóng vai trò tư ơng tự như Vector ban đầu. Hai thành phần đư ợc đề cập đư ợc kết hợp trong một quy trình toán học trong đó chúng tôi xáo trộn địa chỉ và tạo một địa chỉ mới. Chúng ta xem xét một hàm toán học bình thư ờng có tải tính toán hạn chế và để tạo ra sự hỗn loạn trong đầu ra của nó đến mức không thể đoán đư ợc toàn bộ hàm hoặc tạo thành chuỗi của nó, chúng tôi sử dụng một hàm gọi là Mobius.

Trư ớc khi đư a ra các định nghĩa khác, chúng ta cần giải thích các từ viết tắt trong Bảng 1.

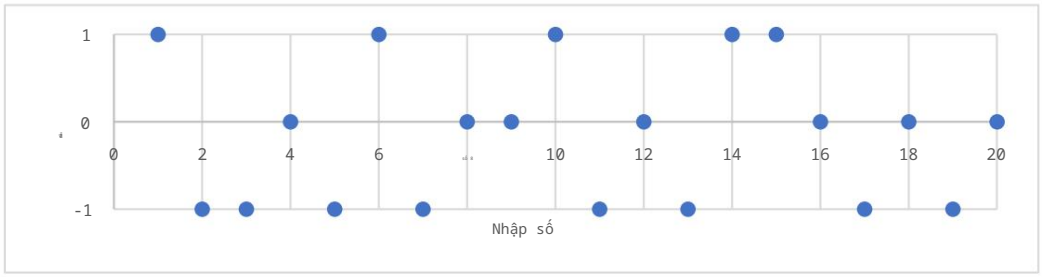
Bảng 1 Bảng viết tắt.

| Các từ viết tắt | Mô tả |
|---|---|
| PA | Địa chỉ trư ớc |
| CA | Địa chỉ hiện tại |
| CTM | Phút thời gian hiện tại |
| NA | Địa chỉ mới |

Định nghĩa 1: Chúng ta xác định hàm Mobius hoặc ( ) cho mỗi đầu vào của = { , , , . } với ba đầu ra { , , } trong a theo cách mà chúng ta coi ( ) là căn bậc n của đơn vị thứ nhất. Hàm này có ba điều kiện sau:

- ( ) = + if là số nguyên dư ơng không có bình phư ơng có số chẵn đến thừa số thứ nhất.
- ( ) = nếu có thừa số bình phư ơng thứ nhất.
- ( ) = nếu là một số nguyên dư ơng nhỏ hơn với số lẻ đến thừa số nguyên tố.

Một ví dụ về đầu ra của hàm đư ợc đề cập đư ợc hiển thị trong Hình 3.




Hình 3 Đồ thị hàm Mobius.

và sau đây, bằng cách sử dụng chức năng Mobius, chúng tôi sẽ tạo một địa chỉ mới cứ sau ba phút.

Định nghĩa 2: = ([( . )] + % ).

Định nghĩa 3: = ( ).

Định nghĩa 4: = + | |.

Trong các chức năng trên, CA của thiết bị đư ợc sử dụng làm Vector ban đầu. Trư ớc khi bắt đầu thao tác, chúng ta cần thiết lập thời điểm bắt đầu địa chỉ cho giao thức ESB và chúng tôi gọi nó là CA. Sau đó, chúng tôi tính tích CA của ngày 8/9. Lý do sử dụng 9/8 là để đồng thời tăng giá trị như ng không vư ợt quá không gian đư ợc trích xuất cho không gian địa chỉ vì chúng tôi có giới hạn không gian dựa trên tải trọng của gói khung. Nó chỉ đơn giản là một nỗ lực nhằm thực hiện một cơ chế xáo trộn liên tục địa chỉ đư ợc sử dụng trong giao thức ESB. Tiếp theo, bằng cách thiết lập chức năng Mobius, chúng tôi cố gắng tạo ra sự hỗn loạn trong hoạt động của chức năng của mình. Ta tính giá trị tuyệt đối của kết quả Mobius chức năng làm cho việc đoán số trở nên phức tạp hơn và thêm nó vào PA để tạo địa chỉ mới. Quá trình này diễn ra mỗi ba phút. Việc chọn số ba và số năm trong cơ chế này chỉ là do chúng ta cần hai số khác nhau. Mặt khác tay, thay vì số ba, chúng ta có thể chọn ít số hơn để xáo trộn địa chỉ nhanh hơn. Trong phư ơng pháp này, chúng tôi chỉ đơn giản cố gắng đảm bảo khả năng xáo trộn địa chỉ thư ờng xuyên cho giao thức ESB. Tuy nhiên, trư ớc đây, trong trư ờng hợp này, một hoạt động tư ơng tự đã không đư ợc thực hiện. như ng trong lĩnh vực mạng máy tính, các hàm lư ợng giác, hàm mũ và logarit đã đư ợc sử dụng rất nhiều để nhận ra xáo trộn địa chỉ với mô hình nhảy.

Để chứng minh tính hiệu quả của phư ơng pháp này, chúng ta phải kết luận rằng đối thủ phải đối mặt với thách thức trong kiểu tấn công này (các kiểu tấn công). các cuộc tấn công phân tích mạng, DoS, SYN Flood, v.v.).

Như một kịch bản mẫu, hãy xem xét một mạng đơn giản bao gồm nút phát T và nút thu R. Sử dụng mô hình đã đề cập ở trên phương pháp xáo trộn địa chỉ, địa chỉ của R được xáo trộn cứ sau 3 phút. Giả sử địa chỉ đầu tiên của R là 200 thì dựa trên NA công thức xác định ta thu được Bảng 2.

Bảng 2 Ví dụ về các địa chỉ được tạo.

| Địa chỉ | Phút |
|---|---|
| 200 | 0 |
| 225 | 3 |
| 256 | 6 |
| 289 | 9 |

Lúc đầu ta có địa chỉ 200 là địa chỉ đầu tiên, sau 3 phút sẽ là địa chỉ 255, các địa chỉ còn lại cũng vậy sẽ thay đổi. Giả sử kẻ xâm nhập C muốn sử dụng tấn công SYN Flood hoặc bất kỳ loại tấn công DoS nào để chiếm đoạt tài nguyên của R. hệ thống. C phải tính toán địa chỉ của R cùng một lúc trong mỗi chu kỳ rồi gửi các gói SYN tới nó, việc này thường rất tốn kém cho anh ấy. C nên tính toán NA và cập nhật các gói của nó bằng cách quét và phân tích mạng cũng như lưu lượng truy cập của nó. Đồng thời, R là đang có ý định vào NA. Thật tốt khi C chờ đợi và phân tích đầy đủ mạng và hình thành một chuỗi địa chỉ, nhưng nó gặp phải vấn đề trong việc hình thành tỉ số chung của hàm số. Mặt khác, nó thậm chí có thể gặp vấn đề trong việc tìm ra địa chỉ chính. Vì Ví dụ: nếu chúng tôi giả sử rằng C phân tích 50 địa chỉ mỗi phút thì sẽ chỉ mất 4 phút để đến địa chỉ ban đầu của chúng tôi. Bây giờ, với tư cách là một một bài toán, chúng ta biết rằng hàm Mobius là một hàm của lý thuyết số mà chúng ta đã sử dụng để xáo trộn địa chỉ. Nút R tính toán địa chỉ mới của nó cứ sau ba phút. Chúng tôi biết rằng các cuộc tấn công DoS dưới bất kỳ hình thức nào đều dựa trên địa chỉ tĩnh.

Định lý 1: Hàm Mobius có tính chất ngẫu nhiên. Nghĩa là, với mọi số nguyên dương n, xác suất để μ(n) bằng một các giá trị 1, 0 hoặc -1 không bằng nhau.

Định lý 2: Hàm Mobius là hàm toán học bất đối xứng và với cả hai số m và n thì xác suất μ(m) = μ(n) là rất thấp.

Định lý 3: Hàm Mobius có tính chất gián đoạn và với mỗi n thì xác suất μ(n) = μ(n+1) là rất thấp.

Với 3 định lý trên, có thể nói hàm Mobius khiến các NA của R xáo trộn một cách ngẫu nhiên, không đối xứng, và không liên tục trong mỗi khoảng thời gian, và điều này có nghĩa là đối thủ C không thể tìm thấy một mẫu cụ thể để xáo trộn địa chỉ bằng cách sử dụng thuật toán dự đoán hoặc hồi quy. Kết quả là các cuộc tấn công DoS chống lại phương pháp này trở nên kém hiệu quả và khó khăn hơn rất nhiều.

Vấn đề cơ bản tiếp theo để tạo ra sự đồng bộ ở cả hai phía trong giao tiếp là phải có cùng một đồng hồ. Đề xuất của chúng tôi để tăng độ chính xác là lấy giá trị thời gian chính xác từ yếu tố thứ ba, chẳng hạn như Hệ thống vệ tinh dẫn đường toàn cầu (GNSS) hoặc GPS để có được CT chính xác Một điểm quan trọng là trong các giao thức GPS, do khung thông báo của chúng, chúng cung cấp cho chúng ta thời gian ở dạng thô và tách biệt. dưới dạng này, chúng tôi chỉ sử dụng giá trị phút của giờ để khiến việc đoán địa chỉ của chúng tôi trở nên phức tạp hơn. Trong trường hợp này, cả hai bên sẽ biết về cơ chế xáo trộn địa chỉ của nhau mà không truyền địa chỉ hiện tại hoặc tương lai của nhau trên đường truyền mạng, làm tăng yếu tố bảo mật.

Nếu cơ chế này được thiết lập để duy trì tính sẵn sàng thì đối thủ sẽ phải đối mặt với thách thức nghiêm trọng đối với hầu hết các cuộc tấn công, đặc biệt là Các cuộc tấn công DoS. chúng tôi cho rằng các phương pháp MTD tương tự như phương pháp của chúng tôi, có thể được sử dụng trong UAV, máy bay không người lái và các hệ thống IoT hoặc WSN quan trọng vì những phương pháp như vậy rất đơn giản, nhẹ nhàng và tốt cho nguồn lực hạn chế.

2) Thiết lập trách nhiệm giải trình với xác thực ngư ời dùng/nút chống lại các cuộc tấn công thay đổi danh tính, Sybil và mạo danh

Sau đây, để hoàn thiện cơ chế đề xuất nhẹ, ít tốn kém và phù hợp với các hệ thống dựa trên IoT hoặc

Các WSN có tài nguyên hạn chế đang sử dụng giá trị bí mật an toàn (SSV) làm mật khẩu mà cả hai bên liên lạc hoặc thậm chí các bên khác

trong một hệ thống phân tán đều biết về nó. Để xác thực lặp đi lặp lại các bên, điểm nhấn trong phư ơng pháp này là lặp đi lặp lại và liên tục.

xác thực trong mỗi tin nhắn. Lư u ý rằng số lư ợng SSV này phải đư ợc cấp cho các nút mạng bởi một ngư ời hoặc nhóm đáng tin cậy

bởi vì nếu điều này đư ợc đặt bởi ngư ời dùng bình thư ờng của hệ thống này, hầu hết mọi ngư ời có xu hư ớng chọn một mật khẩu đơn giản để tránh ghi nhớ những mật khẩu phức tạp.

mật khẩu [41,42]. Mặt khác, một ngày nào đó một ngư ời có thể xuất hiện như một ngư ời nội bộ độc hại, cuối cùng dẫn đến việc mạo danh

các cuộc tấn công. Đề xuất của chúng tôi để tạo ra giá trị bí mật an toàn này là sử dụng mẫu ASCII, trong đó có 95 ký tự và có thể đư ợc

đư ợc sử dụng để tạo SSV này. 95 ký tự này bao gồm 52 chữ cái tiếng Anh viết hoa và viết thư ờng, 10 số và 33 ký hiệu. Vì

tăng độ phức tạp của việc đoán mật khẩu nhanh ngay cả với máy tính, chúng tôi khuyên bạn nên sử dụng SSV 8 byte để duy trì mức tối thiểu

mức độ an ninh. Ví dụ: SSV phù hợp có thể là giá trị " *a$4D2s6 ". Các gói tin đư ợc gửi từ mỗi ngư ời gửi đến mỗi

ngư ời nhận bao gồm nội dung trong đó thông tin của SSV đư ợc đư a vào đầu tiên và sau đó là thông báo gốc như đư ợc đề cập trong Hình.

4.

| Lời mở đầu<br>1 byte | Địa chỉ<br>3-5 byte | (PCF)<br>9 bit | (SSVu \|\| Tin nhắn gốc) | CRC<br>1-2 byte |
|---|---|---|---|---|

Hình 4 Khung tin nhắn có xác thực nhẹ.

Trư ờng hợp gửi bản tin như vậy ở phía đích, trư ớc tiên ngư ời nhận phải tách biệt hai phần chính của bản tin và phần

SSV và kiểm tra nó để nếu nó đúng thì phần gốc của thông báo sẽ đư ợc xem xét.

3) Thiết lập tính toàn vẹn của tin nhắn bằng mã xác thực tin nhắn (MAC) chống lại các cuộc tấn công giả mạo dữ liệu và

bảo mật với mã hóa chống nghe lén và tấn công MITM

Để thiết lập tính toàn vẹn của tin nhắn, chúng tôi khuyên bạn nên sử dụng phư ơng pháp SipHash. Sở dĩ có sự lựa chọn này là tốc độ phù hợp,

độ phức tạp thấp và tính bảo mật thích hợp của SipHash dựa trên các bảng so sánh. Quan trọng nhất là một số tùy chọn có sẵn khác, chẳng hạn như

như MD5 hoặc SHA1, vốn rất phổ biến và không có độ dài thông báo lớn, đã lỗi thời. Một số khác, có một lớn

đầu ra tóm tắt thông báo sẽ là một thách thức đối với chúng tôi để phù hợp với phần tải trọng của khung thông báo ESB và nó sẽ dẫn đến việc sử dụng

một thuật toán khác để cắt bớt chúng. Ngoài ra, chúng tôi đã đề cập trư ớc đó rằng do tốc độ cao, bảo mật tốt và mức độ chấp nhận cao của công chúng,

chúng tôi sẽ sử dụng thuật toán AES để mã hóa và cụ thể là chúng tôi sẽ sử dụng phư ơng pháp AES-128 cho cơ chế đư ợc đề xuất có

Đầu ra mã hóa 16 byte. Cuối cùng, chúng tôi đã đặt một SSV 8 byte ở giữa phần tải trọng của khung thông báo, đó là

bên cạnh nội dung thư đư ợc mã hóa và MAC đư ợc tạo từ đó. Giá trị MAC này ban đầu đư ợc thêm vào toàn bộ nội dung trong

tải trọng. Vấn đề là MAC có độ dài 8 byte này là kết quả của thuật toán SipHash. Độ dài của tin nhắn gốc

đư ợc bao gồm ở cuối tải trọng cũng phải bằng 16 byte sau khi mã hóa. Chúng tôi có xu hư ớng sử dụng giá trị 16 byte này trong đề xuất của chúng tôi

cơ chế. Như ng điểm chính trong phư ơng pháp này, so với các phư ơng pháp khác mà chúng tôi đã xem xét trong các bài viết liên quan, là việc sử dụng Mã hóa

Sau đó, phư ơng pháp MAC. Mục đích là để ngăn chặn tốt hơn các cuộc tấn công giả mạo dữ liệu. Đầu tiên, chúng tôi mã hóa nội dung của tin nhắn gốc

chứa thông báo chính với AES-128 và sau đó sử dụng thông báo thông báo với SipHash MAC. Với phư ơng pháp này, về phía ngư ời nhận, 11

nếu một tin nhắn giả mạo đã được gửi tới nó, nó không cần phải giải mã tin nhắn để kiểm tra tính toàn vẹn sau đó và nó có thể trực tiếp kiểm tra sự chính trực ở thời điểm hiện tại. Khung thông báo cuối cùng có dạng Hình 5 tương tự như Hình 1, nhưng tải trọng an toàn là MAC || SSVu || E (Khóa [Tin nhắn gốc]).

| Lời mở đầu 1 byte | Địa chỉ 3-5- Byte | (PCF) 9 bit | Tải trọng an toàn | CRC 1-2 byte |
|---|---|---|---|---|

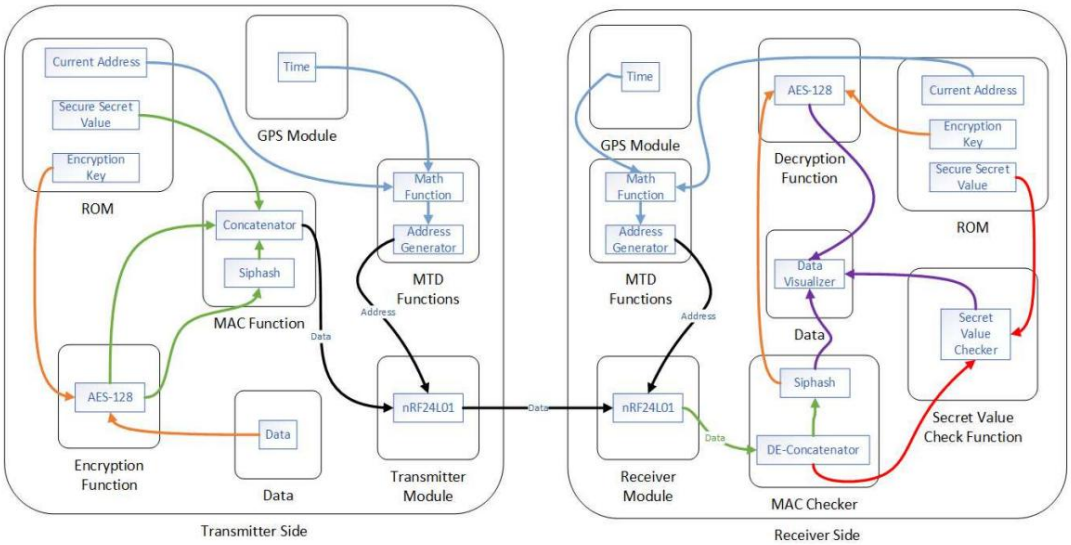
Hình 5 Khung thông báo được đề xuất cuối cùng cho giao thức Shock Burst nâng cao.

Ngoài ra, trọng tải an toàn được đề xuất của cơ chế bảo mật của chúng tôi được hiển thị trong Hình 6.

| Thông báo MAC 8-Byte | SSVu 8 byte | E (Khóa [Tin nhắn gốc]) 16 byte |
|---|---|---|

Hình 6 Tải trọng an toàn được đề xuất ở các phần riêng biệt.

Chúng tôi sử dụng sơ đồ khối để mô tả cơ chế sử dụng mô-đun GPS như được nêu trong Hình 7 Như có thể thấy, trong sơ đồ khối được hiển thị trong Hình 7, chúng tôi giả định rằng chúng tôi có thiết bị phát và thiết bị thu, cả hai đều dựa trên mạng ESB giao thức truyền thông và sử dụng mô-đun truyền thông nRF24L01. Chúng ta có thể sử dụng bộ phát và bộ thu riêng biệt hoặc bộ thu phát. Chúng ta nên có hai thiết bị làm bộ thu phát để gửi hoặc nhận dữ liệu đồng thời.




Hình 7 Sơ đồ khối của cơ chế đề xuất.

Như chúng ta có thể thấy trong mã giả trong Bảng 3., lúc đầu, khóa mã hóa và giá trị SSV sẽ được tạo bởi một cơ quan đáng tin cậy và sẽ được nhúng vào bộ vi điều khiển của máy phát và máy thu. Ở cả phía máy phát và máy thu, trong khi bật mô-đun, thời gian hiện tại được nhận từ GPS và địa chỉ mới được tạo ra sau mỗi ba phút. sau đó, từ máy phát, thông báo M được mã hóa và bản tóm tắt MAC được tạo từ văn bản mật mã (Mã hóa rồi MAC). Cả tin nhắn được mã hóa và MAC và SSV sẽ được gửi đến người nhận. Ở phía nhận, tin nhắn được chia thành ba phần, đầu tiên, giá trị MAC là được xác nhận thì giá trị SSV sẽ được xác nhận và nếu cả hai đều được xác nhận thì tin nhắn gốc sẽ được giải mã và sẽ được sử dụng.

Như được trình bày trong Bảng 4, do sự hiện diện của kỹ thuật xáo trộn địa chỉ và cách sử dụng nó nên có thể tránh được tất cả các loại DoS. tấn công ở mức độ lớn. Trên thực tế, bất chấp tính năng như vậy, kẻ tấn công phải tìm kiếm địa chỉ truyền dữ liệu trong không gian địa chỉ 5 byte. Nếu kẻ tấn công tìm thấy nó, anh ta sẽ có cơ hội hạn chế để phân tích mạng vì địa chỉ sẽ sớm bị xáo trộn trở lại.

Bằng cách sử dụng hàm Mobius, chúng tôi đã cố gắng tạo một điều kiện trong hành vi xáo trộn địa chỉ trong đó NA không thể dễ dàng đoán được và tạo ra một loại hỗn loạn. Do đó, kẻ tấn công phải trải qua một quy trình phức tạp với cơ hội hạn chế để tiếp cận CA của chúng tôi. Trong trường hợp này, chúng tôi có thể khẳng định rằng chúng tôi đã tạo ra một giải pháp phòng thủ phù hợp trước các cuộc tấn công DoS. Trong bước tiếp theo, nếu kẻ tấn công có thể đoán CA và thậm chí một chuỗi địa chỉ, chúng ta sẽ có khả năng trở thành nạn nhân của một cuộc tấn công DoS. Tuy nhiên, chúng tôi đã xem xét một số thử nghiệm sử dụng một số hệ thống trí tuệ nhân tạo để đoán chuỗi địa chỉ của chúng tôi trong các tình huống khác nhau nhưng không thành công.

Bảng 3 Mã giả của cơ chế bảo mật được đề xuất.

| Trung tâm đăng ký là đáng tin cậy Thẩm quyền | Phía máy phát | Bên nhận |
|---|---|---|
| + Tạo SSVu, Khóa mã hóa và Khóa MAC.<br>+ Triển khai SSVu và Keys trên thiết bị. | | |
| | + Lấy thời gian của GPS.<br>+ Mỗi 3 phút: tính PA, μ(PA), NA và xáo trộn địa chỉ.<br><br>Khi sử dụng địa chỉ mới: +<br>Tạo tin nhắn mới M.<br>+ Tính M'= E (Khóa [M]) bằng AES-128.<br>+ Tính MAC(M') bằng thuật toán Siphash.<br><br>+ M"= MAC(M') \|\| SSVu \|\| M'.<br>+ Gửi M" tới người nhận bằng nRF24L01. | + Lấy thời gian của GPS.<br>+ Mỗi 3 phút: tính PA, μ(PA), NA và xáo trộn địa chỉ.<br><br>Trong khi sử dụng địa chỉ mới: +<br>Lấy M" từ Bộ phát sử dụng nRF24L01.<br><br>+ Tách thông điệp thành 3 phần M"= MAC(M')/ SSVu /M'.<br>+ Xác minh SSVu.<br>+ Kiểm tra MAC của M' bằng thuật toán Siphash.<br><br>+ M= Giải mã M' bằng AES-128.<br>+ Sử dụng lệnh hoặc dữ liệu trong M. |

Các cuộc tấn công thành công không xảy ra miễn là các biến số của chúng tôi, bao gồm cả địa chỉ phút và địa chỉ ban đầu, vẫn được giữ bí mật. Điều này có nghĩa là rằng một người không thể đoán được rằng một trong những biến số ảnh hưởng đến việc xáo trộn địa chỉ là thời gian và cũng có một giá trị địa chỉ ban đầu. Ngoài ra, do sử dụng cùng cơ chế xáo trộn địa chỉ nên việc xảy ra các cuộc tấn công khác cũng sẽ là thách thức nghiêm trọng đối với kẻ tấn công. Cụ thể, các cuộc tấn công ảnh hưởng đến các mô-đun truyền thông không dây dựa trên giao thức truyền thông ESB có thể phải đối mặt với một thách thức nghiêm trọng với kỹ thuật này, ngoại trừ các cuộc tấn công dựa trên việc gửi tiếng ồn hoặc gây nhiễu, mà các giải pháp này không hiệu quả. kháng cự. Mặt khác, giả sử, kẻ tấn công có thể lấy được thông tin chi tiết về mạng của chúng tôi bằng cách phân tích các điều kiện này và hình thành chuỗi địa chỉ, sử dụng mã hóa phù hợp dựa trên AES-128, anh ta sẽ mất khả năng thực hiện tấn công MITM hoặc tấn công nghe lén hoạt động miễn là khóa chính của chúng tôi sẽ được tiết lộ. Một trong những tính năng của mã hóa AES-128 là đảm bảo tính bảo mật, vì miễn là khóa mã hóa không bị lộ. Ngoài ra, do sự hiện diện của bản tóm tắt MAC loại SipHash, khả năng xảy ra các cuộc tấn công như việc giả mạo bị loại bỏ và kẻ tấn công khó có thể phá hủy tính toàn vẹn của quá trình gửi tin nhắn của chúng tôi, miễn là hắn không biết chúng tôi sử dụng thuật toán SipHash và khóa là gì. Một kỹ thuật khác trong phương pháp này so với các phương pháp khác là sử dụng mã hóa và MAC. Trong các cách tiếp cận phổ biến mà bạn đã thấy trong phần công việc liên quan, trước tiên, chúng ta đã thấy cài đặt tóm tắt MAC và

sau đó quá trình mã hóa đư ợc áp dụng cho sự kết hợp giữa MAC và tin nhắn gốc. Để thiết lập an ninh chống lại danh tính giả mạo hoặc mạo danh và Tấn công Sybil, chúng tôi sử dụng SSV làm thông tin thiết bị để xác thực thiết bị đó trong mạng. bên trong cuối cùng, vì SSV của thiết bị đư ợc lư u trữ trong bộ vi điều khiển và cũng có sự hiện diện của cơ chế xác thực, nên việc xảy ra Các cuộc tấn công Sybil cũng sẽ là một thách thức nghiêm trọng đối với kẻ thù vì đối với mỗi tin nhắn đư ợc gửi trong mạng, chúng tôi đều có cơ chế xác thực. chư ơng trình nghị sự. Điều đó có nghĩa là một nút độc hại không thể kết nối một số nút độc hại khác với hệ thống của chúng tôi mà không có đủ số lư ợng SSV. Trong cơ chế này, chúng tôi quản lý để tạo một kênh không dây an toàn đồng thời đảm bảo tính bảo mật, tính toàn vẹn thông tin, thời gian đồng bộ hóa, trách nhiệm giải trình và tính sẵn sàng.

Bảng 4 So sánh việc thiết lập cơ chế bảo mật cho phư ơng pháp đề xuất với các phư ơng pháp trư ớc đó.

| Yêu cầu và tính năng bảo mật chống lại nhiều loại tấn công | [17] [18] [19] [20] | Đề xuất Cơ chế |
|---|---|---|
| Yêu cầu về trách nhiệm giải trình (SR-1) | Không Không Không Không | Đúng |
| Yêu cầu về tính toàn vẹn (SR-2) | Có Không Có Không | Đúng |
| Yêu cầu về tính bảo mật (SR-3) | có có có có | Đúng |
| Yêu cầu về tính sẵn có (SR-4) | Không Không Không Không | Đúng |
| Phòng thủ mục tiêu di động (SF-1) | Không Không Không Không | Đúng |
| Xác thực ngư ời dùng/nút (SF-2) | Không Không Không Không | Đúng |
| Tấn công nghe lén (SF-3) | có có có có | Đúng |
| Ngư ời đàn ông tấn công ở giữa (SF-4) | có có có có | Đúng |
| Tấn công Sybil (SF-5) | Không Không Không Không | Đúng |
| Tấn công mạo danh / giả mạo danh tính (SF-6) | Không Không Không Không | Đúng |
| Tấn công từ chối dịch vụ (DoS) (SF-7) | Không Không Không Không | Đúng |
| Tấn công đoán mật khẩu (SF-8) | Không Không Không Không | Đúng |
| Tấn công giả mạo (SF-9) | Có Không Có Không | Đúng |
| Tấn công lũ lụt SYN (SF-10) | Không Không Không Không | Đúng |

## 6. Kết quả thực hiện và thử nghiệm

Để thực hiện cơ chế đề xuất, chúng tôi đã sử dụng nền tảng Arduino và cụ thể là loại Uno bao gồm Vi điều khiển Atmega328p. Trong số các lý do nên sử dụng nền tảng Arduino là giá cả hợp lý, sức mạnh xử lý đủ do thiếu kỳ vọng cao trong quy trình thí nghiệm, dễ sử dụng nền tảng (đặc biệt là số lư ợng thư viện có sẵn cho nền tảng này) và hiệu quả trong các quy trình trong phòng thí nghiệm.

Tuy nhiên, nên công nghiệp hóa thiết kế hiện có, đồng thời thử nghiệm bộ vi điều khiển hỗ trợ đã đề cập của chúng tôi. phư ơng pháp. Tùy thuộc vào mức sử dụng bộ nhớ, sức mạnh xử lý, mức tiêu thụ điện năng và số lư ợng tín hiệu analog và kỹ thuật số các chân trên bộ vi điều khiển, các công nghệ đư ợc hỗ trợ và các thư viện đề xuất sẽ đư ợc nhóm phát triển lựa chọn. Ngoài ra, để Đư ợc hư ởng lợi từ giao thức GPS, chúng tôi đã sử dụng mô-đun GPS NEO6M, hoạt động như một bên thứ ba để nhận thời gian. Mô-đun này ngoài nhận dữ liệu địa lý cũng có những khả năng độc đáo như xác định độ cao so với mực nư ớc biển, vĩ độ, kinh độ, tốc độ của chuyển động và thời gian Greenwich tức thời ở dạng chuẩn hoặc dạng thô [43]. Mô-đun NEO6M sử dụng giao thức truyền thông I2C để kết nối với các linh kiện điện tử khác, bao gồm cả bộ vi điều khiển. Các mô-đun hỗ trợ kiểu giao tiếp này có hai Chân TXD và RXD bên cạnh hai chân cấp nguồn VCC và GND. Thông tin đư ợc gửi từ chân TXD đến vi điều khiển, và thông qua chân RXD, nó nhận đư ợc thông tin cần thiết từ bộ vi điều khiển.

Ngoài ra, để làm việc với giao thức truyền thông ESB, chúng tôi đã sử dụng mô-đun nRF24L01, có khả năng truyền thông tin ở các tốc độ khác nhau lên tới 2 Mbps. Ngoài ra, nếu chúng ta cần tăng chất lượng hoặc phạm vi liên lạc, chúng ta có thể sử dụng các giải pháp khác các mô-đun thuộc họ này, chẳng hạn như nRF24L01+PA+LNA.

Sử dụng phần mềm Fritzing, chúng ta có thể vẽ thiết kế điện tử và ánh xạ các kết nối của các thiết bị điện tử với nhau. Trong bảng 4. và Hình 8 chi tiết và Hình 9 là cách triển khai nguyên mẫu, có thể xem cách kết nối các thành phần điện tử khác nhau với Arduino cho một nút thu phát trong mạng.

Hãy nhớ rằng trong thiết kế này, chúng tôi đã trực tiếp cung cấp năng lượng cho hai mô-đun giao tiếp Neo6M và nRF24L01 từ bộ vi điều khiển, nhưng ở chế độ hiệu quả hơn, tốt hơn là không cung cấp năng lượng từ bộ vi điều khiển. TRÊN mặt khác, điều quan trọng cần biết là điện áp làm việc của Neo6M tương đương với 5 volt và điện áp làm việc của nRF24L01 tương đương với 3,3 volt.

Điều đáng chú ý là các mô-đun giao tiếp nRF24L01 được hưởng lợi từ khả năng phân tán theo mặc định và cuối cùng bạn có thể hưởng lợi từ giao tiếp nhiều-nhiều trong đó [44].

Bảng 4 Kết nối mạch để xây dựng một nút với mô-đun giao tiếp nrf24l01 & mô-đun GPS neo6m với Arduino.

| Loại cổng | Pin cổng | Arduino Uno Pin |
|---|---|---|
| nRf24L01 | MISO | 12 |
| | SCK | 13 |
| | CN | 9 |
| | MOSI | 11 |
| | CSN | 8 |
| | VCC | 3v3 |
| | GND | GND |
| NEO6M | TXD | 4 |
| | RXD | 3 |
| | VCC | 5V |
| | GND | GND |

Để triển khai cơ chế bảo mật được đề xuất trên bộ vi điều khiển Atmega328p trong Arduino, chúng tôi đã sử dụng hai thư viện "SipHash-2-4" và "AESLib Master" trong môi trường Arduino IDE bằng ngôn ngữ C++. Trong thực tế, phương pháp được đề xuất của chúng tôi cho thấy hiệu quả rất tốt. tốc độ hoạt động. Trong phương pháp đề xuất của chúng tôi, thời gian cần thiết cho mỗi lần mã hóa bằng thuật toán AES-128 chỉ là 284 micro giây và thời gian để tính toán thông số MAC chỉ là 864 micro giây, tổng cộng mất tới 1148 micro giây, như chúng ta có thể xem trong Hình 10 và 11.

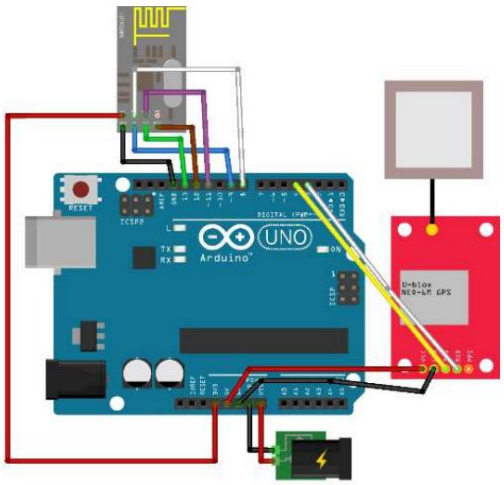
Xét về thời gian thực hiện so với bài báo [19], phương pháp đề xuất của chúng tôi mang lại tốc độ thực hiện cao hơn trên một nền tảng hoàn toàn tương tự như trong Hình 10.

Ngoài ra, về mặt tốc độ thực hiện, phương pháp đề xuất của chúng tôi có thể được so sánh với [17] với giả định rằng chúng tôi biết rằng bộ vi điều khiển được sử dụng trong nghiên cứu của họ yếu hơn gần hai lần so với bộ vi điều khiển mà chúng tôi sử dụng, nhưng việc so sánh cả hai mẫu về tốc độ thực hiện, trong khi phương pháp [17] sử dụng 5 chế độ làm việc và chúng tôi chỉ sử dụng một chế độ, là rất có ý nghĩa thể hiện trong hình 11.

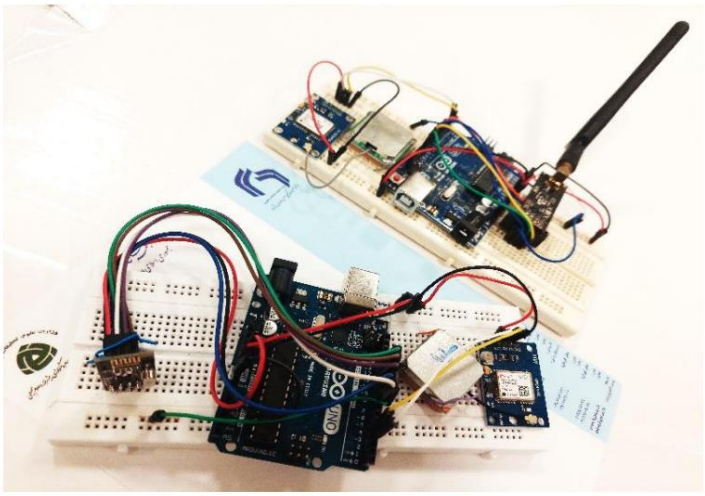
Cuối cùng, cần đề cập rằng trong mạch chúng tôi xây dựng, bất kể quá trình xáo trộn địa chỉ và sự hiện diện của Mô-đun GPS, mức tiêu thụ dòng điện trung bình bằng 0,33 mA và nếu chúng ta thêm mô-đun GPS để xáo trộn địa chỉ thường xuyên, nó sẽ có mức tiêu thụ dòng điện trung bình là 0,90 mA.

Ngoài ra, mức tiêu thụ điện là 3,33 mW khi không có GPS và xáo trộn địa chỉ và 1,11 mW khi không có GPS và xáo trộn địa chỉ.

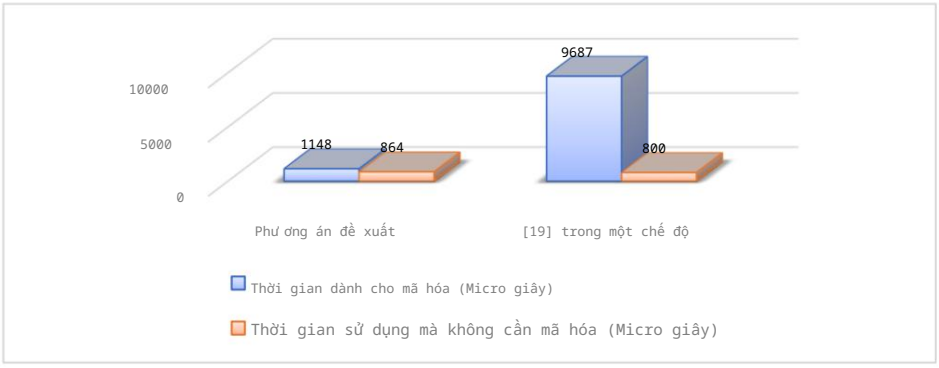
Ngoài ra, trong Hình 12, chúng tôi so sánh chi phí của hệ thống được đề xuất với một số phương pháp khác.



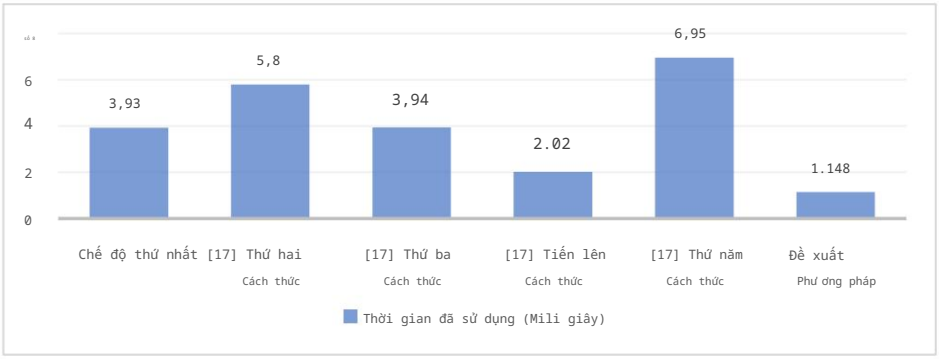

Hình 8 Mạch nguyên mẫu được đề xuất.



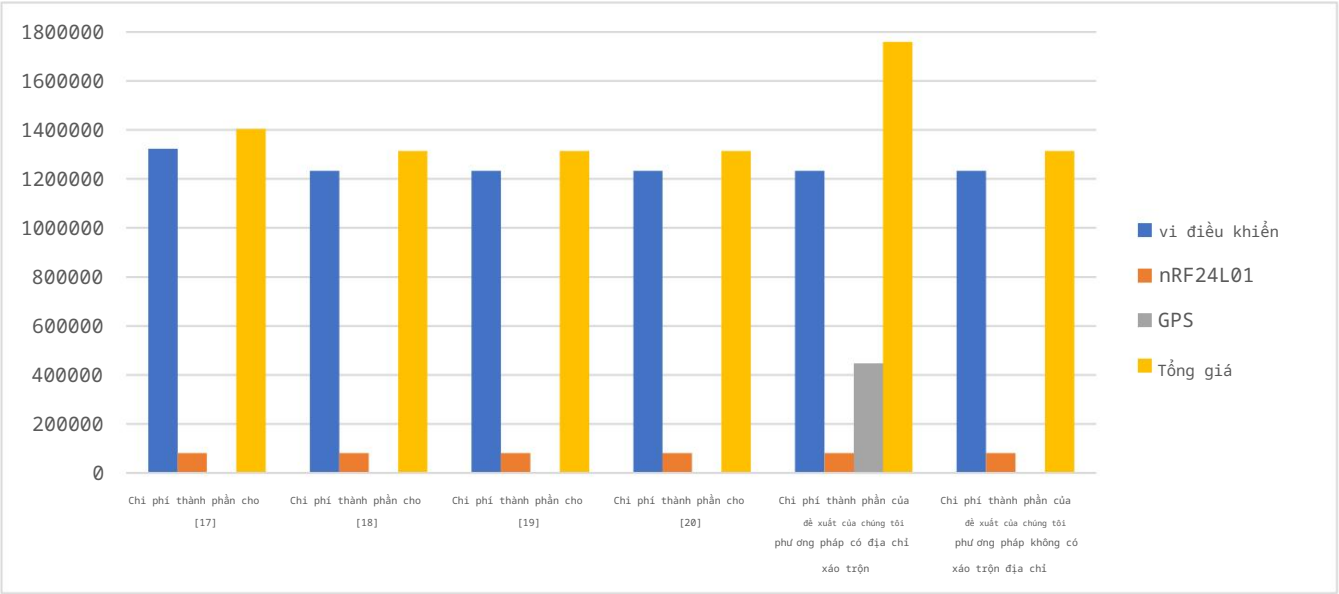
Hình 9 Các nguyên mẫu được triển khai.




Hình 10 Thời gian sử dụng của phương pháp đề xuất so với [19].




Hình 11 Thời gian sử dụng của phương pháp đề xuất so với [17].




Hình 12 Sơ đồ so sánh chi phí linh kiện

## 7. Kết luận và công việc trong tương lai

Tầm quan trọng của việc thiết lập bảo mật trong các lĩnh vực IoT, WSN và tất cả các lĩnh vực liên quan ngày nay không còn là bí mật đối với bất kỳ ai. Trong bài viết này, những nỗ lực đã được thực hiện nhằm cung cấp tính bảo mật, xác thực, tính toàn vẹn của thông báo và mức độ truy cập cao cùng với với tốc độ và mức tiêu thụ năng lượng phù hợp. Trước đây, nhiều sơ đồ bảo mật đã được trình bày cho các giao thức mạng khác nhau trong lĩnh vực IoT và WSN, tuy nhiên vấn đề bảo mật trong phương pháp đề xuất của chúng tôi có một số điểm khác biệt. Trong Cơ chế đề xuất của chúng tôi, dựa trên giao thức truyền thông ESB, chúng tôi có thể cung cấp một cơ chế bảo mật, ngoài tính nhẹ, còn có khả năng được sử dụng trong bất kỳ ứng dụng nào của giao thức liên lạc ESB, bao gồm cả máy bay không người lái và đặc biệt là máy bay không người lái phương tiện giao thông (UAV), hệ thống cơ khí, hệ thống công nghiệp, IoT, WSN đóng vai trò an toàn hơn trước.

Đối với công việc trong tương lai, chúng tôi tin rằng nên nghĩ đến một cơ chế đối phó với các cuộc tấn công gây nhiễu. Ngoài ra, nếu rất nhanh và phương pháp mã hóa được chấp nhận an toàn được cung cấp, chúng có thể được sử dụng thay vì AES-128. Mặt khác, nếu có một thuật toán tốt hơn được tạo ra hơn Siphash, cho phép tốc độ cao hơn, bảo mật hơn và độ dài thông báo MAC phù hợp, nó có thể được thay thế bằng Siphash. Ngoài ra trong việc xác thực, để tăng tính bảo mật cho SSV được truyền đi trên mạng, chúng ta có thể sử dụng SALT. Ngoài ra, để đối phó phát lại các cuộc tấn công, dấu thời gian có thể được thêm vào gói để ngăn chặn các cuộc tấn công phát lại.

Với tất cả các cách giải thích, cơ chế đề xuất của chúng tôi cho giao thức truyền thông ESB đã phản hồi tốt và chúng tôi đã cố gắng tạo ra một kênh bảo mật có vẻ an toàn trước ví dụ tấn công đã đề cập, theo một phương pháp, miễn là chúng ta biết thông tin ban đầu địa chỉ là và chúng tôi cũng biết hai hoặc ba địa chỉ tiếp theo, không những chúng tôi không thể tạo chuỗi địa chỉ chính xác dựa trên kiến thức toán học với các hàm toán học mà cả với hệ thống trí tuệ nhân tạo dựa trên Bing cũng không thể tạo thành một dãy địa chỉ chính xác và không thành công. Cuối cùng, điều đáng nói là về phương pháp xáo trộn địa chỉ, để sử dụng lâu dài truyền thông, cần xác định một ngưỡng thời gian để các địa chỉ được đặt lại và đầu ra của chức năng xáo trộn địa chỉ không bao gồm số lượng rất lớn.

1. Khan, MA, & Abuhasel, KA (2021). Khung kích thư ớc siêu dữ liệu nâng cao cho Internet vạn vật công nghiệp không đồng nhất. Trí tuệ tính toán, 37(3), 1367-1387.
2. Ojha, T., Misra, S., & Raghuwanshi, NS (2021). Internet vạn vật cho các ứng dụng nông nghiệp: Công nghệ tiên tiến. Internet IEEE Tạp chí sự vật, 8(14), 10973-10997.
3. Khan, MA (2020). Khung IoT để dự đoán bệnh tim dựa trên bộ phân loại MDCNN. Truy cập IEEE, 8, 34717-34727.
4. Estrada-López, JJ, Castillo-Atoche, AA, Vázquez-Castillo, J., & Sánchez-Sinencio, E. (2018). Hệ thống ư ớc tính thông số đất thông minh sử dụng mạng cảm biến không dây tự động với chiến lư ợc quản lý năng lư ợng động. Tạp chí cảm biến IEEE, 18(21), 8913-8923.
5. Hassan, WH (2019). Nghiên cứu hiện tại về bảo mật Internet of Things (IoT): Một cuộc khảo sát. Mạng máy tính, 148, 283-294.
6. Bálint, Á., & Sárosi, J. (2016). Thiết kế và thi công hệ thống đèn led điều khiển bằng sóng vô tuyến. Analecta Technica Szegedinensia, 10(1), 29-34.
7. Ghosh, S., Ghosh, K., Karamakar, S., Prasad, S., Debabhuti, N., Sharma, P., và những ngư ời khác. Phát triển kiến trúc mạnh mẽ dựa trên IOT để giám sát môi trư ờng bằng UAV. Năm 2019 Hội nghị quốc tế Hội đồng Ấn Độ lần thứ 16 của IEEE (INDICON), 2019 (trang 1-4): IEEE
8. Lv, D., Liang, C., & Zhang, Y. (2023). Nghiên cứu thiết kế UAV 4 cánh quạt dựa trên Cascade PID. Những tiến bộ trong nhân tạo Hệ thống Y tế và Giáo dục VI (trang 88-99): Springer.
9. Kulasekara, V., Balasooriya, S., Chandran, J., & Kavalchuk, I. Thiết kế mạng không dây dựa trên NRF24L01 công suất thấp mới lạ dành cho robot tự hành. Năm 2019, Hội nghị Truyền thông Châu Á-Thái Bình Dư ơng (APCC) lần thứ 25, 2019 (trang 342-346): IEEE 10. Luo, Y.-B., Wang, B.-S., Wang, X.-F., Hu , X.-F., Cai, G.-L., & Sun, H. RPAH: Nhảy địa chỉ và cổng ngẫu nhiên để ngăn chặn đối thủ bên trong và bên ngoài. Năm 2015 IEEE Trustcom/BigDataSE/ISPA, 2015 (Tập 1, trang 263-270): IEEE 11. MacFarland, DC, & Shue, CA SDN shuffle: Tạo hệ thống phòng thủ mục tiêu di động bằng cách sử dụng phần mềm đư ợc xác định trên máy chủ mạng. Trong Kỷ yếu Hội thảo ACM lần thứ hai về Phòng thủ mục tiêu di động, 2015 (trang 37-41)
12. Wang, F., Wang, H., Wang, X., & Su, J. (2012). Một cách tiếp cận đa tầng mới để phát hiện các cuộc tấn công DDoS tinh vi. Toán học và Mô hình máy tính, 55(1-2), 198-213.
13. Benyezza, H., Bouhedda, M., Kara, R., & Rebouh, S. (2023). Nền tảng thông minh dựa trên IoT và WSN để giám sát và kiểm soát của nhà kính trong bối cảnh nông nghiệp chính xác. Internet vạn vật, 23, 100830.
14. Mahbub, M. (2020). Khái niệm nông nghiệp thông minh dựa trên thiết bị điện tử nhúng thông minh, internet vạn vật và cảm biến không dây mạng. Internet vạn vật, 9, 100161.
15. Zhang, L., Suzuki, H., & Koyama, A. (2021). Nhận dạng thông tin bữa ăn bằng cách sử dụng mạng thần kinh hồi quy và tái phát có kiểm soát đơn vị. Internet vạn vật, 13, 100358.
16. Sokullu, R., Akkaş, MA, & Demir, E. (2020). IoT hỗ trợ nhà thông minh cho ngư ời già. Internet vạn vật, 11, 100239.
17. Selimis, G., Huang, L., Massé, F., Tsekoura, I., Ashouei, M., Catthoor, F., et al. (2011). Một chư ơng trình bảo mật nhẹ dành cho Mạng vùng cơ thể không dây: thiết kế, đánh giá năng lư ợng và thiết kế bộ vi xử lý đề xuất. Tạp chí hệ thống y tế, 35(5), 1289-1298.
18. Babu, PS, & Panda, BS Bảo mật và xác thực trọng lư ợng nhẹ trong Mạng vùng cơ thể không dây (Wban). Năm 2020 Hội nghị quốc tế về Khoa học, Kỹ thuật và Ứng dụng Máy tính (ICCSEA), 2020 (trang 1-7): IEEE 19. Rivera, D., García, A., Martín-Ruiz, ML, Alarcos, B., Velasco, JR, & Oliva, AG (2019). Bảo mật thông tin liên lạc và dữ liệu đư ợc bảo vệ cho nền tảng đồ chơi thông minh Internet of Things. Tạp chí Internet vạn vật của IEEE, 6(2), 3785-3795.
20. Kanthi, M., & Dilli, R. (2023). Hệ thống đèn đư ờng thông minh sử dụng ứng dụng di động: phát hiện và chẩn đoán lỗi an toàn với quyền lực tối ư u. Mạng không dây, 1-14.
21. Đội, ME (2015). Kết thúc hỗ trợ cho mật mã RC4 trong Microsoft Edge và Internet Explorer 11. https://blogs.windows.com/msedgedev/2015/09/01/ending-support-for-the-rc4-cipher-in-microsoft-edge-and-internet-explorer-11/.
22. Liu, Y., & Han, X. Phân tích tốc độ truyền tối đa dựa trên hệ thống chip nRF24L01. Năm 2010 Hội nghị quốc tế lần thứ 2 về Kỹ thuật thông tin và Khoa học máy tính, 2010 (trang 1-3): IEEE
23. Chuyên sâu: Cách hoạt động và giao diện của Mô-đun không dây nRF24L01+ với Arduino (2018). https://lastphútengineers.com/nrf24l01-arduino-không dây-giao tiếp/.
24. nRF24L01. https://www.nordicsemi.com/products/nrf24-series.
25. Walters, JP, Liang, Z., Shi, W., & Chaudhary, V. (2007). An ninh mạng cảm biến không dây: Một cuộc khảo sát. Trong Bảo mật trong điện toán phân tán, lư ới, di động và lan tỏa (trang 367-409): Ấn phẩm Auerbach.
26. William, S. (2011). Những yếu tố cần thiết về an ninh mạng: Ứng dụng và tiêu chuẩn (Dành cho VTU): Pearson Education India.
27. Van Steen, M., & Tanenbaum, AS (2017). Hệ thống phân phối: Maarten van Steen Leiden, Hà Lan.
28. Tsao, K.-Y., Girdler, T., & Vassilakis, VG (2022). Khảo sát các mối đe dọa an ninh mạng và giải pháp cho thông tin liên lạc bằng UAV và các mạng ad-hoc bay. Mạng Ad Hoc, 133, 102894.
29. Wheeler, E. (2011). Quản lý rủi ro bảo mật: Xây dựng chư ơng trình quản lý rủi ro bảo mật thông tin từ đầu: Khác.
30. van Oorschot, PC (2020). Bảo mật máy tính và Internet: Springer.
31. Halak, B., Yilmaz, Y., & Shiu, D. (2022). Phân tích so sánh chi phí năng lư ợng của mã hóa bất đối xứng và dựa trên mã hóa đối xứng các ứng dụng bảo mật. Truy cập IEEE, 10, 76707-76719.

32. Yassein, MB, Aljawarneh, S., Qawasmeh, E., Mardini, W., & Khamayseh, Y. Nghiên cứu toàn diện về khóa đối xứng và thuật toán mã hóa khóa bất đối xứng. Hội nghị quốc tế về kỹ thuật và công nghệ (ICET) năm 2017 (trang 12) 1-7): IEEE
33. Mousavi, SK, Ghaffari, A., Besharat, S., & Afshari, H. (2021). Bảo mật internet vạn vật dựa trên thuật toán mã hóa: một cuộc khảo sát. Mạng không dây, 27, 1515-1555.
34. Abood, OG, & Guirguis, SK (2018). Khảo sát về thuật toán mật mã. Tạp chí khoa học và nghiên cứu quốc tế Ấn phẩm, 8(7), 495-516.
35. NIST (2022). NIST ngừng sử dụng thuật toán mã hóa SHA-1 https://www.nist.gov/news-events/news/2022/12/nist-retires-sha-1-thuật toán mật mã.
36. Hagenlocher, P. (2018). Hiệu suất của mã xác thực tin nhắn cho ethernet an toàn. Mạng, 27.
37. Aumasson, J.-P., & Bernstein, DJ SipHash: PRF đầu vào ngắn nhanh. Tại Hội nghị Quốc tế về Mật mã học ở Ấn Độ, 2012 (trang 489-508): Springer
38. Wang, T.-Z., Wang, H.-M., Liu, B., Ding, B., Zhang, J., & Shi, P.-C. (2012). Phân tích sâu hơn về cuộc tấn công sybil trong việc giảm thiểu các botnet ngang hàng. Giao dịch KSII trên Internet và Hệ thống Thông tin (TIIS), 6(10), 2731-2749.
39. Zheng, Y., Li, Z., Xu, X., & Zhao, Q. (2022). Phòng thủ năng động trong an ninh mạng: Kỹ thuật, phương pháp và thách thức. Mạng và Truyền thông Kỹ thuật số, 8(4), 422-435.
40. Cai, G., Wang, B., Wang, X., Yuan, Y., & Li, S. Giới thiệu về xáo trộn địa chỉ mạng. Năm 2016 Hội nghị quốc tế lần thứ 18 về công nghệ truyền thông tiên tiến (ICACT), 2016 (trang 185-190): IEEE 41. He, D., & Hu, H. (2013). Phân tích
mật mã sơ đồ xác thực người dùng từ xa dựa trên ID động với khả năng kiểm soát truy cập cho môi trường nhiều máy chủ. GIAO DỊCH IEICE về Thông tin và Hệ thống, 96(1), 138-140.
42. He, D., Wu, S., & Chen, J. (2012). Lưu ý về 'Thiết kế sơ đồ cập nhật và xác thực mật khẩu cải tiến dựa trên hình elip mật mã đường cong'. Mô hình toán học và máy tính, 3(55), 1661-1664.
43. Buchli, B., Sutton, F., & Beutel, J. Nút mạng cảm biến không dây được trang bị GPS cho các ứng dụng định vị có độ chính xác cao. Trong Mạng cảm biến không dây: Hội nghị Châu Âu lần thứ 9, EWSN 2012, Trento, Ý, ngày 15-17 tháng 2 năm 2012. Kỷ yếu ngày 9 năm 2012 (trang 179-195): Springer
44. Gia, TN, Dhaou, IB, Ali, M., Rahmani, AM, Westerlund, T., Liljeberg, P., và cộng sự. (2019). Hệ thống IoT hỗ trợ sương mù tiết kiệm năng lượng để theo dõi bệnh nhân tiểu đường mắc bệnh tim mạch. Hệ thống máy tính thế hệ tương lai, 93, 198-211.

Aref Ayati tốt nghiệp Đại học Isfahan với bằng Cử nhân khoa học máy tính vào năm 2020 và lấy bằng Thạc sĩ Kỹ thuật Công nghệ Thông tin vào năm 2023 tại Đại học Công nghệ Tiên tiến Kerman của Iran. Các lĩnh vực quan tâm của ông bao gồm quản lý CNTT, IoT, WSN, Hệ thống UAV, Mạng máy tính và bảo mật.

Hamid Reza Naji là phó giáo sư kỹ thuật máy tính tại Đại học Công nghệ tiên tiến, Iran. Mối quan tâm nghiên cứu của ông bao gồm các hệ thống nhúng, hệ thống phân tán, song song và đa tác nhân, mạng và bảo mật. Tiến sĩ Naji có bằng tiến sĩ. về kỹ thuật máy tính của Đại học Alabama ở Huntsville, Hoa Kỳ.