# KHẢO SÁT CÁC VẤN ĐỀ BẢO MẬT TRONG MẠNG CẢM BIẾN KHÔNG DÂY

**Nguyễn Văn Trường[*], Dương Tuấn Anh[*], Nguyễn Quý Sỹ[+]**

[*]VNPT Thừa Thiên Huế
[+]Học viện Công nghệ Bưu chính Viễn thông

***Tóm tắt:*** Trong những năm gần đây, mạng cảm biến không dây WSN (Wireless Sensor Network) đang nổi lên như một lĩnh vực nghiên cứu đầy hứa hẹn do chi phí cảm biến ngày càng thấp, phạm vi ứng dụng đa dạng và dễ dàng triển khai. Các WSN tập trung vào việc cảm nhận và truyền dữ liệu theo thời gian thực từ môi trường giám sát cụ thể về các hệ thống đầu cuối để xử lý và phân tích. Tuy nhiên, thông tin giám sát thường nhạy cảm, các cảm biến thường hoạt động trong môi trường khắc nghiệt và không được giám sát, do đó mối quan tâm về bảo mật và quyền riêng tư đối với các hệ thống WSN đã trở thành một chủ đề luôn được thảo luận sôi nổi. Trong bài viết này, chúng tôi trình bày một cuộc khảo sát về các vấn đề bảo mật đối với WSN. Đầu tiên, chúng tôi giới thiệu tổng quan về WSN, các ràng buộc và yêu cầu bảo mật. Sau đó, chúng tôi trình bày một cái nhìn toàn diện về các mối đe dọa đối với các WSN và phân loại các phương thức phòng thủ dựa trên các lớp theo mô hình OSI. Ngoài ra, chúng tôi cũng tóm tắt các kỹ thuật và phương pháp bảo mật mới được công bố trong những năm gần đây và chỉ ra các vấn đề và hướng nghiên cứu mở trong từng lĩnh vực.

***Từ khóa:*** Mạng cảm biến không dây, xác thực, định tuyến an toàn, bảo mật, từ chối dịch vụ.

## I. MỞ ĐẦU

Trong thập kỷ qua, thế giới đã có những tiến bộ công nghệ đáng kể trong lĩnh vực cảm biến, sự phát triển trong giao tiếp không dây và điện tử đã cho phép phát triển các nút cảm biến đa năng, chi phí thấp. Theo thống kê của Grand View Research [1], quy mô thị trường mạng cảm biến không dây công nghiệp toàn cầu được định giá là 3.282,2 triệu USD vào năm 2018 và dự kiến sẽ đạt 8.669,8 triệu USD vào năm 2025, tăng trưởng với tốc độ khoảng 15,2% từ năm 2019 đến 2025. Những dự báo này cho thấy tầm quan trọng của WSN và chúng ta có thể hình dung rằng thế giới của chúng ta sẽ bị ảnh hưởng đáng kể bởi các công nghệ liên quan đến WSN.

Chúng ta có thể dễ dàng tìm thấy sự hiện diện của các mạng cảm biến trong nhiều ứng dụng và trong nhiều lĩnh vực khác nhau, như giám sát công nghiệp, ghi dữ liệu môi trường, đo lưu lượng giao thông, tự động hóa, phát hiện cháy, y tế, các ứng dụng quân sự… Nhiều mạng cảm biến có nhiệm vụ thu thập thông tin quan trọng, việc sử dụng thông tin không đúng cách hoặc sử dụng thông tin giả mạo có thể gây rò rỉ thông tin không mong muốn và cung cấp kết quả không chính xác. Do đó, việc cung cấp bảo mật thông tin là một vấn đề lớn trong WSN. Tuy nhiên, những hạn chế tài nguyên nghiêm trọng do thiếu bộ nhớ lưu trữ dữ liệu và năng lượng giới hạn là những trở ngại chính đối với việc triển khai các kỹ thuật bảo mật máy tính truyền thống trong WSN [2]. Những hạn chế này yêu cầu chúng ta phải xem xét lại các giải pháp hiện tại về tính hiệu quả giữa bảo mật và hiệu suất, để bảo đảm các mạng cảm biến không dây an toàn mà ít tiêu tốn năng lượng của chúng. Trong bài viết này, chúng tôi khảo sát các vấn đề bảo mật khác nhau trong WSN, phân loại chúng và đưa ra những lưu ý so sánh về các phương pháp bảo mật khác nhau hiện có. Do đó, đóng góp của chúng tôi là cung cấp một cái nhìn tổng quan và những phân tích chi tiết nhưng ngắn gọn về một số kỹ thuật bảo mật mới được công bố trong những năm gần đây, điều này sẽ cho phép những người triển khai WSN tiếp cận bảo mật theo một cách có tổ chức.

Phần còn lại của bài báo được tổ chức như sau. Phần II đưa ra một cái nhìn tổng quan về các ràng buộc và yêu cầu bảo mật khác nhau. Phần III phân loại các cuộc tấn công và phương pháp phòng thủ trong WSN dựa trên các lớp theo mô hình OSI. Phần IV trình bày vắn tắt những giải pháp bảo mật mới trong thời gian gần đây. Cuối cùng, trong Phần V, chúng tôi kết luận bài viết và đưa ra một số hướng nghiên cứu trong tương lai về bảo mật WSN.

## II. NHỮNG RÀNG BUỘC VÀ YÊU CẦU BẢO MẬT

### *A. Những ràng buộc*

WSN là một mạng đặc biệt có nhiều ràng buộc hơn so với mạng máy tính truyền thống. Do những hạn chế này, khó có thể sử dụng trực tiếp các phương pháp bảo mật hiện có vào WSN. Do đó, để phát triển các cơ chế bảo mật hữu ích, trước tiên cần phải biết và hiểu rõ các ràng buộc này [3, 4].

Tác giả liên hệ: Nguyễn Văn Trường
Email: nvtruong.dhkh@gmail.com
Đến tòa soạn: 2/2020, chỉnh sửa 4/2020, chấp nhận đăng 4/2020

**Tài nguyên giới hạn:** Tất cả các phương pháp bảo mật đòi hỏi một lượng tài nguyên nhất định để thực hiện, bao gồm bộ nhớ dữ liệu, không gian mã và năng lượng để cung cấp cho cảm biến. Tuy nhiên, hiện tại các tài nguyên này rất hạn chế trong một số trường hợp thực tiễn khi nút cảm biến nhỏ và kết nối không dây.

**Truyền thông không đáng tin cậy:** Đây là một trong những mối đe dọa chính đối với bảo mật cảm biến. Bảo mật của mạng phụ thuộc rất nhiều vào một giao thức được xác định, do đó phụ thuộc vào truyền thông giao tiếp. Các tham số chính là chuyển giao không đáng tin cậy, độ trễ và xung đột.

**Hoạt động không giám sát:** Tùy thuộc vào chức năng của mạng cảm biến cụ thể, các nút cảm biến có thể hoạt động độc lập trong thời gian dài. Có ba cảnh báo chính cho các nút cảm biến không giám sát:

- Tiếp xúc với các cuộc tấn công vật lý: Cảm biến có thể được triển khai trong môi trường thù địch, thời tiết xấu… Do đó, khả năng cảm biến bị tấn công vật lý trong môi trường như vậy cao hơn nhiều so với các máy tính thông thường, được đặt ở một nơi an toàn và chủ yếu phải đối mặt với các cuộc tấn công từ mạng.

- Quản lý từ xa: Quản lý từ xa mạng cảm biến khiến hầu như không thể phát hiện sự giả mạo vật lý và các vấn đề bảo trì vật lý (ví dụ: thay pin).

- Không có điểm quản lý trung tâm: Mạng cảm biến có thể là mạng phân tán mà không có điểm quản lý trung tâm. Điều này sẽ tăng sức sống của mạng cảm biến. Tuy nhiên, nếu được thiết kế không chính xác, nó sẽ làm cho tổ chức mạng gặp khó khăn, không hiệu quả và dễ sụp đổ.

Có lẽ quan trọng nhất, cảm biến càng để lâu không được giám sát thì tấn công càng có nhiều khả năng làm tổn thương nút.

*B. Các yêu cầu bảo mật*

Mạng cảm biến là một loại mạng đặc biệt, nó mang một số điểm tương đồng với một mạng máy tính điển hình, nhưng cũng đặt ra các yêu cầu riêng của nó. Do đó, chúng ta có thể xem xét các yêu cầu của mạng cảm biến không dây bao gồm cả nhu cầu mạng thông thường và các nhu cầu cần thiết duy nhất chỉ phù hợp với mạng cảm biến không dây [4].

**Bảo mật dữ liệu:** Trong mạng cảm biến, luồng dữ liệu từ nhiều nút trung gian và dẫn đến khả năng rò rỉ dữ liệu cao hơn [5]. Bảo mật dữ liệu là vấn đề quan trọng nhất trong bảo mật mạng, mỗi mạng với bất kỳ trọng tâm bảo mật nào thường sẽ giải quyết vấn đề này đầu tiên. Bảo mật đề cập đến việc giới hạn truy cập và tiết lộ thông tin chỉ cho những người được ủy quyền; và ngăn chặn nó từ những người không được ủy quyền [6]. Người được ủy quyền và các nút được ủy quyền có thể truy cập dữ liệu, trong khi những người không được ủy quyền và các nút trái phép không thể truy cập dữ liệu. Nó đảm bảo sự riêng tư của dữ liệu và bảo vệ dữ liệu trở nên vô nghĩa đối với bất kỳ kẻ xấu nào. Bảo mật bao gồm hai phần, ủy quyền truy cập và quyền riêng tư [7, 8]. Quyền truy cập chỉ cho phép truy cập dữ liệu đối với người dùng hợp pháp, trong khi quyền riêng tư bảo vệ dữ liệu nhạy cảm khỏi tất cả những người không được ủy quyền. Cách tiếp cận tiêu chuẩn để giữ bí mật dữ liệu nhạy cảm là mã hóa dữ liệu bằng một khóa bí mật để chỉ người nhận có thể giải mã dữ liệu về dạng ban đầu.

**Xác thực:** Những kẻ tấn công không chỉ giới hạn trong việc sửa đổi gói dữ liệu, mà chúng còn có thể thay đổi toàn bộ luồng gói tin bằng cách tiêm thêm gói [4, 9]. Trong bất kỳ quy trình ra quyết định nào, các nút nhận cần phải đảm bảo rằng dữ liệu bắt nguồn từ nguồn đáng tin cậy. Do đó, xác thực là cần thiết trong quá trình trao đổi thông tin kiểm soát trong mạng, tính xác thực dữ liệu là sự đảm bảo về danh tính của các nút giao tiếp. Trong xác thực chung, có khá nhiều phương pháp được sử dụng, ví dụ: xác thực dữ liệu có thể đạt được thông qua cơ chế đối xứng hoàn toàn: người gửi và người nhận chia sẻ một khóa bí mật để tính mã xác thực bản tin của tất cả dữ liệu được truyền [7].

**Toàn vẹn dữ liệu:** Với việc thực hiện bảo mật, một kẻ tấn công có thể không đánh cắp được thông tin. Tuy nhiên, điều này không có nghĩa là dữ liệu đã an toàn, kẻ tấn công có thể thay đổi dữ liệu để đưa mạng cảm biến vào tình trạng hỗn loạn. Ví dụ, một nút độc hại có thể thêm một số đoạn hoặc điều chỉnh dữ liệu trong một gói, gói mới này sau đó có thể được gửi đến người nhận ban đầu. Do đó, tính toàn vẹn dữ liệu đảm bảo rằng tất cả các thuộc tính dữ liệu gốc được tạo trong nút cảm biến được duy trì trong suốt quá trình định tuyến đến trạm gốc trong suốt vòng đời dữ liệu [10]. Sử dụng mã toàn vẹn bản tin là một cách tiếp cận tiêu chuẩn để đảm bảo tính toàn vẹn dữ liệu.

**Độ mới dữ liệu:** Ngay cả khi tính bảo mật và tính toàn vẹn dữ liệu được đảm bảo, chúng ta cũng cần đảm bảo độ mới của mỗi bản tin. Độ mới của dữ liệu cho thấy rằng dữ liệu là mới và đảm bảo rằng không có bản tin cũ nào được phát lại [11]. Yêu cầu này đặc biệt quan trọng khi có các cơ chế chia sẻ khóa được sử dụng trong thiết kế. Thông thường các khóa chia sẻ cần phải được thay đổi theo thời gian, nhưng cần có thời gian để các khóa chia sẻ mới được truyền tới toàn bộ mạng. Trong trường hợp này, kẻ tấn công có thể khởi động một cuộc tấn công phát lại bằng khóa cũ vì khóa mới đang được làm mới và lan truyền đến tất cả các nút trong WSN. Điều này có thể được giải quyết bằng cách thêm một số bộ đếm thời gian liên quan để kiểm tra độ mới của dữ liệu.

**Khả dụng:** Tính khả dụng là cơ bản đối với WSN, vì điều này cho phép dữ liệu luôn có sẵn cho người dùng được ủy quyền, ngay cả trong trường hợp có một số cuộc tấn công như từ chối dịch vụ [11]. Bên cạnh đó, việc điều chỉnh các thuật toán mã hóa truyền thống để phù hợp với mạng cảm biến không dây cũng sẽ phát sinh một số chi phí bổ sung, các nút cảm biến có thể hết pin do tính toán hoặc giao tiếp quá mức và không khả dụng. Yêu cầu bảo mật không chỉ ảnh hưởng đến hoạt động của mạng mà còn rất quan trọng trong việc duy trì tính khả dụng của toàn mạng.

**Tự tổ chức:** Trong mạng cảm biến không dây, mọi nút cảm biến đều độc lập và đủ linh hoạt để tự tổ chức và tự phục hồi theo từng môi trường phức tạp khác nhau. Do việc triển khai ngẫu nhiên của các nút nên không có cơ sở hạ tầng cố định để quản lý WSN. Tính năng vốn có này cũng mang đến một thách thức lớn đối với bảo mật trong WSN. Các mạng cảm biến phân tán phải tự tổ chức để hỗ trợ định tuyến đa bước, chúng cũng phải tự tổ chức để tiến hành quản lý khóa và xây dựng mối quan hệ tin cậy giữa các cảm biến. Một số sơ đồ tiền phân phối khóa đã

được đề xuất trong bối cảnh của mã hóa đối xứng [12, 13].

**Đồng bộ hóa thời gian:** Hầu hết các ứng dụng mạng cảm biến dựa trên một số hình thức đồng bộ hóa thời gian và bất kỳ cơ chế bảo mật nào cho WSN cũng phải được đồng bộ hóa theo thời gian. Để tiết kiệm năng lượng, một nút cảm biến riêng lẻ có thể được tắt theo định kỳ. Một mạng cảm biến hợp tác hơn có thể yêu cầu đồng bộ hóa nhóm để theo dõi ứng dụng. Trong [14], các tác giả đề xuất một bộ giao thức đồng bộ hóa an toàn cho người gửi - người nhận (cặp đôi), đa bước người gửi - người nhận (để sử dụng khi cặp nút không nằm trong phạm vi đơn bước), và đồng bộ hóa nhóm.

**Định vị an toàn:** Thông thường, tính hữu dụng của mạng cảm biến sẽ dựa vào khả năng xác định chính xác và tự động định vị từng cảm biến trong mạng. Một mạng cảm biến được thiết kế để xác định vị trí lỗi sẽ cần thông tin vị trí chính xác để xác định vị trí lỗi. Tuy nhiên, kẻ tấn công có thể dễ dàng thao túng thông tin vị trí không được bảo mật bằng cách báo cáo sai về cường độ tín hiệu, phát lại tín hiệu…

## III. PHÂN LOẠI CÁC CUỘC TẤN CÔNG VÀ CƠ CHẾ PHÒNG THỦ

Do tính chất vô tuyến và các nút cảm biến thường nằm trong môi trường nguy hiểm hoặc thù địch khó bảo vệ, do đó các WSN rất dễ bị tổn thương trước các cuộc tấn công bảo mật. Kẻ tấn công có thể tấn công đường truyền vô tuyến, thêm các bit dữ liệu của riêng chúng vào kênh, phát lại các gói cũ hay bất kỳ kiểu tấn công nào khác. Danh sách các cuộc tấn công rất phong phú và đa dạng, và chúng ta cũng có nhiều cách để phân loại chúng như: phân loại theo chủ động và thụ động, theo bên trong và bên ngoài, theo phân lớp, theo khả năng, theo định tuyến… Tuy nhiên, trong bài báo này, chúng tôi chỉ tóm tắt và phân loại theo lớp dựa trên mô hình OSI, là mô hình rất thông dụng đối với người đọc.

Tiếp theo, chúng tôi giới thiệu một số cuộc tấn công thông dụng nhất đã và đang được các nhà khoa học nghiên cứu.

### *A. Lớp vật lý*

Lớp vật lý chịu trách nhiệm lựa chọn tần số, tạo tần số sóng mang, phát hiện tín hiệu, điều chế và mã hóa dữ liệu [15]. Như vậy với bất kỳ phương tiện nào dựa trên vô tuyến cũng tồn tại khả năng gây nhiễu trong các WSN. Ngoài ra, các nút trong WSN có thể được triển khai trong môi trường thù địch hoặc không an toàn nơi kẻ tấn công có quyền truy cập vật lý dễ dàng. Gây nhiễu, giả mạo và nghe lén là các loại tấn công vật lý chủ yếu tại lớp này.

**Gây nhiễu:** Là một loại tấn công làm nhiễu tần số vô tuyến mà các nút mạng đang sử dụng [16]. Kẻ tấn công gửi một số sóng vô tuyến ở cùng tần số với các mạng cảm biến không dây, bằng cách sử dụng các thiết bị đặc biệt để chặn tín hiệu như thiết bị gây nhiễu tần số. Do đó, các nút không thể giao tiếp trên môi trường truyền thông tràn ngập bởi các nhiễu sóng vô tuyến, điều này làm cho mạng không khả dụng. Với một thiết bị gây nhiễu các cảm biến xung quanh, kẻ tấn công có thể phá vỡ toàn bộ mạng cảm biến bằng cách triển khai đủ lớn số lượng thiết bị như vậy.

Để chống lại các cuộc tấn công gây nhiễu, một số các biện pháp sau có thể được sử dụng [16, 17, 18, 19]: Công suất truyền tải; Trải phổ nhảy tần FHSS (Frequency Hopping Spread Spectrum), Trải phổ chuỗi trực tiếp DSSS (Direct Sequence Spread Spectrum), DSSS/FHSS lai; Ăng-ten định hướng; Lướt kênh; Truyền bá mã; Phát hiện xâm nhập dựa trên độ tin cậy lớp vật lý.

**Giả mạo:** Mạng cảm biến thường hoạt động trong môi trường ngoài trời. Do tính chất không được giám sát và phân phối, các nút trong WSN rất dễ bị tấn công vật lý [20]. Cách đơn giản nhất để tấn công là phá hỏng, sửa đổi các cảm biến về mặt vật lý hay thậm chí có thể thay thế nó bằng một nút độc hại, và do đó làm dừng hoặc thay đổi dịch vụ của chúng. Tác hại sẽ lớn hơn nếu các trạm cơ sở hoặc các điểm thu thập dữ liệu bị tấn công thay vì các cảm biến thông thường. Tuy nhiên, hiệu quả của các cuộc tấn công giả mạo thiết bị này rất hạn chế do tính dư thừa cao vốn có trong hầu hết các WSN, trừ khi số lượng lớn cảm biến bị xâm phạm, còn không thì hoạt động của WSN sẽ không bị ảnh hưởng nhiều. Một cách tấn công khác, kẻ tấn công bắt nút và trích xuất thông tin nhạy cảm trên đó. Khi các cuộc tấn công trở nên phức tạp hơn (như giả mạo và từ chối dịch vụ) được thực hiện bằng cách này (dựa trên dữ liệu nhạy cảm), thì mối đe dọa có thể nghiêm trọng hơn nhiều.

Để chống lại các cuộc tấn công giả mạo, một số các biện pháp sau có thể được sử dụng [21, 22, 23, 24, 25, 26]: Tối ưu hóa và sử dụng bộ xử lý tiền điện tử hoặc bộ xử lý an toàn vật lý; Áp dụng các biện pháp phòng ngừa tiêu chuẩn trong mạng; Thay đổi phần cứng / phần mềm; Ngụy trang / ẩn cảm biến; Phát triển và sử dụng các giao thức thích hợp; Hạn chế tiếp cận; Bảo mật dữ liệu.

**Nghe trộm:** Kẻ tấn công sẽ lắng nghe mạng, theo dõi lưu lượng truyền trên các kênh liên lạc và thu thập dữ liệu, nếu những dữ liệu này được gửi mà không được mã hóa thì có thể bị phân tích và trích xuất thông tin nhạy cảm [27]. WSN đặc biệt dễ bị tổn thương trước các cuộc tấn công như vậy vì truyền dẫn không dây là phương thức liên lạc chủ yếu được sử dụng bởi các cảm biến. Trong quá trình truyền, tín hiệu không dây được truyền trong không khí và do đó có thể truy cập công khai. Vì cuộc tấn công này không sửa đổi dữ liệu, cho nên rất khó để phát hiện ra nó.

Để chống lại các cuộc tấn công này, một số các biện pháp sau có thể được sử dụng [6, 18, 22, 27]: Kiểm soát truy cập; Định tuyến an toàn; Hạn chế tiếp cận; Mã hóa.

### *B. Lớp liên kết*

Lớp liên kết dữ liệu chịu trách nhiệm ghép kênh các luồng dữ liệu, phát hiện khung dữ liệu, truy cập phương tiện và kiểm soát lỗi [15]. Nó đảm bảo các kết nối điểm - điểm và điểm - đa điểm đáng tin cậy trong một mạng truyền thông, và việc gán kênh cho giao tiếp nút lân cận với nút lân cận cũng là nhiệm vụ chính của lớp này. Va chạm, cạn kiệt tài nguyên và không công bằng là những cuộc tấn công chính trong lớp này.

**Va chạm**: Xung đột xảy ra khi hai nút cố gắng truyền trên cùng một tần số. Khi các gói va chạm, một sự thay đổi có thể sẽ xảy ra trong phần dữ liệu, gây ra sự không khớp đối với việc kiểm tra ở đầu nhận. Các gói sau đó sẽ bị loại bỏ như một trường hợp không hợp lệ [28, 29]. Kẻ tấn công có thể gây ra xung đột trong các gói. Các gói bị

ảnh hưởng được truyền lại, làm tăng năng lượng và chi phí thời gian cho việc truyền. Một cuộc tấn công như vậy làm giảm sự hoàn hảo của mạng [9].

Một biện pháp bảo mật điển hình chống va chạm là sử dụng mã sửa lỗi [30]. Hầu hết các mã hoạt động tốt nhất với mức độ va chạm thấp, chẳng hạn như các mã gây ra bởi lỗi môi trường hoặc xác suất. Tuy nhiên, các mã này cũng làm phát sinh thêm chi phí xử lý và liên lạc. Bên cạnh đó, một số biện pháp khác để chống lại các cuộc tấn công va chạm có thể kể đến như [26, 31, 32, 33, 34, 35]: Các phương pháp chống nhiễu; Thuật toán điều khiển truy nhập môi trường CA-MAC (Collision Avoidance - Medium Access Control); Đa dạng thời gian; Giới hạn tỷ lệ yêu cầu MAC; Sử dụng các khung nhỏ; Mã hóa lớp liên kết; Bảo vệ danh tính.

**Cạn kiệt tài nguyên:** Kẻ tấn công có thể tạo ra cuộc tấn công DoS bằng cách tạo ra các nỗ lực truyền lại nhiều lần. Ngay cả khi không có lưu lượng cao, nếu một nút phải liên tục truyền lại do va chạm thì cuối cùng năng lượng của nó có thể bị cạn kiệt [17].

Một giải pháp điển hình đó là áp dụng các giới hạn tốc độ gửi MAC để mạng có thể bỏ qua các yêu cầu quá mức, do đó ngăn chặn sự tiêu hao năng lượng do truyền đi lặp lại [36]. Và một số biện pháp khác để chống lại các cuộc tấn công này là [35, 36, 37]: Sử dụng ghép kênh phân chia thời gian trong đó mỗi nút được phân bổ một khe thời gian mà nó có thể truyền; Back-off ngẫu nhiên; Hạn chế các đáp ứng không liên quan.

**Không công bằng:** Không công bằng có thể được coi là một phần của một cuộc tấn công từ chối dịch vụ DoS (Denial of Service) [36]. Kẻ tấn công có thể gây ra sự không công bằng trong mạng bằng cách lặp đi lặp lại các cuộc tấn công lớp MAC dựa trên sự cạn kiệt hoặc va chạm hoặc sử dụng lạm dụng các cơ chế ưu tiên lớp MAC. Thay vì ngăn chặn quyền truy cập vào một dịch vụ hoàn toàn, kẻ tấn công có thể làm suy giảm nó để đạt được lợi thế như khiến các nút khác trong giao thức MAC thời gian thực bỏ lỡ thời hạn truyền.

Giải pháp khả thi để chống lại các cuộc tấn công này là sử dụng các khung nhỏ làm giảm tác dụng của các cuộc tấn công, như vậy làm giảm lượng thời gian kẻ tấn công có thể chiếm được kênh liên lạc [38, 39].

### *C. Lớp mạng và định tuyến*

Các nút cảm biến thường nằm rải rác trong một vùng khép kín hoặc bên trong các môi trường đặc biệt. Do đó, các giao thức định tuyến không dây đa bước đặc biệt giữa các nút cảm biến và nút thu nhận là cần thiết để cung cấp dữ liệu trên toàn mạng. Lớp mạng và định tuyến của WSN thường được thiết kế theo các nguyên tắc sau [15, 40]: Hiệu quả năng lượng; Trung tâm dữ liệu; Nhận biết địa chỉ và vị trí. Các cuộc tấn công phổ biến của lớp mạng này bao gồm: Thông tin định tuyến giả mạo, thay đổi hoặc phát lại; Chuyển tiếp chọn lọc; Tấn công Sinkhole; Tấn công Sybil; Wormhole; Tấn công làm tràn HELLO; và Giả mạo xác thực.

**Thông tin định tuyến giả mạo, thay đổi hoặc phát lại:** Đây là cuộc tấn công trực tiếp phổ biến nhất đối với giao thức định tuyến. Cuộc tấn công này nhắm vào thông tin định tuyến trao đổi giữa các nút. Kẻ tấn công có thể giả mạo, thay đổi hoặc phát lại thông tin định tuyến để phá vỡ lưu lượng trong mạng [26, 41]. Những gián đoạn này bao gồm việc tạo các vòng định tuyến, thu hút hoặc từ chối lưu lượng mạng từ các nút được chọn, mở rộng và rút ngắn các định tuyến nguồn, tạo thông báo lỗi giả mạo, phân vùng mạng và tăng độ trễ từ đầu đến cuối.

Một biện pháp chống lại các cuộc tấn công giả mạo và thay đổi là thêm MAC phía sau bản tin gửi đi. Bằng cách thêm MAC vào bản tin, người nhận có thể xác minh xem các bản tin đã bị giả mạo hay thay đổi. Để bảo vệ chống lại thông tin được phát lại, kỹ thuật dấu thời gian hoặc bộ đếm có thể được bao gồm trong các bản tin [7]. Ngoài ra, một số biện pháp đối phó khác có thể được xem xét đến như [26, 27, 42]: Xác thực theo cặp; Xác thực lớp mạng; Xác thực, mã hóa lớp liên kết và các kỹ thuật chia sẻ khóa; Cơ chế định tuyến đáng tin cậy dựa trên Blockchain và học tăng cường.

**Chuyển tiếp chọn lọc:** Một giả định quan trọng được thực hiện trong các mạng đa bước là tất cả các nút trong mạng sẽ chuyển tiếp chính xác các bản tin nhận được. Kẻ tấn công có thể tạo các nút độc hại chỉ chuyển tiếp có chọn lọc một số bản tin nhất định và bỏ qua các bản tin khác. Một hình thức cụ thể của cuộc tấn công này là cuộc tấn công Blackhole trong đó một nút làm rơi tất cả các bản tin mà nó nhận được.

Một biện pháp chống lại các cuộc tấn công chuyển tiếp có chọn lọc là sử dụng nhiều đường dẫn để gửi dữ liệu [43]. Cách phòng thủ thứ hai là phát hiện nút độc hại hoặc cho rằng nó đã thất bại và tìm kiếm một tuyến đường thay thế. Ngoài ra, một số biện pháp đối phó khác có thể kể đến như [27, 42, 44]: Bổ sung số thứ tự gói dữ liệu trong tiêu đề gói; Giám sát mạng thường xuyên; Tự động chọn bước nhảy tiếp theo của gói từ một nhóm ứng viên; Bảo vệ toàn vẹn dữ liệu.

**Sinkhole:** Trong một cuộc tấn công Sinkhole, kẻ tấn công cố gắng thu hút lưu lượng truy cập từ một khu vực cụ thể thông qua nút bị xâm nhập bằng cách giả mạo thông tin định tuyến [43]. Kết quả cuối cùng là các nút xung quanh sẽ chọn nút bị xâm phạm làm nút tiếp theo để định tuyến dữ liệu của chúng. Kiểu tấn công này làm cho việc chuyển tiếp chọn lọc trở nên rất đơn giản, vì tất cả lưu lượng truy cập từ một khu vực lớn trong mạng sẽ chảy qua nút độc hại [45]. Kẻ tấn công thường nhằm vào nơi nó có thể thu hút nhiều lưu lượng truy cập nhất để tạo ra Sinkhole, có thể gần trạm cơ sở hơn để nút độc hại có thể được coi là trạm cơ sở.

Để chống lại các cuộc tấn công này, một số các biện pháp sau có thể được sử dụng [27, 39, 46]: Định tuyến an toàn; Giao thức định tuyến địa lý GPSR (Geographic Routing Protocol); Xác xuất lựa chọn bước nhảy tiếp theo; Xác thực thông tin được quảng bá bởi các nút lân cận; Quản lý khóa; Hạn chế truy cập định tuyến.

**Sybil:** Tấn công Sybil được định nghĩa là một thiết bị độc hại chiếm giữ trái phép nhiều danh tính [32, 43]. Ban đầu nó được mô tả là một cuộc tấn công có thể đánh bại các cơ chế dự phòng của các hệ thống lưu trữ dữ liệu phân tán trong các mạng ngang hàng [47]. Ngoài ra, cuộc tấn công Sybil cũng có hiệu quả đối với các thuật toán định tuyến, tổng hợp dữ liệu, phân bổ tài nguyên hợp lý và ngăn chặn phát hiện sai. Trong WSN, tấn công Sybil thường được sử dụng để tấn công một số loại giao thức [48]. Đây là một mối đe dọa nghiêm trọng đối với các giao thức dựa trên vị trí, trong đó thông tin vị trí được trao đổi để định tuyến hiệu quả.

Để chống lại cuộc tấn công Sybil, chúng ta cần một cơ chế để đảm bảo rằng một danh tính cụ thể là danh tính duy nhất được giữ bởi một nút vật lý nhất định. Các tác giả trong [32] trình bày hai phương pháp để đảm bảo danh tính, xác thực trực tiếp và xác thực gián tiếp. Trong xác thực trực tiếp, một nút đáng tin cậy trực tiếp kiểm tra xem danh tính tham gia có hợp lệ không. Trong xác thực gián tiếp, một nút đáng tin cậy khác được phép chứng minh (hoặc chống lại) tính hợp lệ của nút tham gia. Một số kỹ thuật khác để bảo vệ chống lại cuộc tấn công Sybil là [4, 27, 32, 46]: Sử dụng các kỹ thuật tiền phân phối khóa ngẫu nhiên; Phát hành chứng chỉ và sử dụng chứng chỉ nhận dạng; Giới hạn số lượng nút lân cận.

**Wormhole:** Wormhole là một liên kết có độ trễ thấp giữa hai phần của mạng nơi mà kẻ tấn công phát lại các bản tin mạng [43]. Trong cuộc tấn công này tồn tại hai hoặc nhiều nút độc hại có trong mạng tại các địa điểm khác nhau. Khi nút gửi truyền thông tin thì một nút độc hại sẽ chuyển thông tin đến một nút độc hại khác. Nút nhận độc hại sau đó gửi thông tin đến các nút lân cận. Bằng cách này, kẻ tấn công thuyết phục các nút gửi và nhận rằng chúng nằm ở khoảng cách một hoặc hai bước nhưng khoảng cách thực tế giữa hai bước này là nhiều bước nhảy và thường cả hai đều nằm ngoài phạm vi. Chủ yếu tấn công Wormhole và chuyển tiếp chọn lọc được sử dụng kết hợp với nhau. Nếu chúng kết hợp thêm với tấn công Sybil thì việc phát hiện tấn công là vô cùng khó khăn [49].

Một biện pháp phòng chống điển hình đó là sử dụng giao thức dây xích gói để phát hiện và bảo vệ chống lại các cuộc tấn công của Wormholes [34, 50]. Dây xích là bất kỳ thông tin nào được thêm vào gói đã thiết kế để hạn chế khoảng cách truyền tối đa cho phép của gói. Hai loại dây xích đã được giới thiệu: dây xích địa lý và dây xích tạm thời. Ngoài ra, một số biện pháp đối phó khác có thể kể đến như [24, 33, 39]: Giao thức định tuyến trạng thái liên kết tối ưu OLSR (Optimized Link-State Routing); Thuật toán chia tỷ lệ đa chiều; Sử dụng thông tin vùng lân cận cục bộ; Thiết kế các giao thức định tuyến thích hợp cục bộ dựa trên cụm; Xác minh thông tin các nút lân cận công bố; Đồng bộ thời gian; Sử dụng Anten định hướng.

**Làm tràn bản tin HELLO**: Nhiều giao thức định tuyến trong WSN yêu cầu các nút phát bản tin HELLO để thông báo cho nút lân cận của chúng. Một nút nhận được bản tin như vậy có thể cho rằng nó nằm trong phạm vi phát sóng của nút gửi. Trong một cuộc tấn công làm tràn HELLO, bản tin HELLO được phát ra với công suất cao bởi kẻ tấn công. Các nút nhận bản tin HELLO này sẽ gửi các gói dữ liệu đến nút kẻ tấn công [51]. Kẻ tấn công có thể thay đổi hoặc sửa đổi gói dữ liệu hoặc có thể bỏ gói. Theo cách này, rất nhiều năng lượng bị lãng phí và cũng xảy ra tắc nghẽn mạng.

Cuộc tấn công này có thể được bảo vệ bằng các biện pháp điển hình như [39, 43, 51, 52]: Xác minh tính định hướng của các liên kết cục bộ trước khi sử dụng chúng; Sử dụng các giao thức phát sóng được xác thực; Phát hiện nút đáng ngờ bằng cường độ tín hiệu; Hạn chế số lượng nút lân cận; Kỹ thuật chuyển tiếp dữ liệu nhiều trạm gốc đa đường; Mã hóa.

**Giả mạo xác thực:** Các thuật toán định tuyến được sử dụng trong các mạng cảm biến đôi khi yêu cầu phải sử dụng xác thực. Một nút tấn công có thể bắt gói tin được gửi từ các nút lân cận của nó và giả mạo các xác nhận, từ đó cung cấp dữ liệu sai cho các nút [43]. Ví dụ như kẻ tấn công tuyên bố rằng một nút còn sống trong khi thực tế nó đã chết. Các giao thức chọn bước nhảy tiếp theo dựa trên các vấn đề về độ tin cậy rất dễ bị giả mạo.

Các biện pháp phòng thủ chống lại các cuộc tấn công giả mạo xác thực gồm [42, 43, 53]: Mã hóa; Xác nhận bản tin phù hợp; Sử dụng đường dẫn khác nhau để truyền lại bản tin.

### *D. Lớp vận chuyển*

Lớp vận chuyển chịu trách nhiệm quản lý các kết nối đầu cuối. Hai cuộc tấn công điển hình có thể xảy ra trong lớp này là tấn công làm tràn và mất đồng bộ [17].

**Tấn công làm tràn:** Các cuộc tấn công làm tràn gây cạn kiệt bộ nhớ tài nguyên của các nút cảm biến, bằng cách liên tục thực hiện các yêu cầu kết nối mới cho đến khi tài nguyên được yêu cầu bởi mỗi kết nối đã cạn kiệt hoặc đạt đến giới hạn tối đa [17]. Nó tạo ra các ràng buộc tài nguyên nghiêm trọng cho các nút hợp pháp.

Một số giải pháp được đề xuất cho vấn đề này là [17, 42, 54, 57]: Thuật toán câu đố của khách hàng; Giới hạn số lượng kết nối của nút; Hạn chế truy cập định tuyến; Quản lý khóa; Định tuyến an toàn.

**Mất đồng bộ:** Mất đồng bộ đề cập đến sự gián đoạn của một kết nối hiện có giữa hai cảm biến đầu cuối [26]. Kẻ tấn công có thể liên tục giả mạo bản tin đến máy chủ cuối, khiến máy chủ đó yêu cầu truyền lại các khung bị bỏ lỡ. Các cuộc tấn công này có thể làm giảm hoặc thậm chí ngăn khả năng của máy chủ cuối trao đổi thành công dữ liệu, do đó khiến chúng lãng phí năng lượng bằng cách cố gắng khôi phục từ các lỗi chưa từng tồn tại.

*Bảng 1. Phân loại các cuộc tấn công và cơ chế phòng thủ*

| Lớp | Cuộc tấn công | Yêu cầu bảo mật | Giải pháp, cơ chế phòng thủ | Tài liệu |
|---|---|---|---|---|
| Lớp vật lý | Gây nhiễu | -Tính khả dụng<br>-Tính toàn vẹn | Công suất truyền tải; Trải phổ nhảy tần FHSS, Trải phổ chuỗi trực tiếp DSSS, DSSS/FHSS lai; Ăng-ten định hướng; Lướt kênh; Truyền bá mã; Phát hiện xâm nhập dựa trên độ tin cậy lớp vật lý. | 16, 17, 18, 19, 40, 59, 60 |
| | Giả mạo | -Xác thực<br>-Bảo mật<br>-Tính khả dụng | Tối ưu hóa và sử dụng bộ xử lý tiền điện tử hoặc bộ xử lý an toàn vật lý; Áp dụng các biện pháp phòng ngừa tiêu chuẩn trong mạng; Thay đổi phần cứng / phần mềm; Ngụy trang / ẩn cảm biến; Phát triển và sử dụng các giao thức thích hợp; Hạn chế tiếp cận; Bảo mật dữ liệu. | 21, 22, 23, 24, 25, 26 |
| | Nghe trộm | -Bảo mật | Kiểm soát truy cập; Định tuyến an toàn; Hạn chế tiếp cận; Mã hóa. | 6, 18, 22, 27 |
| Lớp liên kết | Va chạm | -Tính khả dụng | Các phương pháp chống nhiễu; Thuật toán điều khiển truy nhập môi trường CA-MAC; Đa dạng thời gian; Giới hạn tỷ lệ yêu cầu MAC; Sử dụng các khung nhỏ; Mã hóa lớp liên kết; Bảo vệ danh tính. | 26, 30, 31, 32, 33, 34, 35 |
| | Cạn kiệt tài nguyên | -Tính khả dụng | Giới hạn tốc độ gửi MAC; Sử dụng ghép kênh phân chia thời gian trong đó mỗi nút được phân bổ một khe thời gian mà nó có thể truyền; Back-off ngẫu nhiên; Hạn chế các đáp ứng không liên quan. | 35, 36, 37, 41 |
| | Không công bằng | -Tính khả dụng | Sử dụng các khung nhỏ làm giảm lượng thời gian kẻ tấn công có thể chiếm được kênh liên lạc. | 38, 39 |
| Lớp mạng và định tuyến | Thông tin định tuyến giả mạo, thay đổi hoặc phát lại | -Tính toàn vẹn<br>-Tính khả dụng | Dấu thời gian hoặc bộ đếm trong bản tin; Xác thực theo cặp; Xác thực lớp mạng; Xác thực, mã hóa lớp liên kết và các kỹ thuật khóa được chia sẻ; Cơ chế định tuyến đáng tin cậy dựa trên Blockchain và học tăng cường. | 7, 26, 27, 42, 62 |
| | Chuyển tiếp chọn lọc | -Bảo mật<br>-Tính khả dụng | Sử dụng nhiều đường dẫn để gửi dữ liệu; Bổ sung số thứ tự gói dữ liệu trong tiêu đề gói; Giám sát mạng thường xuyên; Tự động chọn bước nhảy tiếp theo của gói từ một nhóm ứng viên; Bảo vệ toàn vẹn dữ liệu. | 27, 42, 43, 44 |
| | Sinkhole | -Bảo mật<br>-Tính toàn vẹn<br>-Tính khả dụng | Định tuyến an toàn; Giao thức định tuyến địa lý GPSR; Xác xuất lựa chọn bước nhảy tiếp theo; Xác thực thông tin được quảng bá bởi các nút lân cận; Quản lý khóa; Hạn chế truy cập định tuyến. | 27, 39, 46 |
| | Sybil | -Xác thực<br>-Tính khả dụng | Đảm bảo danh tính duy nhất được giữ bởi một nút vật lý nhất định; Sử dụng các kỹ thuật tiền phân phối khóa ngẫu nhiên; Phát hành chứng chỉ và sử dụng chứng chỉ nhận dạng; Giới hạn số lượng nút lân cận. | 4, 27, 32, 46 |
| | Wormholes | -Bảo mật<br>-Xác thực | Giao thức dây xích gói; Giao thức định tuyến trạng thái liên kết tối ưu OLSR; Thuật toán chia tỷ lệ đa chiều; Sử dụng thông tin vùng lân cận cục bộ; Thiết kế các giao thức định tuyến thích hợp cục bộ dựa trên cụm; Xác minh thông tin các nút lân cận công bố; Đồng bộ thời gian; Sử dụng Anten định hướng. | 24, 33, 34, 39, 50 |
| | Làm tràn bản tin HELLO | -Tính khả dụng | Xác minh tính định hướng của các liên kết cục bộ trước khi sử dụng chúng; Sử dụng các giao thức phát sóng được xác thực; Phát hiện nút đáng ngờ bằng cường độ tín hiệu; Hạn chế số lượng nút lân cận; Kỹ thuật chuyển tiếp dữ liệu nhiều trạm gốc đa đường; Mã hóa. | 39, 43, 51, 52 |
| | Giả mạo xác nhận | -Xác thực<br>-Tính khả dụng | Mã hóa; Xác nhận bản tin phù hợp; Sử dụng đường dẫn khác nhau để truyền lại bản tin. | 42, 43, 53 |
| Lớp vận chuyển | Tấn công làm tràn | -Tính khả dụng | Thuật toán câu đố của khách hàng; Giới hạn số lượng kết nối của nút; Hạn chế truy cập định tuyến; Quản lý khóa; Định tuyến an toàn. | 17, 42, 54, 57 |
| | Mất đồng bộ | -Xác thực<br>-Tính khả dụng | Xác thực gói; Hợp tác đồng bộ hóa thời gian; Duy trì thời gian thích hợp. | 26, 42, 55, 57 |
| Lớp ứng dụng | Tấn công tập hợp dữ liệu | -Tính toàn vẹn<br>-Bảo mật<br>-Tính khả dụng | Bảo vệ tính toàn vẹn dữ liệu; Bảo vệ bí mật dữ liệu; Kiểm soát truy cập. | 27, 56, 57 |
| | Chuyển tiếp bản tin chọn lọc | -Tính toàn vẹn<br>-Bí mật | Giám sát mạng thường xuyên; Sử dụng định tuyến khác; Hạn chế truy cập định tuyến; Quản lý khóa; Bảo vệ tính toàn vẹn dữ liệu; Bảo vệ bí mật dữ liệu; Cơ chế chia sẻ khóa bí mật đa thức nhẹ. | 27, 56, 57, 64 |
| | Đồng bộ thời gian | -Bảo mật<br>-Xác thực<br>-Tính toàn vẹn | Cơ chế xác thực mạnh mẽ; Phát hiện các nút độc hại; Bảo vệ tính toàn vẹn dữ liệu; Bảo vệ bí mật dữ liệu. | 27, 56, 57 |
| Nhiều lớp | Tấn công từ chối dịch vụ DoS | -Xác thực<br>-Bảo mật<br>-Tính toàn vẹn<br>-Tính khả dụng | Các cơ chế phòng thủ đã trình bày đối với các lớp vật lý, lớp liên kết, lớp mạng và định tuyến, lớp vận chuyển và lớp ứng dụng. | |

Một số giải pháp phòng thủ được đề xuất cho các cuộc tấn công này là [26, 42, 55, 57]: Xác thực gói; Hợp tác đồng bộ hóa thời gian; Duy trì thời gian thích hợp.

### *E. Lớp ứng dụng*

Lớp ứng dụng cũng rất dễ bị ảnh hưởng về bảo mật so với các lớp khác. Lớp ứng dụng hỗ trợ các giao thức khác nhau như FTP, TELNET, HTTP và SMTP bao gồm dữ liệu người dùng cung cấp nhiều điểm truy cập và tồn tại nhiều lỗ hổng cho kẻ tấn công. Các cuộc tấn công điển hình đối với lớp ứng dụng trên các mạng cảm biến gồm [56]: Tấn công tập hợp dữ liệu, chuyển tiếp bản tin chọn lọc, mã độc, tấn công thoái thác, tấn công đồng bộ thời gian, tấn công tiêm dữ liệu sai.

**Tấn công tập hợp dữ liệu:** Sau khi dữ liệu được thu thập, các cảm biến thường gửi chúng trở lại các trạm gốc để xử lý. Kẻ tấn công có thể sửa đổi dữ liệu được tập hợp và làm cho dữ liệu cuối cùng được tính toán bởi các trạm cơ sở bị biến dạng. Điều này sẽ làm trạm cơ sở có những phân tích sai về môi trường mà cảm biến đang theo dõi và có thể dẫn đến những quyết định không phù hợp. Khi kết hợp tấn công tập hợp dữ liệu với tấn công Blackhole và Sinkhole, dữ liệu sẽ không thể đến được nút thu nhận.

Một số giải pháp phòng thủ được đề xuất cho các cuộc tấn công này là [27, 56, 57]: Bảo vệ tính toàn vẹn dữ liệu; Bảo vệ bí mật dữ liệu; Kiểm soát truy cập.

**Chuyển tiếp bản tin chọn lọc:** Đối với cuộc tấn công này, kẻ tấn công phải ở trên tuyến đường giữa nguồn và đích và do đó chịu trách nhiệm chuyển tiếp gói cho nguồn [27]. Cuộc tấn công có thể hoạt động bằng cách chuyển tiếp một số hoặc một phần bản tin có chọn lọc. Lưu ý rằng cuộc tấn công này khác với cuộc tấn công chuyển tiếp chọn lọc khác trong lớp mạng đã trình bày ở phần trên. Để khởi động tấn công chuyển tiếp chọn lọc trong lớp ứng dụng, kẻ tấn công cần hiểu bản chất của tải trọng các gói lớp ứng dụng (nghĩa là coi mỗi gói là một bản tin có ý nghĩa thay vì một đơn vị nguyên khối) và chọn các gói được chuyển tiếp. Còn đối với cuộc tấn công chuyển tiếp chọn lọc trong lớp mạng chỉ yêu cầu kẻ tấn công biết thông tin của lớp mạng, chẳng hạn như địa chỉ nguồn và đích. Và những kẻ tấn công quyết định có nên chuyển tiếp các gói theo các loại thông tin đó hay không, do đó nó hoạt động ở mức độ khác.

Một số giải pháp phòng thủ được đề xuất cho các cuộc tấn công này là [27, 56, 57]: Giám sát mạng thường xuyên; Sử dụng định tuyến khác; Hạn chế truy cập định tuyến; Quản lý khóa; Bảo vệ tính toàn vẹn dữ liệu; Bảo vệ bí mật dữ liệu; Cơ chế chia sẻ khóa bí mật đa thức nhẹ.

**Đồng bộ thời gian:** Mục tiêu của cuộc tấn công này là sự cần thiết hoạt động một cách đồng bộ của các cảm biến. Bằng cách phổ biến thông tin thời gian sai, các cuộc tấn công sẽ làm lệch thời gian của các nút cảm biến gây nên sự mất đồng bộ trong WSN [27].

Để chống lại các cuộc tấn công này, một số giải pháp điển hình sau có thể được áp dụng [27, 56, 57]: Cơ chế xác thực mạnh mẽ; Phát hiện các nút độc hại; Bảo vệ tính toàn vẹn dữ liệu; Bảo vệ bí mật dữ liệu.

### *F. Tấn công từ chối dịch vụ (DoS)*

Từ chối dịch vụ (DoS) được tạo ra do lỗi vô ý của các nút hoặc do các hành động độc hại. Cuộc tấn công này là một mối đe dọa phổ biến và có thể được khởi chạy từ nhiều lớp của mạng cảm biến [4, 26, 58]. Các mạng cảm biến nhạy cảm về năng lượng và hạn chế tài nguyên rất dễ bị tấn công DoS. Cuộc tấn công DoS đơn giản nhất cố gắng làm cạn kiệt tài nguyên có sẵn đối với nút nạn nhân, bằng cách gửi thêm các gói không cần thiết và do đó ngăn người dùng mạng hợp pháp truy cập các dịch vụ hoặc tài nguyên mà họ được hưởng. Cuộc tấn công DoS không chỉ có ý nghĩa đối với nỗ lực của kẻ tấn công để tìm cách phá hoại, phá vỡ hoặc phá hủy mạng mà còn cho bất kỳ sự kiện nào làm giảm khả năng của mạng để cung cấp dịch vụ. Trong WSN, một số loại tấn công DoS trong các lớp khác nhau có thể được thực hiện. Ở lớp vật lý, các cuộc tấn công DoS có thể kể đến như gây nhiễu và giả mạo. Ở lớp liên kết, các cuộc tấn công DoS điển hình là va chạm, cạn kiệt, không công bằng. Trong khi ở lớp mạng và định tuyến, các cuộc tấn công định tuyến sai, Homing và Blackhole thường được nhắc đến. Lớp vận chuyển cũng dễ bị tấn công, như trong trường hợp tấn công làm tràn. Tấn công làm tràn có thể đơn giản như gửi nhiều yêu cầu kết nối đến một nút nhạy cảm. Trong trường hợp này, tài nguyên phải được phân bổ để xử lý yêu cầu kết nối. Cuối cùng, tài nguyên của nút sẽ bị cạn kiệt, do đó khiến cho nút trở nên vô dụng. Cuối cùng, một cuộc tấn công DoS có thể được thực hiện đối với giao thức cấp ứng dụng cụ thể, ví dụ điển hình là sự gián đoạn của giao thức tập hợp dữ liệu.

Để chống lại các cuộc tấn công DoS, chúng ta có thể sử dụng các cơ chế phòng thủ như đã trình bày đối với các lớp vật lý, lớp liên kết, lớp mạng và định tuyến, lớp vận chuyển và lớp ứng dụng [4, 26, 58].

Tóm tắt về phân loại các cuộc tấn công và cơ chế phòng thủ như bảng 1.

## IV. CÁC GIẢI PHÁP BẢO MẬT ĐỐI VỚI WSN TRONG THỜI GIAN GẦN ĐÂY

Các tác giả trong [59] đã đề xuất một cách tiếp cận để phát hiện các hình thức tấn công gây nhiễu khác nhau, trong đó thuật toán phát hiện gây nhiễu được triển khai trên cụm trưởng để phát hiện các cuộc tấn công trong các nút thành viên và cả trên các trạm cơ sở để phát hiện các cuộc tấn công trong các cụm trưởng bằng cách sử dụng gói số liệu IAT. Số liệu này được sử dụng để phát hiện sự thay đổi đột ngột trong chuỗi gói gây ra bởi tình huống gây nhiễu do các cuộc tấn công bằng thuật toán EMWA (Exponentially Weighted Moving Average). Để đánh giá tính hiệu quả, tác giả đã sử dụng bộ dữ liệu có sẵn công khai CRAWDAD bao gồm ba cuộc tấn công gây nhiễu khác nhau, đó là gây nhiễu liên tục, gây nhiễu định kỳ và gây nhiễu phản ứng; cùng với một dấu vết không gây nhiễu. Kết quả thu được cho thấy phương pháp được đề xuất có thể phát hiện hiệu quả sự hiện diện của một cuộc tấn công gây nhiễu với rất ít hoặc không tốn kém chi phí trong WSN.

Các tác giả trong [60] đã đề xuất một hệ thống phát hiện xâm nhập PL-IDS (Physical Layer trust based Intrusion Detection System) để tính toán độ tin cậy cho các WSN ở lớp vật lý. Giá trị tin cậy của nút cảm biến được tính theo độ lệch của các yếu tố chính ở lớp vật lý. Cơ chế đề xuất có hiệu quả để xác định các nút bất thường trong WSN. Các nút bất thường chủ yếu tấn công lớp vật lý bằng cách tấn công từ chối dịch vụ. Chúng sử dụng cuộc tấn công gây nhiễu bằng cách tiêu thụ tài nguyên của các nút đích thực, dẫn đến việc từ chối dịch vụ. Để phân tích hiệu suất của PL-IDS, tác giả đã thực hiện cuộc tấn công gây nhiễu định kỳ trong mạng. Kết quả cho thấy PL-IDS hoạt động tốt hơn về tỷ lệ cảnh báo sai và tỷ lệ chính xác trong việc phát hiện nút độc hại.

Các tác giả trong [61] đã đề xuất một cơ chế tìm kiếm và chia sẻ dữ kiệu DSS (Dating Sharing and Searching) an toàn và hiệu quả có thể đồng thời chống lại cả hai loại tấn công đoán từ khóa là KGA trực tuyến và KGA ngoại tuyến được thực hiện bởi kẻ tấn công bên trong và bên ngoài mạng. Cơ chế này đã khắc phục được tồn tại của mã hóa khóa công khai PEKS (Public Key Encryption with Keyword Search), là kỹ thuật cho phép người nhận dữ liệu truy xuất dữ liệu được mã hóa có chứa một số từ khóa cụ thể trong WSN được hỗ trợ trên đám mây. Cơ chế này không chỉ thực hiện chức năng tìm kiếm từ khóa trong đám mây mà còn thực hiện chức năng mã hóa / giải mã tập dữ liệu. Phân tích hiệu suất cho thấy chi phí tính toán tại các thiết bị di động nhẹ được giảm đáng kể. Các kết quả mô phỏng đã chứng minh rằng cơ chế được đề xuất đạt được bảo mật từ khóa và bảo mật tài liệu.

Các tác giả trong [62] đã đề xuất một cơ chế định tuyến đáng tin cậy dựa trên Blockchain và học tăng cường

RLBC (Reinforcement Learning and Blockchain) để cung cấp một môi trường định tuyến đáng tin cậy và cải thiện hiệu suất của mạng định tuyến. Là một hệ thống phi tập trung, mạng Blockchain cung cấp một cơ chế khả thi để quản lý thông tin định tuyến và một nền tảng đối với học tăng cường về lập lịch định tuyến. Tác giả sử dụng mã thông báo Blockchain để thể hiện các gói định tuyến, và mỗi giao dịch định tuyến được phát hành cho mạng Blockchain thông qua xác nhận của các nút hợp lệ, điều này làm cho thông tin định tuyến có thể theo dõi và không thể giả mạo. Mô hình học tăng cường được sử dụng để giúp các nút định tuyến tự động chọn các liên kết định tuyến hiệu quả và đáng tin cậy hơn. Các kết quả thử nghiệm cho thấy hệ thống có thể ngăn chặn hiệu quả các cuộc tấn công của các nút độc hại, ngay cả trong môi trường định tuyến có 50% nút độc hại, cơ chế định tuyến đề xuất vẫn có hiệu suất trễ tốt so với các thuật toán định tuyến khác. Các chỉ số hiệu suất khác như tiêu thụ năng lượng và thông lượng cũng cho thấy cơ chế này là khả thi và hiệu quả.

Các tác giả trong [63] đã đề xuất một thuật toán định tuyến an toàn mới là nhận biết độ tin cậy năng lượng dựa trên thuật toán định tuyến an toàn EATSRA (Energy Aware Trust based Secure Routing Algorithm) để cung cấp định tuyến an toàn và tối ưu trong WSN. Trong mô hình này, đánh giá điểm tin cậy được sử dụng để phát hiện người dùng độc hại một cách hiệu quả hơn trong WSN và cây quyết định dựa trên thuật toán định tuyến được sử dụng để chọn đường dẫn bảo mật tốt nhất. Hơn nữa, các ràng buộc không gian - thời gian đã được sử dụng để đưa ra quyết định định tuyến hiệu quả hơn. Kết quả mô phỏng đã chứng minh rằng thuật toán định tuyến dựa trên độ tin cậy được đề xuất đạt được sự cải thiện hiệu suất đáng kể so với các sơ đồ hiện có (như LEACH, HEED và STRM) về bảo mật, hiệu quả năng lượng và tỷ lệ phân phối gói.

Các tác giả trong [64] đã đề xuất một cơ chế chia sẻ khóa bí mật đa thức nhẹ LWPK (Lightweight Polynomial Secrete Key) để truyền thông dựa trên cụm phân cấp an toàn. Cơ chế này được xây dựng dựa trên mật mã đường cong Elip bằng cách trao đổi khóa đối xứng ECC để truyền dữ liệu an toàn. Cơ chế đề xuất đảm bảo yêu cầu bảo mật tốt hơn và nó có thể chống lại một cách mạnh mẽ các cuộc tấn công độc hại. Tác giả đã so sánh cơ chế đề xuất với cơ chế khóa nhóm hiện tại và tiến hành đánh giá hiệu suất về chi phí hoạt động, tỷ lệ phân phối gói, độ trễ từ đầu đến cuối và tiêu thụ năng lượng. Kết quả mô phỏng cho thấy cơ chế đề xuất có hiệu quả tốt hơn so với cơ chế khóa nhóm, và cơ chế này cũng tiết kiệm về năng lượng.

Các tác giả trong [65] đã đề xuất một giao thức định tuyến an toàn dựa trên tối ưu hóa đàn kiến đa mục tiêu SRPMA (Secure Routing Protocol based on Multi-objective Ant-colony-optimization) để giải quyết các vấn đề về giới hạn tài nguyên và sự an toàn của định tuyến trong WSN. Thuật toán đàn kiến được cải tiến thành thuật toán định tuyến đa mục tiêu với việc xem xét năng lượng còn lại của các nút và giá trị tin cậy của đường dẫn là hai mục tiêu tối ưu hóa. Mô hình đánh giá tin cậy nút được thiết lập bằng cách sử dụng lý thuyết bằng chứng D-S được cải tiến với tiền xử lý xung đột để đánh giá mức độ tin cậy của nút. Kết quả định tuyến đa mục tiêu thu được thông qua việc sử dụng cơ chế giải pháp tối ưu Pareto bằng cách sử dụng phương pháp lưu trữ bên ngoài với tiêu chí khoảng cách đám đông. Các kết quả mô phỏng được thực hiện với NS2 cho thấy thuật toán được đề xuất có thể đạt được hiệu suất mong muốn chống lại cuộc tấn công Blackhole trong định tuyến WSN.

Các tác giả trong [66] đã đề xuất một phương pháp độ chính xác phát hiện cảm biến bất thường ASDA-RSA (Abnormal Sensor Detection Accuracy) được sử dụng để chống lại các cuộc tấn công từ chối giấc ngủ (Denial of Sleep - DoS) để giảm lượng năng lượng tiêu thụ, các cuộc tấn công DoS gây mất năng lượng trong các cảm biến bằng cách giữ cho các nút không chuyển sang chế độ ngủ nhằm tiết kiệm năng lượng. Cơ chế ASDA-RSA bao gồm hai giai đoạn để tăng cường bảo mật trong các WSN. Trong pha đầu tiên, một cách tiếp cận phân cụm dựa trên năng lượng và khoảng cách được sử dụng để chọn cụm trưởng thích hợp. Và trong pha thứ hai, thuật toán mã hóa RSA và giao thức khóa liên động được sử dụng kết hợp cùng với phương thức xác thực, để ngăn chặn các cuộc tấn công DoS. Hơn nữa, phương pháp ASDA-RSA còn được đánh giá thông qua các mô phỏng mở rộng được thực hiện trong NS2. Kết quả mô phỏng chỉ ra rằng các số liệu hiệu suất mạng WSN được cải thiện về thông lượng trung bình, tỷ lệ phân phối gói, tuổi thọ mạng và tỷ lệ phát hiện.

## V. KẾT LUẬN

Khi tốc độ phát triển và nhu cầu sử dụng mạng cảm biến không dây trong cuộc sống ngày nhiều hơn, thì vấn đề về bảo mật trong WSN ngày càng trở nên rõ ràng và cấp thiết. Trong bài báo này, chúng tôi trình bày một cuộc khảo sát gần như toàn diện đối với lĩnh vực bảo mật gồm: những ràng buộc, yêu cầu bảo mật, các cuộc tấn công điển hình, phân loại chúng dựa trên các lớp theo mô hình OSI, và tóm tắt các nghiên cứu gần đây nhất về bảo mật trong WSN. Mục đích của bài báo là đưa ra một cái nhìn tổng quan chung đối với vấn đề bảo mật hiện nay, từ đó cung cấp những kiến thức nền tảng cho các nhà nghiên cứu về lĩnh vực bảo mật trong WSN. Tuy nhiên, phần đóng góp của bài báo vẫn còn hạn chế do chưa đưa ra được sự so sánh giữa các nghiên cứu gần đây, đồng thời chưa chỉ ra được những tồn tại của các phương pháp này. Trong thời gian tới, bài báo sẽ được phát triển bằng cách khắc phục những hạn chế ở trên, từ đó đưa ra được những phân tích và đề xuất cụ thể hơn về bảo mật đối với các WSN hạn chế về tài nguyên.

## TÀI LIỆU THAM KHẢO

[1] Grand View Research, “Industrial Wireless Sensor Network (IWSN) Market Size, Share & Trends Analysis Report By Component (Hardware, Software, Service), By Type, By Technology, By Application, By End Use, And Segment Forecasts, 2019 - 2025”, 2019.

[2] M. K. Jain, “Wireless sensor networks: security issues & challenges”, IJCIT, vol. 2, no. 1, pp. 62-67, 2011.

[3] D. Carman, P. Kruus, B. J. Matt, “Constraints and approaches for distributed sensor network security”, Technical Report 00-010, NAI Labs, 2000.

[4] M. Conti, “Secure Wireless Sensor Networks: Threats and Solutions”, Advances in Information Security, vol. 65, 2016.

[5] C. H. Tseng, S. H. Wang, W. J. Tsaur, "Hierarchical and Dynamic Elliptic Curve Cryptosystem Based Self-Certified Public Key Scheme for Medical Data Protection", IEEE Transactions on Reliability, Vol. 64, Issue: 3, pp. 1078-1085, 2015.

[6] J. P. Walters, Z. Liang, W. Shi, V. Chaudhary, "Wireless sensor network security: A survey," Proceedings of the Security in Distributed, Grid, Mobile, and Pervasive Computing. CRC Press, Boca Raton, FL, USA, 2007.

[7] A. Perrig, R. Szewczyk, V. Wen, D.E. Culler, J.D. Tygar, "SPINS: security protocols for sensor networks, Proceedings of the 7th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom'01), pp. 189-199, 2001.

[8] T. Winkler, B. Rinner, "Security and privacy protection in visual sensor networks: A survey", ACM Computing Surveys (CSUR), vol. 47, no. 1, 2014.

[9] A. Singla, R. Sachdeva, "Review on security issues and attacks in wireless sensor networks", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 4, pp. 529-534, 2013.

[10] C. M. Chen, "RCDA: Recoverable concealed data aggregation for data integrity in wireless sensor networks", IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 4, pp. 727-734, 2012.

[11] M. Dener, "Security analysis in wireless sensor networks", International Journal of Distributed Sensor Networks, vol. 10, no. 10, 2014.

[12] H. Chan, A. Perrig, D. Song, "Random key pre distribution schemes for sensor networks", Proceedings of the IEEE Symposium on Security and Privacy, IEEE Computer Society, pp. 197, 2003.

[13] D. Liu, P. Ning, R. Li, "Establishing pair-wise keys in distributed sensor networks", ACM Transactions on Information Systems Security, vol. 8, no. 1, pp. 41-77, 2005.

[14] S. Ganeriwal, C. Popper, S. Capkun, M.B. Srivastava, "Secure time synchronization in sensor networks", ACM Trans. Inf. Syst. Secur. 11(4), pp. 1-35, 2008.

[15] I. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "A survey on sensor networks", IEEE Commun. Mag., vol. 40, pp. 102-114, 2002.

[16] S. Vadlamani, B. Eksioglu, H. Medal, A. Nandi, "Jamming attacks on wireless networks: A taxonomic survey", International Journal of Production Economics, vol. 172, pp. 76-94, 2016.

[17] Y. Wang, G. Attebury, B. Ramamurthy, "A Survey of Security Issues In Wireless Sensor Networks", IEEE Communications Surveys & Tutorials, vol 8, no. 2, 2006.

[18] X. Chen, K. Makki, K. Yen, N. Pissinou, "Sensor Network Security: A Survey", IEEE Communications Surveys & Tutorial, vol 11, no. 2, 2009.

[19] Y. Zhou, Y. Fang, Y. Zhang, "Security Wireless Sensor Networks: A Survey", IEEE Communication Surveys, 2008.

[20] X. Wang, W. Gu, K. Schosek, S. Chellappan, D. Xuan, "Sensor network configuration under physical attacks", Technical report (OSU-CISRC-7/04-TR45), 2004.

[21] A. Becher, Z. Benenson, M. Dornseif, "Tampering with Motes: Real-World Physical Attacks on Wireless Sensor Networks", International Conference on Security in Pervasive Computing, pp. 104-118, 2006.

[22] S. Mohammadi, H. Jadidoleslamy, "A Comparison of Physical Attacks on Wireless Sensor Networks", International Journal of Peer to Peer Networks (IJP2P), Vol. 2, No. 2, 2011.

[23] M. L. Messai, "Classification of Attacks in Wireless Sensor Networks", International Congress on Telecommunication and Application' 14, 2014.

[24] R. H. Khokhar, M. A. Ngadi, S. Mandala, "A Review of Current Routing Attacks in Mobile Ad Hoc Networks", Faculty of Computer Science and Information System", 2008.

[25] T. Kavitha, D. Sridharan, "Security Vulnerabilities in Wireless Sensor Networks: A Survey", Journal of Information Assurance and Security, 2009.

[26] A. Wood, J. Stankovic, "Denial of Service in Sensor Networks", IEEE Computer, vol. 35, 2002.

[27] K. Xing, S. S. R Srinivasan, M. Jose, J. Li, X. Cheng, "Attacks and Countermeasures in Sensor Networks: A Survey", Network security, 2010.

[28] C. K.Marigowda, M. Shingadi, "Security Vulnerability Issues In Wireless Sensor Networks: A Short Survey", International Journal Of Advance Research In Computer And communication Engineering, Vol. 2, Issue 7, 2013.

[29] J. Sen, "A Survey on Wireless sensor Network Security", International Journal of Communication Networks and Information Security, Vol. 1, No. 2, 2009.

[30] J. Sen, "Security in wireless sensor networks", Wireless Sensor Networks: Current Status and Future Trends, 2012.

[31] I. Dbibih, I. Iala, D. Aboutajdine, O. Zytoune, "Collision avoidance and service differentiation at the MAC layer of WSN designed for multi-purpose applications", Cloud Computing Technologies and Applications (CloudTech), 2nd International Conference, IEEE, 2016.

[32] J. Newsome, E. Shi, D. Song, A. Perrig, "The Sybil Attack in Sensor Networks: Analysis & Defenses", Center for Computer and Communications Security, 2004.

[33] L. Hu, D. Evans, "Using Directional Antennas to Prevent Wormhole Attacks", Network and Distributed System Security Symposium (NDSS), 2004.

[34] Y. Hu, A. Perrig, D. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks", 22nd Annual Joint Conference of the IEEE Computer and Communications Societies, 2003.

[35] Z. Gavrić, D. Simić, "Overview of DOS attacks on wireless sensor networks and experimental results for simulation of interference attacks", Ingenieria e Investigación, Vol. 38, No. 1, pp. 130-138, 2018.

[36] N. Fatema, R. Brad, "Attacks and counterattacks on wireless sensor networks", International Journal of Ad hoc, Sensor and Ubiquitous Computing, vol. 4(6), pp. 1-15, 2013.

[37] S. Mohammadi, H. Jadidoleslamy, "A Comparison of Link Layer Attacks on Wireless Sensor Networks", International Journal on applications of graph theory in wireless ad hoc networks and sensor networks, Vol. 3, No. 1, 2011.

[38] T. A. Zia, A. Zomaya, "A Security Framework for Wireless Sensor Networks", IEEE Sensors Applications Symposium, 2006.

[39] K. Sharma, M. K. Ghose, "Wireless Sensor Networks: An Overview on its Security Threats", IJCA, Special Issue on "Mobile Ad-hoc Networks" MANETs, 2010.

[40] C.A. Balanis, "Antenna theory: analysis and design", 4th Edition, John Wiley & Sons, 2016.

[41] M. Kamarei, A. H. N. Barati, A. Patooghy, M. Fazeli, "The More the Safe, the Less the Unsafe: An efficient method to

unauthenticated packets detection in WSNs", 7th Conference on Information and Knowledge Technology (IKT), Iran, 2015.

[42] S. Mohammadi, H. Jadidoleslamy, "A Comparison of Routing Attacks on Wireless Sensor Networks", Journal of Information Assurance and Security, Vol. 6, pp. 195-215, 2011.

[43] C. Karlof, D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures", Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications, pp. 113-127, 2003.

[44] R. I. Mulla, R. Patil, "Review of Attacks on Wireless Sensor Network and their Classification and Security", Imperial Journal of Interdisciplinary Research (IJIR), vol. 2, 2016.

[45] J. Ahlawat, M. Chawla, K. Sharma, "Attacks and Countermeasures in Wireless Sensor Network", International Journal of Computer Science and Communication Engineering (IJCSCE), pp. 66-69, 2012.

[46] M. Saxena, "Security in Wireless Sensor Networks: A Layer based Classification", Computer Science, 2007.

[47] J.R. Douceur, "The sybil attack", Proceedings of the 1st International Workshop on Peerto-Peer Systems (IPTPS'02), pp. 251-260, 2002.

[48] Gagandeep, Aashima, "Study on Sinkhole Attacks in Wireless Adhoc Network", International Journal on Computer Science and Engineering, Vol. 4, pp. 1078-1085, 2012.

[49] B. S. Jangra, V. Kumawat, "A Survey on Security Mechanisms and Attacks in Wireless Sensor Networks", International Journal of Engineering and Innovative Technology (IJEIT), Vol. 2, pp. 291-296, 2012.

[50] N. A. Alrajeh, S. Khan, B. Shams, "Intrusion detection systems in wireless sensor networks: A review", International Journal of Distributed Sensor Networks, 2013.

[51] K. M. Osama, "Hello flood counter measure for wireless sensor network", International Journal of Computer Science and Security, vol. 2, issue 3, 2007.

[52] V. P. Singh, S. Jain, J. Singhai, "Hello Flood Attack and its Countermeasures in Wireless Sensor Networks", International Journal of Computer Science Issues, Vol. 7, Issue 3, No. 11, 2010.

[53] J. Shukla, B. Kumari, "Security Threats and Defense Approaches in Wireless Sensor Networks: An Overview", International Journal of Application or Innovation in Engineering & Management (IJAIEM), 2013.

[54] H.N. Dai, Q. Wang, D. Li, "On eavesdropping attacks in wireless sensor networks with directional antennas", International Journal of Distributed Sensor Networks, 2013.

[55] M. A. Khan, M. Khan, "A Review on Security Attacks and Solution in Wireless Sensor Networks", American Journal of Computer Science and Information Technology, vol. 7, no. 1, 2019.

[56] M. N. Riaz, A. Buriro, A. Mahboob, "Classification of Attacks on Wireless Sensor Networks: A Survey", I.J. Wireless and Microwave Technologies, pp. 15-39, 2018.

[57] S. Mohammadi, H. Jadidoleslamy, "A Comparison of Transport and Application Layers Attacks on Wireless Sensor Networks", Journal of Information Assurance and Security, Vol. 6, pp. 331-345, 2011.

[58] D. R. Raymond, S. F. Midkiff, "Denial of Service in Wireless Sensor Network: Attacks and Defenses", Computer Communication, 2008.

[59] O. Osanaiye, A. S. Alfa, G. P. Hancke, "A Statistical Approach to Detect Jamming Attacks in Wireless Sensor Networks", Sensors, 2018.

[60] U. Ghugar, J. Pradhan, S. K. Bhoi, R. R. Sahoo, S. K. Panda, "PL-IDS: physical layer trust based intrusion detection system for wireless sensor networks", International Journal of Information Technology, 2018.

[61] B. Zhu, W. Susilo, J. Qin, F. Guo, Z. Zhao, J. Ma, "A Secure and Efficient Data Sharing and Searching Scheme in Wireless Sensor Networks", Sensors, 2019.

[62] J. Yang, S. He, Y. Xu, L. Chen, J. Ren, "A Trusted Routing Scheme Using Blockchain and Reinforcement Learning for Wireless Sensor Networks", Sensors, 2019.

[63] M. Selvi, K. Thangaramya, S. Ganapathy, K. Kulothungan, H. K. Nehemiah, A. Kannan, "An Energy Aware Trust Based Secure Routing Algorithm for Effective Communication in Wireless Sensor Networks", Wireless Personal Communications, 2019.

[64] S. J. Kalyane, N. B.Patil, "Lightweight Secure and Reliable Authentication for Cluster Based WSN", International Journal of Engineering and Advanced Technology (IJEAT), vol. 9, 2019.

[65] Z. Sun, M. Wei, Z. Zhang, "Secure Routing Protocol based on Multi-objective Ant-colony-optimization for wireless sensor networks", Applied Soft Computing Journal 77, pp. 366-375, 2019.

[66] R. Fotohi, S. F. Bari, M. Yusefi, "Securing Wireless Sensor Networks Against Denial-of-Sleep Attacks Using RSA Cryptography Algorithm and Interlock Protocol", International Journal of Communication Systems, 2019.

## A SURVEY OF SECURITY ISSUES IN WIRELESS SENSOR NETWORKS

***Abstract:*** In recent years, Wireless Sensor Network (WSN) is emerging as a promising field of research due to the low cost of sensors, widely applications, and easily deployment. WSNs focus on sensing the statuses of particular object and then transmitting real-time data from the sensors to the back-end systems for processing and analysis. However, the sensing information are normally private and confidential, and sensors often operate in harsh and unattended environments, so the security and privacy of WSN systems are being a considerable topic. In this article, we present a survey of security issues for WSN. First, we introduce the overview of WSN including the constraints and security requirements. We then show a comprehensive review of the threats to WSNs and classify the defenses based on layers according to the OSI model. In addition, we summarize new security techniques and methods that have been published recently and point out the problems and directions in open research issues for each mentioned problem.

***Keyword:*** Wireless Sensor Network (WSN), Authentication, Secure routing, Security, Denial of Service (DoS).

**Nguyễn Văn Trường,** Nhận học vị Thạc sỹ năm 2010. Hiện đang công tác tại VNPT Thừa Thiên Huế và là nghiên cứu sinh tại Học viện Công nghệ Bưu chính Viễn thông. Lĩnh vực nghiên cứu: Mạng cảm biến không dây và IoT.

**Dương Tuấn Anh,** Nhận học vị Tiến sỹ năm 2013. Hiện đang công tác tại VNPT Thừa Thiên Huế. Lĩnh vực nghiên cứu: Hệ thống chuyển mạch, mạng truy nhập, đa truy nhập vô tuyến và IoT.

**Nguyễn Quý Sỹ,** nhận học vị Tiến sĩ năm 2003. Hiện công tác tại Học viện Công nghệ Bưu chính viễn. Lĩnh vực nghiên cứu: Hệ thống chuyển mạch, mạng truy nhập, truyền dữ liệu, đa truy nhập vô tuyến, kiến trúc máy tính và IoT.