# HỆ THỐNG IDS VÀ TỐI ƯU NĂNG LƯỢNG ĐỐI VỚI PHƯƠNG PHÁP PHÁT HIỆN LƯU LƯỢNG BẤT THƯỜNG DỰA TRÊN LOGIC MỜ TRONG WSN

**Nguyễn Văn Trường[*], Dương Tuấn Anh[*], Nguyễn Quý Sỹ[+]**
[*]VNPT Thừa Thiên Huế
[+]Học viện Công nghệ Bưu chính Viễn thông

***Tóm tắt:*** Mạng cảm biến không (WSN) dây là một trong những công nghệ hứa hẹn với phạm vi ứng dụng vô cùng đa dạng, từ chăm sóc sức khỏe cho đến chiến thuật quân sự. Và khi WSN ngày càng trở nên phổ biến thì các mối đe dọa bảo mật cũng ngày càng được đa dạng hóa và có chủ ý. Những phương pháp tiếp cận bảo mật dựa trên phòng ngừa như mật mã, xác thực và quản lý khóa đã được sử dụng để bảo vệ WSN khỏi các loại tấn công khác nhau nhưng các cách tiếp cận này không đủ để bảo vệ mạng khỏi các cuộc tấn công nội bộ có thể trích xuất thông tin nhạy cảm. Do đó, hệ thống phát hiện xâm nhập (IDS) trở thành lớp phòng thủ quan trọng thứ hai để bảo vệ và giữ an toàn cho mạng khỏi các cuộc tấn công độc hại. Phát hiện bất thường là một trong những phương pháp bảo vệ xâm nhập điển hình, trong đó phương pháp hiện bất thường dựa trên suy luận mờ được chúng tôi nghiên cứu trước đây và đã mang lại một số kết quả tốt. Tuy nhiên, nó cũng phải đối mặt với một số thách thức điển hình như khi số biến đầu vào tăng thì năng lượng tiêu tốn cho việc xử lý cũng tăng theo, điều này làm ảnh hưởng đến hiệu năng mạng. Do đó, trong bài báo này, chúng tôi trình bày một cái nhìn toàn diện về hệ thống phát hiện xâm nhập và sử dụng một số kỹ thuật để tối ưu năng lượng đối với phương pháp phát hiện lưu lượng bất thường dựa trên Logic mờ. Kết quả mô phỏng và phân tích so sánh chứng minh rằng sau khi được tối ưu, phương pháp của chúng tôi vẫn có thể giữ được độ chính xác đối với chỉ số cảnh báo và tỷ lệ phát hiện sai trong khi chỉ cần tiêu tốn ít năng lượng dành cho bộ nhớ để xử lý các quy tắc hơn so với ban đầu.

***Từ khóa:*** Mạng cảm biến không dây, IoT, bảo mật, suy luận mờ, phát hiệm xâm nhập.

## I. MỞ ĐẦU

Bảo mật đối với WSN là bắt buộc và đang mang lại nhiều thách thức tương ứng cho các nhà nghiên cứu. Các kỹ thuật dựa trên phòng ngừa về cơ bản được xây dựng dựa trên mật mã, xác thực và quản lý khóa là tuyến phòng thủ đầu tiên để bảo vệ WSN. Tuy nhiên, trong trường hợp tuyến phòng thủ đầu tiên bị phá vỡ, các nút bị xâm nhập có thể bị trích xuất thông tin nhạy cảm về bảo mật như khóa bí mật, dẫn đến vi phạm bảo mật. Do đó, việc phát triển những kỹ thuật dựa trên phát hiện xâm nhập được xem như là tuyến phòng thủ thứ hai ngày càng có tầm quan trọng lớn.

Phát hiện bất thường là một nhánh của phát hiện xâm nhập. Phát hiện bất thường được định nghĩa là quá trình so sánh các định nghĩa của hoạt động được coi là bình thường với những sự kiện được quan sát nhằm xác định các sai lệch đáng kể. Hơn nữa, sự bất thường trong tập dữ liệu được định nghĩa là một quan sát có vẻ không nhất quán với phần còn lại của tập dữ liệu [1].

Hầu hết những công việc trước đây về mô tả sự kiện trong WSN đều sử dụng các giá trị chính xác, còn được gọi là rõ ràng, để chỉ định các tham số đặc trưng cho một sự kiện. Ví dụ, chúng ta có thể nhận được những giá trị số chính xác "100 độ C" hay "120 kilogram". Tuy nhiên, những kết quả cảm biến không phải lúc nào cũng chính xác. Ngoài ra, các cảm biến khác nhau, ngay cả khi đặt gần nhau, thường khác nhau về giá trị mà chúng thể hiện. Xét một tình huống ví dụ, sử dụng định nghĩa "rõ" nếu một người có chiều cao ≥ 1.8 m thì được gọi là cao. Do đó, một người cao 1.79 m không được coi là cao, nhưng nếu một người khác có chiều cao 1.81 m thì lại được coi là cao trong khi chênh lệnh giữa họ là không nhiều. Trong khi sử dụng các định nghĩa mờ, 2 người này sẽ được coi là cao với 2 mức độ khác nhau, điều này cung cấp thông tin có tính chính xác cao hơn.

Việc xác định các ngưỡng sự kiện chính xác trở thành một nhiệm vụ cực kỳ khó khăn khiến chúng tôi tin rằng việc sử dụng các giá trị rõ nét để mô tả các sự kiện WSN không phải là cách tiếp cận phù hợp nhất. Qua đó có thể thấy được, suy luận mờ có thể giải quyết những thách thức này tốt hơn suy luận rõ nét.

Phần còn lại của bài báo được tổ chức như sau. Phần II giới thiệu một số hệ thống phát hiện xâm nhập trong WSN. Phần III giới thiệu về phát hiện lưu lượng bất thường bằng phương pháp suy luận mờ. Phần IV trình bày giải pháp tối ưu năng lượng đối với phát hiện bất thường dựa trên suy luận mờ [2]. Cuối cùng, trong Phần V, chúng tôi kết luận bài viết và đưa ra một số hướng nghiên cứu trong tương lai.

Tác giả liên hệ: Nguyễn Văn Trường,
Email: nvtruong.dhkh@gmail.com
Đến tòa soạn: 11/2021, chỉnh sửa: 12/2021, chấp nhận đăng: 12/2021.

## II. MỘT SỐ HỆ THỐNG PHÁT HIỆN XÂM NHẬP TRONG WSN

### *A. Hệ thống IDS tập trung trong WSN*

Trong hệ thống IDS tập trung, các nút thành viên sau khi thu thập thông tin cảm biến sẽ được chuyển trực tiếp đến trạm gốc (BS). Trạm gốc thường có công suất và nguồn cung lớn với bộ xử lý cũng như dung lượng bộ nhớ mạnh hơn nhiều so với các nút cảm biến, với những liên kết băng thông cao để liên lạc với chúng. Mặt khác, các nút cảm biến bị hạn chế tài nguyên nên sử dụng công suất thấp hơn, băng thông thấp hơn, phạm vi hoạt động ngắn hơn.

Nghiên cứu [3] đề xuất một hệ thống IDS để phát hiện xâm nhập hiệu quả năng lượng dựa trên tiếp cận phát hiện hành vi bất thường. Mô hình đề xuất có thể phát hiện những kỹ thuật tấn công như chuyển tiếp có chọn lọc và tấn công Blackhole. Hệ thống IDS này sử dụng kiến trúc phát hiện tập trung vì thế BS có nhiệm vụ đảm nhận việc phát hiện các kẻ tấn công. Trong [4], một cơ chế phát hiện xâm nhập tập trung, sử dụng hai thông số đặc trưng là thông tin về nút chuyển tiếp và thông tin về định tuyến (ví dụ như số lượng bước) để phát hiện các cuộc tấn công chuyển tiếp có chọn lọc và Blackhole. IDS được đề xuất dựa trên kỹ thuật Support Vector Machines (SVM) và cửa sổ trượt (Sliding Windows). Các tác giả thông qua kiến trúc phát hiện tập trung, nơi quá trình phát hiện xâm nhập được thực hiện tại trạm gốc để nhận diện những cuộc tấn công Blackhole và những cuộc tấn công chuyển tiếp có chọn lọc với độ chính xác cao mà không làm cạn kiệt năng lượng của các nút. Tương tự, nghiên cứu [5] là một giải pháp đơn giản phát hiện xâm nhập cho IDS tập trung bằng cách sử dụng một cơ chế nghe quá mức để giảm gửi đi gói tin cảnh báo.

### *B. Hệ thống IDS phân tán trong WSN*

Hệ thống IDS phân tán trong WSN là một trong những hệ thống theo quy tắc (Rule-Based) đầu tiên và phổ biến nhằm phát hiện xâm nhập theo các phương thức tấn công khác nhau cho từng lớp trong mạng WSN [6]. Hệ thống có ba pha chính bao gồm: 1) Pha thu thập dữ liệu: các nút giám sát sẽ lắng nghe và lọc những thông tin quan trọng để phân tích. 2) Pha thiết lập quy tắc: các bản tin sẽ được kiểm thử qua những quy tắc đã được định nghĩa trước, nếu bản tin không vượt qua những quy tắc này thì bộ đếm lỗi sẽ tăng lên. 3) Pha phát hiện xâm nhập: số lượng lỗi phát sinh trong pha lập quy tắc sẽ được so sánh với một ngưỡng cho trước (thường được định nghĩa bằng số lượng lỗi trung bình trong các trường hợp hay xảy ra xâm nhập). Nếu tổng số lượng lỗi phát sinh ở pha trước vượt quá ngưỡng cảnh báo xâm nhập sẽ được phát ra.

Hệ thống IDS phân tán được chứng minh làm việc hiệu quả trong việc phát hiện xâm nhập bằng các loại tấn công khác nhau [7-11]. Tuy nhiên, một trong những điểm yếu của hệ thống là việc xác định số lượng nút giám sát cần thiết, cũng như làm sao để lựa chọn và đảm bảo độ tin cậy của các nút này trở nên khó khăn và không nhất quán đối với các loại tấn công khác nhau. Hơn nữa, hệ thống cũng gặp khó khăn đối với các loại tấn công mới mà không có các quy tắc được xác định từ trước [12].

### *C. Hệ thống IDS phân cấp trong WSN*

Trong hệ thống IDS phân cấp (Hierrachical IDS), mạng cảm biến được chia thành các cụm các nút gần nhau. Các nút này được quản lý và giám sát bởi một nút trưởng cụm (Cluster Head - CH). Nút trưởng cụm thu thập dữ liệu từ các nút thành viên do đó hệ thống này thường phù hợp với các cấu hình mạng trong đó nút trưởng cụm được cung cấp năng lượng và khả năng tính toán mạnh.

Một số nghiên cứu gần đây về hệ thống IDS phân cấp bao gồm: Cơ chế bộ lọc hai pha để phát hiện tấn công Sinkhole trong mạng WSN được đề xuất bởi Wazid và cộng sự [13], cơ chế phân nhóm (Group-based) chịu trách nhiệm phát hiện tấn công Blackhole [14]. Đặc điểm chung của hai giải pháp trên là cơ chế phân cụm hai mức được đề xuất nhằm tăng khả năng phát hiện tấn công trong khi giảm chi phí mào đầu giữa các gói tin trao đổi nhằm tối ưu năng lượng. Khi nút trưởng cụm của nhóm có mức thấp (nhóm con) phát hiện có xâm nhập, nó gửi bản tin tương ứng tới nút trưởng cụm mức cao để chuyển tiếp tới trạm gốc. Mặc dù các phương pháp này được chứng minh hiệu quả với việc nút trưởng cụm chỉ giám sát một số lượng nút thành viên ít hơn, vấn đề của mô hình là nếu nút trưởng cụm bị nhiễm mã độc, nó sẽ không gửi hoặc cố tính gửi sai cảnh báo tới nút trưởng cụm cao hơn hoặc trạm gốc.

### *D. Hệ thống IDS dựa vào độ uy tín*

Một số nghiên cứu điển hình về hệ thống IDS dựa vào độ uy tín (Reputation-Based IDS) đã được đề xuất trước đây [15-20]. Các tác giả trong [21] đã đề xuất ý tưởng đánh dấu các gói tin trao đổi trong khi sử dụng thuật toán xếp hạng để phát hiện gói tin bị nhiễm mã độc. Khi nút Sink nhận được gói tin đã được đánh dấu, nó sẽ tính toán tỷ lệ rớt gói trung bình cho mỗi nút thành viên. Nếu tỷ lệ này vượt qua một ngưỡng cho trước, nút này sẽ bị phân loại là nút bị nhiễm mã độc. Nghiên cứu trong [22] đã đề xuất hệ thống phát hiện các hoạt động bất thường trong mạng WSN sử dụng đồng thời phương pháp phát hiện hành vi sai khác của các nút và mô hình đánh giá độ tin cậy ở mức độ hệ thống. Ý tưởng chính của hệ thống là mỗi nút thành viên sẽ tính toán độ tin cậy của các nút hàng xóm dựa theo hành vi mà nó quan sát được. Trạm gốc sẽ phân loại nút bất thường bằng cách kết hợp những giá trị này sau khi được tính toán và gửi về từ các nút thành viên và các quy tắc mà nó đã định nghĩa trước về các nút bất thường. Kết quả mô phỏng cho thấy phương pháp này hoạt động hiệu quả trong các mạng WSN tập trung, giảm năng lượng tiêu thụ so với các hệ thống không sử dụng IDS. Tuy nhiên, nghiên cứu này không chỉ rõ độ tin cậy của hệ thống và chỉ giới hạn cho các mạng WSN tập trung.

### *E. Hệ thống IDS xuyên lớp*

Các tác giả trong [23] đề xuất hệ thống IDS xuyên lớp (Cross-layer IDS) sử dụng một cơ chế phát hiện xâm nhập trung gian để trao đổi thông tin giữa lớp vật lý, lớp MAC và lớp mạng trong mô hình giao thức OSI. Thông tin trao đổi bao gồm những hành vi khác nhau như cảnh báo rớt gói, kích hoạt cờ của các nút hàng xóm,... Phương pháp được đánh giá hiệu quả trong việc phát hiện một số loại xâm nhập khác nhau như tấn công Sinkhole, tấn công định tuyến hoặc tấn công DDoS. Tuy nhiên, hạn chế của phương pháp là chỉ tập trung vào phát hiện nhưng chưa đề xuất được giải pháp cho các loại tấn công này.

*Bảng 1. Tóm tắt các hệ thống phát hiện xâm nhập*

| Hệ thống IDS | Cơ chế, giải pháp | Phát hiện tấn công | Nhược điểm trong mạng WSN | Tài liệu |
|---|---|---|---|---|
| Tập trung | Trạm gốc đảm nhận việc phát hiện hành vi bất thường của nút giám sát; sử dụng quy tắc được định nghĩa từ trước để phát hiện tấn công. | - Selective forwarding<br>- Blackhole | Chỉ hoạt động tốt đối với mạng WSN có kiến trúc phẳng. | 3, 4 |
| | | - Routing | | 5 |
| Phân tán | Sử dụng quy tắc được định nghĩa từ trước để phát hiện tấn công; gồm ba pha: thu thập dữ liệu, thiết lập quy tắc, phát hiện xâm nhập. | - Blackhole<br>- Sinkhole<br>- Selective Forwarding<br>- DoS<br>- DDoS | Khó khăn trong việc xác định số lượng nút giám sát cần thiết; không có quy tắc nhất quán đối với các loại tấn công khác nhau; khó lựa chọn nút giám sát có độ tin cậy cao. | 6, 7, 8, 9, 10, 11, 12 |
| Phân cấp | Mạng cảm biến được chia thành các cụm bao gồm các nút gần nhau và được giám sát bởi nút trưởng cụm; nút trưởng cụm có năng lực tính toán lớn để thu thập dữ liệu từ các nút thành viên. | - Sinkhole | Chỉ hoạt động tốt khi nút trưởng cụm giám sát số lượng ít nút thành viên; khó phòng chống nếu nút trưởng cụm bị tấn công. | 13 |
| | | - Blackhole | | 14 |
| Dựa vào độ uy tín | Đánh dấu các gói tin trao đổi trong khi sử dụng thuật toán xếp hạng để phát hiện gói tin bị nhiễm mã độc; tính toán tỷ lệ rớt gói trung bình cho các nút thành viên để so sánh với ngưỡng cảnh báo; tính toán độ tin cậy của các nút hàng xóm dựa theo hành vi mà nó quan sát được. | - Sinkhole<br>- Selective Forwarding<br>- Routing<br>- Internal<br>- Packet dropping | Khó đánh giá chính xác độ tin cậy của các nút hàng xóm, dẫn đến sai khác về độ tin cậy cho toàn bộ hệ thống; thường chỉ giới hạn cho các mạng WSN tập trung. | 15, 18, 19, 21, 22 |
| Xuyên lớp | Trao đổi thông tin giữa lớp vật lý, lớp MAC và lớp mạng trong mô hình giao thức như cảnh báo rớt gói, kích hoạt cờ nút hàng xóm. Sử dụng nút mobile trung gian để phát hiện xâm nhập. | - Sinkhole<br>- Routing<br>- DoS | Chỉ tập trung vào phát hiện nhưng chưa đề xuất được giải pháp cho các loại tấn công này. | 23 |
| | | - Sinkhole<br>- Wormhole<br>- Sybil | Chỉ áp dụng cho các mô hình mạng WSN phẳng mà không áp dụng cho các mạng WSN phân cấp | 24 |
| Dựa trên lý thuyết trò chơi | Áp dụng tiếp cận phân cấp và phát hiện xâm nhập ở ba cấp độ khác nhau: cấp nút cảm biến, cấp cụm trưởng và cấp trạm gốc. Có thể áp dụng các lý thuyết trò chơi khác nhau như trò chơi không hợp tác, trò chơi hợp tác, trò chơi lặp, trò chơi Markov. | - DoS<br>- DDoS<br>- Packet dropping<br>- Route compromise<br>- Selfish behavior | Chỉ phát hiện được một sự kiện tấn công trong mạng, trong khi mạng WSN thường chịu nhiều cuộc tấn công với nhiều phương thức khác nhau. | 25, 26, 27, 30, 31, 32, 33 |
| | Lý thuyết đấu giá, trò chơi liên minh | - Tăng cường khả năng bảo mật | | 34, 35 |
| Dựa trên đặc tính thống kê | Sử dụng biểu đồ luồng dựa trên phân tích đa biến thống kê Chi-square; Mô hình Markov ẩn; thuật toán di truyền. | - Sinkhole<br>- DoS<br>- Unauthorized | Một số phương pháp yêu cầu giám sát tất cả các nút thành viên dẫn đến phát sinh năng lượng tiêu thụ. | 36, 37, 38, 39, 40 |
| | Dựa trên các quy tắc suy luận mờ | - Hầu hết mọi loại tấn công | Yêu cầu sử dụng nhiều năng lượng. | 41 |
| Dựa trên học máy | Học nông: k-NN, LR, SVM, DT, RF, Neural Networks; học sâu: Deep Learning. | - Malware<br>- DoS<br>- Phân loại hành vi bình thường/bất thường | Muốn hệ thống phát hiện xâm nhập với độ chính xác cao cần tiêu tốn nhiều năng lượng để huấn luyện dữ liệu; độ tin cậy cho dữ liệu không được đảm bảo. | 42, 43, 44 |
| | | - Blackhole<br>- Opportunistic<br>- DDoS<br>- Sinkhole<br>- Wormhole | | 45, 46 |
| Dựa trên suy luận mờ | Sử dụng các bộ ước tính mờ và bộ quy tắc để thiết lập ngưỡng phát hiện xâm nhập; có thể bỏ qua sự thiếu toàn vẹn và chính xác của dữ liệu cảm biến. | - Jamming<br>- DoS<br>- DDoS<br>- Sinkhole<br>- Packet dropping | Cần các quy tắc được thiết lập trước quá trình phát hiện; số lượng các quy tắc tăng theo cấp số mũ theo số lượng các biến, dẫn đến yêu cầu bộ nhớ lớn và làm chậm quá trình truy vấn và ra quyết định. | 51, 53, 54, 55, 56, 58 |
| | | - Eavesdropping<br>- De-synchronization<br>- DoS<br>- Collision<br>- Traffic analysis<br>- Selective forwarding<br>- Route information manipulation<br>- Sinkhole<br>- Jamming<br>- Clone | | 60, 61 |

Nghiên cứu trong [24] sử dụng nút mobile trung gian thông qua hai pha để phát hiện xâm nhập cho mạng WSN. Trong pha đầu tiên, tấn công được phát hiện bằng cách tương quan những đặc tính giữa các lớp như lớp MAC và lớp mạng. Những đặc tính này có thể là số lượng các gói được định tuyến/rớt ở lớp mạng và số lượng đa truy nhập/rớt gói ở lớp MAC. Ở pha thứ hai, nếu tấn công được phát hiện, nút mobile trung gian sẽ được sử dụng. Nút mobile này chỉ thỏa hiệp với các nút hàng xóm thông qua cơ chế bắt tay ba bước, cho nên nó sẽ không lắng nghe lưu lượng tạo bởi những nút độc. Do đó, nút mobile trung gian sẽ được tin tưởng để chuyển tiếp lưu lượng từ các nút bình thường tới nút sink. Phương pháp này được chứng minh hiệu quả trong việc phát hiện và ngăn ngừa một số loại tấn công như tấn công Sinkhole, tấn công Wormhole hoặc tấn công Sybil. Tuy nhiên, phương pháp chỉ áp dụng cho các mô hình mạng WSN phẳng mà không áp dụng cho các mạng WSN phân cấp. Hơn nữa, độ tương quan trong pha đầu tiên chỉ sử dụng thông tin về số lượng gói tin truyền được/bị rớt. Một số thông tin như vị trí hoặc thời gian của nút mobile có thể được áp dụng để nâng cao khả năng phát hiện cũng như bảo mật cho mạng WSN.

### *F. Hệ thống IDS dựa trên lý thuyết trò chơi*

Các hệ thống IDS dựa trên lý thuyết trò chơi lần đầu được giới thiệu cho mạng WSN trong tài liệu [25][26]. Mục đích của trò chơi là tìm ra nút được đánh giá là "yếu nhất", khi mà nó có khả năng cao và dễ bị tấn công hoặc xâm nhập từ bên ngoài. Nghiên cứu trong [27] đề xuất phương pháp phát hiện xâm nhập đa lớp dựa trên lý thuyết trò chơi tối ưu năng lượng cho mạng WSN. Phương pháp đề xuất áp dụng tiếp cận phân cấp và phát hiện xâm nhập ở ba cấp độ khác nhau, cụ thể là cấp nút cảm biến, cấp cụm trưởng (CH) và cấp trạm gốc (BS). Tiếp cận này mô hình hóa sự tương tác giữa IDS và nút cảm biến đang được theo dõi như một trò chơi Bayes không hợp tác giữa hai người chơi. Điều này cho phép IDS áp dụng các chiến lược giám sát theo xác suất dựa trên cân bằng Bayesian Nash (BNE), từ đó giảm một số lượng lớn lưu lượng IDS. Ngoài ra, nghiên cứu cũng đề xuất hai cơ chế cập nhật và hủy bỏ độ uy tín khác nhau để mô hình hóa quá trình hợp tác và ngăn cản hành vi ích kỷ giữa các nút giám sát. Các tác giả trong [28] đề xuất phương pháp phát hiện và ngăn ngừa các nút khả nghi bị nhiễm độc bằng lý thuyết trò chơi. Trong đó, mô hình sẽ sử dụng trò chơi lặp (repeated game) để ngăn ngừa các nút độc loại bỏ các gói có độ ưu tiên cao HPPs (High Priority Packets) nhằm tối ưu mức tin cậy ưu tiên của nó (High Priority data Trustworthiness - HPT). Lúc này nó sẽ được các nút giám sát chấp thuận gia nhập mạng từ đó phân tán lưu lượng độc hại cho mạng WSN. Nghiên cứu [29] giới thiệu một chiến lược sử dụng lý thuyết trò chơi kết hợp thuật toán Q-learning. Mô hình đề xuất bao gồm các nút sink, một trạm gốc và một kẻ tấn công chủ động được dùng để kiểm tra các cuộc tấn công DoS phân tán (DDoS). Các tác giả cho rằng mô hình được đề xuất có khả năng bảo vệ tốt so với các giải pháp lý thuyết trò chơi Markov.

Khảo sát trong [30] đã chỉ ra rằng một số mô hình được sử dụng trong lý thuyết trò chơi như mô hình trò chơi không hợp tác (non-cooperative game) [25], trò chơi có hợp các (cooperative game) [31], trò chơi lặp (repeated game) [26][32] hoặc trò chơi Markov [33] có khả năng phòng chống tấn công DoS/DDoS và phát hiện xâm nhập; trong khi lý thuyết đấu giá (auction theory) [34] và trò chơi liên minh (coalitional game) [35] được sử dụng để nâng cao khả năng bảo mật. Tuy nhiên, nhược điểm của tiếp cận sử dụng lý thuyết trò chơi là chúng chỉ phát hiện được một sự kiện tấn công trong mạng, trong khi mạng WSN thường chịu nhiều cuộc tấn công với nhiều phương thức khác nhau.

### *G. Hệ thống IDS dựa trên đặc tính thống kê*

Nghiên cứu trong [36] đã đề xuất một hệ thống IDS phát hiện các cuộc tấn công Sinkhole bằng cách sử dụng một biểu đồ luồng. Giải thuật này áp dụng kỹ thuật phân tích đa biến dựa trên thống kê Chi-square, được thực hiện bằng cách sử dụng mô phỏng và phân tích lý thuyết. Các tác giả đã chỉ ra rằng mô hình đề xuất có chi phí mào đầu thấp nên phù hợp với các mạng IoT. Doumit và Agrawal trong [37] sử dụng mô hình Markov ẩn để phát hiện các hành vi bất thường. Kết quả mô phỏng chứng minh rằng thuật toán đề xuất chỉ yêu cầu tài nguyên xử lý tối thiểu trong các kịch bản thử nghiệm. Do đó, mô hình cũng có thể được sử dụng cho mạng WSN. Nghiên cứu [38] phân tích về một thuật toán dựa trên việc xử lý lưu lượng đến. Đặc biệt, mô hình lưu lượng truy cập đến của một nút được quan sát và dựa trên những nghiên cứu trước đây để đưa ra kỹ thuật phát hiện hành vi bất thường. Thống kê ngắn hạn được thuật toán lưu giữ bằng cách sử dụng cửa sổ trượt đa mức giúp giảm yêu cầu tài nguyên. Do đó, mô hình như vậy cũng có thể được xem xét cho các thiết bị IoT với yêu cầu hạn chế về tài nguyên tính toán. Một thuật toán khác của cùng tác giả được giới thiệu trong [39]. Ở đây, mỗi nút sẽ tự phát triển một mô hình riêng cho các nút lân cận dựa trên hành vi thu phát và tỷ lệ gói tin đến của chúng. Khi có sai lệch lớn, chúng sẽ được coi là hành vi bất thường. Tuy nhiên, cách tiếp cận này có thể yêu cầu giám sát tất cả các nút hàng xóm do vậy năng lượng tiêu thụ có thể phát sinh đáng kể. Vì thế tiếp cận này có thể không phải là một giải pháp khả thi cho các mạng WSN. Nghiên cứu [40] đề xuất một hệ thống IDS có hiệu quả chống lại các cuộc tấn công từ chối dịch vụ (DoS) và trái phép (unauthorized). Kỹ thuật này dựa trên thuật toán di truyền (Genetic Programming). Phương pháp phát hiện xâm nhập dựa trên các quy tắc suy luận mờ được giới thiệu trong [41]. Phương pháp này được các tác giả khẳng định là có độ chính xác 100% cho mọi kiểu tấn công. Tuy nhiên, kỹ thuật này dường như không hiệu quả về việc tối ưu năng lượng nên ít phù hợp hơn với các mạng WSN.

### *H. Hệ thống IDS dựa trên học máy*

Học máy (Machine Learning) đang được áp dụng cho hầu hết mọi lĩnh vực. Những năm gần đây, các hệ thống IDS áp dụng học máy cũng đang được nghiên cứu mạnh mẽ [42] sử dụng giải thuật học sâu (Deep Learning) để phát hiện phần mềm độc hại (malware) trong các mạng IoT với độ chính xác lên đến 99%. Nghiên cứu trong [43] so sánh một số phương pháp học máy phổ biến như K-nearest neighbors (K-NN), Support Vector Machines (SVM), Decision Trees (DT), Random Forests (RF) và Neural Networks (NN) để phân biệt các gói tin IoT bình thường và các gói tin tấn công DoS. Kết quả cho thấy Random Forests có hiệu quả tốt nhất về độ chính xác và thời gian xử lý. Nghiên cứu [44] đề xuất một phương pháp dựa trên học máy để phát hiện xâm nhập cho mạng WSN chuyển động (Mobile WSN). Cụ thể, các giải thuật học máy như Linear Regression và Random Forests được sử dụng cùng với hệ thống IDS có sẵn để phân loại những nút bất thường với các nút bình thường. Kết quả cho thấy

hệ thống có tỷ lệ phát hiện nút độc lên tới 98% trong điều kiện nút di chuyển với tốc độ cao và 90% trong điều kiện nút di chuyển với tốc độ thấp. Các tác giả trong [45][46] phát triển hệ thống IDS dựa trên học sâu cho mạng WSN. Kết quả mô phỏng được thực hiện trên những kịch bản tấn công khác nhau như tấn công blackhole, tấn công cơ hội (Opportunistic attack), tấn công DDoS, tấn công Sinkhole và tấn công Wormhole. Kết quả cho thấy hệ thống IDS áp dụng học sâu có thể phát hiện xâm nhập lên tới 96-99%.

Tóm tắt về các hệ thống phát hiện xâm nhập được trình bày trong bảng 1.

## III. PHÁT HIỆN LƯU LƯỢNG BẤT THƯỜNG BẰNG PHƯƠNG PHÁP SUY LUẬN MỜ

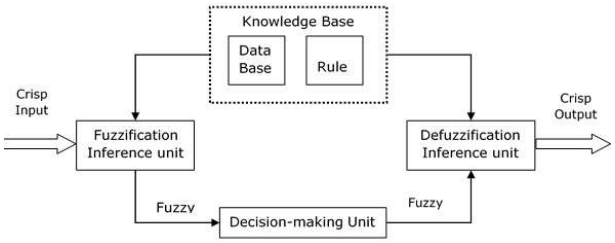
Một trong những đặc trưng nổi bật trong việc suy luận của con người là con người có thể thông qua các thông tin không đầy đủ và thiếu chính xác để đưa ra những quyết định chính xác và tự hoàn thiện thông tin. Trong khi một lượng lớn dữ liệu thu thập được hiện nay có tính trừu tượng cao và không có tính liên kết, gây khó khăn cho việc phân tích với độ chính xác cao. Đặc biệt, mặc dù những nút cảm biến không dây bị giới hạn về năng lực tính toán cũng như nguồn cấp, chức năng của các cảm biến ngày càng được mở rộng để phục vụ nhiều mục đích khác nhau. Hầu hết những nghiên cứu trước đây về WSN đều sử dụng các giá trị tuyệt đối, hay còn gọi là Crisp, là các giá trị mô tả những thông số cần quan tâm. Việc sử dụng các giá trị Crisp trong WSN đôi khi không phải là tiếp cận phù hợp cho nhiều mô hình, khi mà các dữ liệu cảm biến thu thập được không phải lúc nào cũng chính xác.

Trong bối cảnh như vậy, suy luận mờ (Fuzzy Inference) là một tiếp cận khả thi cho mạng WSN khi phương pháp này có thể chấp nhận sự sai số trong dữ liệu cảm biến. Suy luận mờ có cách tiếp cận giống với suy luận của con người hơn là sử dụng các giá trị Crisp hoặc các thuật toán phân loại dựa trên lý thuyết xác suất, điều này khiến cho suy luận mờ trực quan và dễ sử dụng hơn [47]. Là một ngôn ngữ mô hình hóa rất mạnh mẽ, suy luận mờ có thể được sử dụng để đối phó với một phần lớn các trường hợp không chắc chắn trong những tình huống thực tế. Vì tính tổng quát của lý thuyết mờ, nó có thể thích nghi với nhiều hoàn cảnh và ngữ cảnh khác nhau [48]. Nhược điểm của suy luận mờ là số lượng quy tắc phục vụ cho suy luận tăng theo hàm mũ tương ứng với số lượng biến (giả sử n biến, mỗi biến có thể nhận m giá trị, thì số lượng quy tắc có thể thiết lập là $m^n$) và cần một bộ nhớ mạnh mẽ để lưu giữ các giá trị này [49].

Trong nghiên cứu [50], tiếp cận suy luận mờ được sử dụng để xác định có hành vi bất thường trong một khoảng thời gian bằng cách đưa ra một ngưỡng để quan sát luồng dữ liệu đến. Tương tự, các tác giả trong [51] đề xuất một phương pháp nhận diện tấn công Jamming sử dụng suy luận mờ để thiết lập một giá trị ngưỡng cho tập các thông số. Để ước tính lưu lượng truy cập trước đó, suy luận mờ đã được sử dụng cho bộ tham số mô tả luồng lưu lượng. Ước tính mờ (Fuzzy Estimator) các tham số trong các mô hình thống kê đã được phân tích trong nghiên cứu [52], đưa ra một hàm thành viên (Membership Function) chính xác và duy nhất cho các ước tính mờ đối với một số phân phối phổ biến. Trong nghiên cứu [53], các tác giả đã đề xuất một phương pháp dựa trên suy luận mờ để phát hiện những cuộc tấn công DDoS bằng cách xây dựng một ước tính mờ về thời gian đến trung bình giữa các gói tin. Kết quả phân tích đã chỉ ra rằng sử dụng các bộ ước tính mờ có thể tránh được những thiếu sót từ những giả định về mô hình phân phối của lưu lượng.

### A. *Hệ thống suy luận mờ*

Hình 1 giới thiệu về hệ thống suy luận mờ (Fuzzy Inference System - FIS) bao gồm một hệ thống ánh xạ các biến đầu vào thành các biến đầu ra thông qua bộ suy luận mờ được hình thành từ những quy tắc IF-THEN, hàm thành viên, và các toán tử suy luận mờ. Một hệ thống lý luận mờ bao gồm 4 thành phần: Khối cơ sở tri thức, khối mờ hóa, khối quyết định và khối giải mờ. Trong đó khối cơ sở tri thức chứa các tập mờ và các quy tắc mờ.




*Hình 1. Hệ thống suy luận mờ - FIS*

### B. *Nhận diện bất thường trong mạng WSN dựa trên suy luận mờ*

Nghiên cứu trong [54] đề xuất một cơ chế phát hiện xâm nhập dựa trên logic mờ. Một số đặc tính của lưu lượng được trích xuất để xây dựng các quy tắc mờ đó là: mức năng lượng của nút, tốc độ truyền bản tin, danh sách những nút lân cận và tỷ lệ lỗi trong quá trình truyền. Cơ chế được xây dựng nhằm phát hiện và ngăn chặn các cuộc tấn công từ chối dịch vụ DoS vốn luôn làm tiêu hao tài nguyên của hệ thống. Trạm gốc hoặc một số nút giám sát sẽ chịu trách nhiệm thu thập các bản tin từ vùng lân cận và giá trị ngưỡng phát hiện sẽ được bộ điều khiển mờ tính toán dựa trên bốn đặc điểm nêu trên.

Một tiếp cận phát hiện xâm nhập tương tự dựa trên logic mờ khác đã được các tác giả trong [55] đề xuất để phát hiện những cuộc tấn công Sinkhole trong mạng cảm biến khuếch tán có định hướng. Hai đặc tính liên quan đến các giao thức khuếch tán có hướng được sử dụng trong mạng WSN là tỷ lệ tăng cường (Reinforcement Ratio) và bán kính. Tỷ lệ tăng cường là tỷ lệ giữa các bản tin tăng cường được truyền trong một khu vực với số lượng sự kiện cảm nhận được từ các nút. Bán kính được định nghĩa là số bước nhảy giữa hai nút bất kỳ trong khu vực. Trong trường hợp tấn công Sinkhole, sẽ có nhiều lưu lượng bản tin tăng cường trong khu vực hơn bình thường và số bước nhảy sẽ nhỏ hơn. Bộ điều khiển logic mờ sẽ sử dụng hai thông số đặc trưng này như một đầu vào để tạo ra đầu ra, là giá trị phát hiện. Nếu giá trị phát hiện lớn hơn ngưỡng bảo mật được xác định trước, bộ điều khiển sẽ cảnh báo rằng một cuộc tấn công Sinkhole đang diễn ra trong khu vực. Trước khi tính toán giá trị phát hiện, các quy tắc mờ cần được thiết lập dựa theo những biểu hiện thường thấy ở các cuộc tấn công Sinkhole.

Nghiên cứu [56] xây dựng một cơ chế phát hiện xâm nhập cho mạng WSN bằng cách sử dụng hai thông số đặc trưng chính của luồng lưu lượng: tốc độ đến của gói tin và thời gian gói tin đến trong một khung thời gian và sau đó áp dụng suy luận mờ để quyết định xem liệu một cuộc tấn

công đã xảy ra hay chưa. Tuy nhiên, cơ chế này dựa trên Logic mờ, vì vậy nó cần các quy tắc được thiết lập trước quá trình phát hiện. Sự phụ thuộc vào thông tin trước đó khiến cho cơ chế này không thực tế đối với môi trường truyền nhận dữ liệu liên tục như WSN. Ngoài ra, nghiên cứu không chỉ ra những loại tấn công nhất định được phát hiện bởi cơ chế này.

### *C. Tiềm năng và hạn chế của phương pháp suy luận mờ đối với phát hiện xâm nhập trong mạng WSN*

**Ưu điểm của suy luận mờ:** Một số nghiên cứu sử dụng suy luận mờ trong mạng WSN được chứng minh là hiệu quả trong việc phát hiện xâm nhập cũng như phòng chống xâm nhập với độ phức tạp tính toán và năng lượng tiêu thụ ít hơn so với một số phương pháp khác.

Nghiên cứu trong [57] chỉ ra rằng áp dụng suy luận mờ có hiệu quả trong việc phát hiện các nút bị lỗi hoặc bị tấn công gây đọc sai thông tin. Kết quả thực nghiệm chứng minh rằng phương pháp này có thể phát hiện lỗi với độ chính xác cao hơn trong khi giảm độ phức tạp tính toán đáng kể so với các phương pháp khác. Nghiên cứu trong [58] đề xuất một mô hình suy luận mờ có khả năng phát hiện các cuộc tấn công làm rớt gói (Packet drop attack) hoặc cảnh báo sai do nhiều nguyên nhân không chắc chắn. Mô hình này được chứng minh phù hợp với các mạng WSN có tỷ lệ rớt gói cao với mật độ nút thấp.

Nghiên cứu trong [59] đề xuất một mô hình tin cậy đơn giản dựa trên Logic mờ để ngăn chặn xâm nhập trái phép trong mạng WSN. Mô hình này tính toán những giá trị cho mỗi tuyến và đảm bảo các bản tin được truyền đến các nút có giá trị tin cậy cao để tránh việc những nút độc hại đánh cắp gói tin. Các tác giả trong [60] còn chỉ ra rằng tiếp cận suy luận mờ có hiệu quả đối với việc phát hiện xâm nhập bởi 10 loại tấn công khác nhau như: nghe lén, gây mất đồng bộ, DoS, xung đột, phân tích lưu lượng, chuyển tiếp có chọn lọc, thao túng thông tin định tuyến, Sinkhole, Jamming, và giả mạo.

Nghiên cứu [61] đề xuất phương pháp thu thập dữ liệu ba pha dựa trên suy luận mờ. Thông qua các kết quả mô phỏng, phương pháp này được chứng minh giảm thiểu tỷ lệ mất gói do những cuộc tấn công đánh mất gói với năng lượng tiêu thụ ít hơn so với các phương pháp khác.

**Hạn chế của suy luận mờ:** Các nút cảm biến có những hạn chế nghiêm ngặt về nguồn cung và khả năng tính toán, chúng có thể được sử dụng để cảm biến liên tục, phát hiện các sự kiện, xác định sự kiện, cảm biến vị trí, … khiến cho quy tắc thiết lập cho suy luận mờ có thể yêu cầu một lượng bộ nhớ đáng kể. Số lượng các quy tắc tăng theo cấp số mũ theo số lượng các biến. Với $n$ biến, mỗi biến có thể nhận $m$ giá trị, số luật trong bộ quy tắc suy luận mờ là $m^n$. Vì các nút cảm biến có bộ nhớ hạn chế, việc lưu trữ bộ quy tắc đầy đủ trên mỗi nút có thể không hợp lý. Ngoài ra, duyệt liên tục bộ quy tắc có số lượng lớn có thể làm chậm đáng kể việc phát hiện xâm nhập hoặc ra quyết định. Để giải quyết vấn đề này, các tác giả của [62] đã thiết kế một số kỹ thuật làm giảm kích thước của bộ quy tắc như chia nhỏ bộ quy tắc, kết hợp quy tắc với các đầu ra tương tự, hoặc bộ quy tắc không đầy đủ. Đánh giá trong [62] đã chỉ ra rằng hai phương pháp giảm số lượng quy tắc cuối có thể giữ được độ chính xác và thời gian phát hiện sự kiện chỉ với 30% số lượng quy tắc được giữ lại. Các tác giả trong [63] cũng đã đề xuất một phương pháp giảm kích thước bộ quy tắc thông qua qua những thuật toán di truyền ghép mã nhị phân và thực (GAs). Sơ đồ thích nghi được chia thành hai giai đoạn: giai đoạn đầu liên quan đến việc tối ưu hóa các hàm thành viên thành viên và giai đoạn thứ hai được gọi là giai đoạn học và giảm quy tắc tự động cũng như xác định số lượng quy tắc tối thiểu cần thiết để xây dựng các mô hình mờ. Tuy nhiên, phương pháp này phù hợp với các hệ thống có bộ quy tắc lớn.

## IV. TỐI ƯU NĂNG LƯỢNG ĐỐI VỚI PHƯƠNG PHÁP PHÁT HIỆN BẤT THƯỜNG DỰA TRÊN LOGIC MỜ

### *A. Giảm kích thước của bộ quy tắc*

Như đã đề cập ở phần trên, kích thước của bộ quy tắc tăng theo cấp số mũ theo số lượng các biến. Trong một số trường hợp, nó tạo ra một vấn đề tính toán nghiêm trọng khi số lượng đầu vào cao. Những hệ thống mờ để xử lý số lượng lớn đầu vào cũng như số lượng lớn các quy tắc mờ có thể khó thiết kế do tiêu thụ bộ nhớ lớn, độ phức tạp tính toán cao và khả năng chuyển đổi kém trong điều chỉnh tham số.

Số lượng các quy tắc là một vấn đề quan trọng trong cơ sở quy tắc trong khi thiết kế một mô hình mờ. Ngoài mức độ không nhất quán của các cặp quy tắc, việc tìm kiếm các quy tắc thừa, không liên quan, sai hoặc thừa trong cơ sở quy tắc cũng có ý nghĩa. Động cơ đằng sau việc tìm kiếm này là rõ ràng, vì các quy tắc thừa không đóng góp vào hiệu suất của bộ điều khiển. Những quy tắc không liên quan, dư thừa, sai lầm và phức tạp trong cơ sở quy tắc làm nhiễu loạn hiệu suất của bộ điều khiển khi chúng cùng tồn tại. Do đó, điều hợp lý là giảm thiểu bộ quy tắc bằng cách loại bỏ những quy tắc không liên quan, sai lầm và dư thừa khỏi cơ sở quy tắc ban đầu và hợp nhất các quy tắc xung đột, đặc biệt là khi thực hiện các phép tính suy luận mờ trong thời gian thực.

Trong những năm gần đây, một số phương pháp đã được phát triển theo hướng tạo và đơn giản hóa mô hình mờ cũng như giảm kích thước cơ sở quy tắc trong các hệ mờ; hoặc tập trung vào việc lựa chọn những quy tắc quan trọng từ cơ sở quy tắc đóng góp vào cơ chế suy luận; hoặc loại bỏ những quy tắc thừa dựa trên một số tiêu chí hoặc sáp nhập các quy tắc có chung một số đặc điểm [62][63]. Mỗi phương pháp đều có ưu nhược điểm riêng. Tuy nhiên với trường hợp cụ thể của phương pháp phát hiện lưu lượng bất thường dựa trên suy luận mờ mà chúng tôi đã đề xuất ở công trình [2], với hai biến đầu vào là kỳ vọng $\mu$ và phương sai $\delta^2$ của dữ liệu cảm biến, chúng tôi lựa chọn kỹ thuật kết hợp quy tắc với các đầu ra tương tự [62] để giảm bộ quy tắc của hệ thống.

### *B. Kết hợp những quy tắc với các đầu ra tương tự*

Theo những kết quả tính toán ở công trình trước của chúng tôi, ta có bộ quy tắc gồm 9 luật với hai biến đầu vào là giá trị kỳ vọng $\mu$ và giá trị phương sai $\delta^2$ được trình bày ở bảng 2 [2].

*Bảng 2. Bộ quy tắc ban đầu*

| Quy tắc | μ | $\delta^2$ | Quyết định |
|---|---|---|---|
| 1 | Thấp | Nhỏ | Bất thường + |
| 2 | Thấp | Trung bình | Bất thường + |
| 3 | Thấp | Lớn | Bất thường - |
| 4 | Bình thường | Nhỏ | Nghi ngờ + |

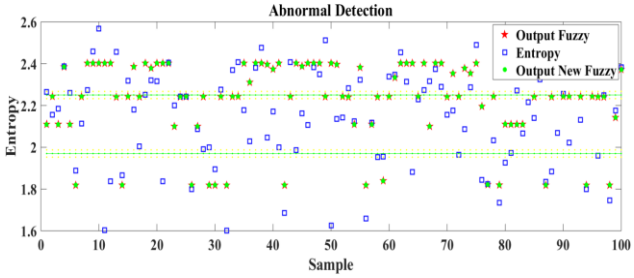
| | | | |
|---|---|---|---|
| 5 | Bình thường | Trung bình | Bình thường |
| 6 | Bình thường | Lớn | Nghi ngờ - |
| 7 | Cao | Nhỏ | Bất thường + |
| 8 | Cao | Trung bình | Nghi ngờ + |
| 9 | Cao | Lớn | Bất thường - |

Ta nhận thấy quy tắc 1 và 7 có cùng kết quả đầu ra là "Bất thường +" và chỉ khác nhau ở các giá trị kỳ vọng $\mu$. Quan sát này cũng phù hợp với quy tắc 3 và 9. Việc kết hợp các cặp quy tắc này có thể giúp chúng ta giảm thêm kích thước của cơ sở quy tắc. Đối với cơ sở quy tắc trong bảng 2, việc áp dụng tối ưu hóa này giúp chúng ta chỉ còn lại 7 quy tắc như bảng 3.

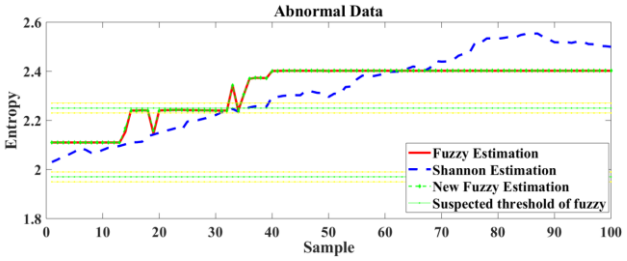
*Bảng 3. Bộ quy tắc sau khi rút gọn*

| Quy tắc | μ | $\delta^2$ | Quyết định |
|---|---|---|---|
| 1 | (Thấp) Or (Cao) | Nhỏ | Bất thường + |
| 2 | Thấp | Trung bình | Bất thường + |
| 3 | (Thấp) Or (Cao) | Lớn | Bất thường - |
| 4 | Bình thường | Nhỏ | Nghi ngờ + |
| 5 | Bình thường | Trung bình | Bình thường |
| 6 | Bình thường | Lớn | Nghi ngờ - |
| 7 | Cao | Trung bình | Nghi ngờ + |

Kết quả mô phỏng sử dụng theo tập dữ liệu tại [2], phương pháp suy luận mờ trước và sau khi thực hiện tối ưu đều cho ra cùng một kết quả như nhau về chỉ số cảnh báo và tỷ lệ phát hiện sai, được thể hiện như hình 2 và 3. Điều này cho thấy rằng với việc tối ưu này chúng ta có thể tiết kiệm được 22.2% năng lượng dành cho bộ nhớ để xử lý các quy tắc.




*Hình 2. Kết quả phát hiện bất thường*




*Hình 3. Tỷ lệ phát hiện bất thường dựa trên sắp xếp lại Entropy*

## 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. Tuy nhiên cũng cần quan tâm tới việc vừa nâng cao bảo mật vừa đảm bảo hiệu năng mạng. Trong bài báo này, chúng tôi trình bày một cách toàn diện về các hệ thống phát hiện xâm nhập và một số kỹ thuật để tối ưu năng lượng đối với phương pháp phát hiện lưu lượng bất thường dựa trên Logic mờ. Việc tối ưu năng lượng bằng cách áp dụng kỹ thuật giảm kích thước bộ quy tắc đã mang lại một số kết quả khả quan, chúng tôi đã tiết kiệm được năng lượng dành cho bộ nhớ xử lý nhưng vẫn giữ nguyên được kết quả so với ban đầu. Trong tương lai, mô hình sẽ được áp dụng cho các kịch bản thực tế trong các nghiên cứu tiếp theo của chúng tôi.

## TÀI LIỆU THAM KHẢO


[1] Hodge VJ, Justin J., "A survey of outlier detection methodologies", Artificial Intelligence Review 2004, 22(2), pp. 85-126, 2004.

[2] Van-Truong Nguyen, Trong-Minh Hoang, Tien-Xuyen Nguyen, Nhu-Lan Vu, "A new Anomaly Traffic Detection Based on Fuzzy Logic Approach in Wireless Sensor Networks", The 10th International Symposium on Information and Communication Technology (SoICT 2019).

[3] Hidoussi, Faouzi, Homero Toral-Cruz, Djallel Eddine Boubiche, Kamaljit Lakhtaria, Albena Mihovska, and Miroslav Voznak. Centralized IDS based on misuse detection for cluster-based wireless sensors networks. Wireless Personal Communications 85, no. 1: pp. 207-224, 2015.

[4] Kaplantzis, S., Shilton, A., Mani, N., & AhmetSekercioglu, Y., "Detecting selective forwarding attacks in wireless sensor networks using support vector machines", In Proceedings of the 3rd international conference on intelligent sensors, sensor networks and information, Melbourne, QLD, pp. 335-340, 2007.

[5] Hai, T. H., Huh, E. N., & Jo, M., "A lightweight intrusion detection framework for wireless sensor networks", Wireless Communications and Mobile Computing, pp. 559-572, 2010.

[6] Da Silva, Ana Paula R., Marcelo HT Martins, Bruno PS Rocha, Antonio AF Loureiro, Linnyer B. Ruiz, and Hao Chi Wong, "Decentralized intrusion detection in wireless sensor networks", In Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks, pp. 16-23, 2005.

[7] Chatzigiannakis, Ioannis, and Andreas Strikos, "A decentralized intrusion detection system for increasing security of wireless sensor networks", In 2007 IEEE Conference on Emerging Technologies and Factory Automation (EFTA 2007), IEEE, pp. 1408-1411, 2007.

[8] Bajaber, Fuad, and Irfan Awan, "Adaptive decentralized re-clustering protocol for wireless sensor networks", Journal of Computer and System Sciences 77, no. 2, pp. 282-292, 2011.

[9] Prabhu, SR Boselin, S. Sophia, P. D. Manivannan, and S. Nithya, "A research on decentralized clustering algorithms for dense wireless sensor networks", International Journal of Computer Applications 57, no. 20, 2012.

[10] Salmon, Helio Mendes, Claudio M. De Farias, Paula Loureiro, Luci Pirmez, Silvana Rossetto, Paulo Henrique de A. Rodrigues, Rodrigo Pirmez, Flávia C. Delicato, and Luiz Fernando R. da Costa Carmo, "Intrusion detection system for wireless sensor networks using danger theory immune-inspired techniques", International journal of wireless information networks 20, no. 1, pp. 39-66, 2013.

[11] Meng, Wei, Lihua Xie, and Wendong Xiao, "Decentralized TDOA sensor pairing in multihop wireless sensor networks", IEEE Signal Processing Letters 20, no. 2, pp. 181-184, 2013.

[12] Xie, Miao, Song Han, Biming Tian, and Sazia Parvin, "Anomaly detection in wireless sensor networks: A survey", Journal of Network and computer Applications 34, no. 4, pp. 1302-1325, 2011.

[13] Wazid M, Das AK, Kumari S, Khan MK, "Design of sinkhole node detection mechanism for hierarchical wireless sensor networks", Security and Communication Networks; 9(17), pp. 4596-4614, 2016.

[14] Wazid, Mohammad, and Ashok Kumar Das, "A secure group-based blackhole node detection scheme for hierarchical wireless sensor networks", Wireless Personal Communications 94, no. 3, pp. 1165-1191, 2017.

[15] Gerrigagoitia, Keldor, Roberto Uribeetxeberria, Urko Zurutuza, and Ignacio Arenaza, "Reputation-based intrusion detection system for wireless sensor networks", In 2012 Complexity in Engineering (COMPENG). Proceedings, IEEE, pp. 1-5, 2012.

[16] Chen, Haiguang, Huafeng Wu, Xi Zhou, and Chuanshan Gao, "Reputation-based trust in wireless sensor networks", In 2007 International Conference on Multimedia and Ubiquitous Engineering (MUE'07), IEEE, pp. 603-607, 2007.

[17] Ozdemir, Suat, "Functional reputation based reliable data aggregation and transmission for wireless sensor networks", Computer Communications 31, no. 17, pp. 3941-3953, 2008.

[18] Fang, Weidong, Chuanlei Zhang, Zhidong Shi, Qing Zhao, and Lianhai Shan, "BTRES: Beta-based Trust and Reputation Evaluation System for wireless sensor networks", Journal of Network and Computer Applications 59, pp. 88-94, 2016.

[19] Bao, Fenye, Ray Chen, MoonJeong Chang, and Jin-Hee Cho, "Trust-based intrusion detection in wireless sensor networks", In 2011 IEEE International Conference on Communications (ICC), pp. 1-6, 2011.

[20] Misra, Sudip, and Ankur Vaish, "Reputation-based role assignment for role-based access control in wireless sensor networks", Computer Communications 34, no. 3, pp. 281-294, 2011.

[21] C. Wang, T. Feng, J. Kim, G. Wang, and W. Zhang, "Catching packet droppers and modifers in wireless sensor networks," in Proceedings of the 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON '09), pp. 1-9, 2009.

[22] Ozcelik, Mert Melih, Erdal Irmak, and Suat Ozdemir, "A hybrid trust based intrusion detection system for wireless sensor networks", In 2017 International Symposium on Networks, Computers and Communications (ISNCC), pp. 1-6. IEEE, 2017.

[23] D. E. Boubiche and A. Bilami, "Cross layer intrusion detection system for wireless sensor network", International Journal of Network Security & Its Applications, vol. 4, no. 2, p. 35, 2012.

[24] Gandhimathi, L., and G. Murugaboopathi, "Cross layer intrusion detection and prevention of multiple attacks in Wireless Sensor Network using Mobile agent", In 2016 International Conference on Information Communication and Embedded Systems (ICICES), IEEE, pp. 1-5, 2016.

[25] A. Agah, S. K. Das, K. Basu, and M. Asadi, "Intrusion detection in sensor networks: a non-cooperative game approach," In Proceedings of the 3rd IEEE International Symposium on Network Computing and Applications (NCA '04), pp. 343–346, 2004.

[26] A. Agah and S. K. Das, "Preventing DoS attacks in wireless sensor networks: a repeated game theory approach", International Journal of Network Security, vol. 5, no. 2, pp. 145–153, 2007.

[27] Subba, Basant, Santosh Biswas, and Sushanta Karmakar, "A game theory based multi layered intrusion detection framework for wireless sensor networks", International Journal of Wireless Information Networks 25, no. 4, pp. 399-421, 2018.

[28] Abdalzaher, Mohamed S., Karim Seddik, and Osamu Muta, "Using repeated game for maximizing high priority data trustworthiness in wireless sensor networks", In 2017 IEEE Symposium on Computers and Communications (ISCC), pp. 552-557, 2017.

[29] S. Shamshirband, A. Patel, N. B. Anuar, M. L. M. Kiah, and A. Abraham, "Cooperative game theoretic approach using fuzzy Q-learning for detecting and preventing intrusions in wireless sensor networks", Engineering Applications of Artifcial Intelligence, vol. 32, pp. 228-241, 2014.

[30] Shen, Shigen, Guangxue Yue, Qiying Cao, and Fei Yu, "A survey of game theory in wireless sensor networks security", Journal of Networks 6, no. 3, 2011.

[31] A. Agah, S. K. Das, and K. Basu, "A game theory based approach for security in wireless sensor networks," Proc. IEEE International Conference on Performance, Computing, and Communications, pp. 259-263, 2004.

[32] L. Yang, D. Mu, and X. Cai, "Preventing dropping packets attack in sensor networks: A game theory approach", Wuhan University Journal of Natural Sciences, vol. 13, pp. 631-635, 2008.

[33] T. Alpcan and T. Basar, "An intrusion detection game with limited observations", 12th International Symposiun On Dynamic Games and Applications, 2006.

[34] A. Agah, K. Basu, and S. K. Das, "Security enforcement in Wireless Sensor Networks: A framework based on noncooperative games", Pervasive and Mobile Computing, vol. 2, Apr. 2006, pp. 137-158.

[35] X. Li and M. R. Lyu, "A novel coalitional game model for security issues in wireless networks," Proc. IEEE Global Telecommunications Conference (GLOBECOM 2008) pp. 1-6, 2008.

[36] E. C. Ngai, J. Liu, and M. R. Lyu, "On the intruder detection for sinkhole attack in wireless sensor networks", in Proceedings of the IEEE International Conference on Communications (ICC '06), vol. 8, pp. 3383-3389, 2006.

[37] S. S. Doumit and D. P. Agrawal, "Self-organized criticality & stochastic learning based intrusion detection system for wireless sensor networks", In Proceedings of the IEEE Military Communications Conference (MILCOM '03), vol. 1, pp. 609-614, 2003.

[38] I. Onat and A. Miri, "A real-time node-based trafc anomaly detection algorithm for wireless sensor networks," in Proceedings of the International Conference on Systems Communications, IEEE Computer, pp. 422-427, 2005.

[39] I. Onat and A. Miri, "An intrusion detection system for wireless sensor networks", In Proceedings of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob '05), vol. 3, pp. 253-259, 2005.

[40] A. Abraham, C. Grosan, and C. Martin-Vide, "Evolutionary design of intrusion detection programs", International Journal of Network Security, vol. 4, no. 3, pp. 328-339, 2007.

[41] A. Abraham, R. Jain, J. Tomas, and S. Y. Han, "D-SCIDS: distributed sof computing intrusion detection system", Journal of Network and Computer Applications, vol. 30, no. 1, pp. 81-98, 2007.

[42] Azmoodeh, A., Dehghantanha, A., Choo, K.K.R, "Robust Malware Detection for Internet of (Battlefield) Things Devices Using Deep Eigenspace Learning", IEEE Trans. Sustain. Comput. 2018, 4, pp. 88-95, 2018.

[43] Doshi, R.; Apthorpe, N.; Feamster, N., "Machine Learning DDoS Detection for Consumer Internet of Things Devices", In Proceedings of the IEEE Security and Privacy Workshops (SPW), San Francisco, CA, USA, pp. 29-35, 2018.

[44] Amouri, Amar, Vishwa T. Alaparthy, and Salvatore D. Morgera, "A Machine Learning Based Intrusion Detection System for Mobile Internet of Things", Sensors 20, no. 2, 2020.

[45] Thamilarasu, G.; Chawla, S., "Towards Deep-Learning-Driven Intrusion Detection for the Internet of Things", Sensors 2019.

[46] Otoum, Safa, Burak Kantarci, and Hussein T. Mouftah., "On the feasibility of deep learning in sensor network intrusion detection", IEEE Networking Letters 1, no. 2, pp. 68-71, 2019.

[47] K. Kapitanova et al., "Using fuzzy logic for robust event detection in wireless sensor networks", Ad Hoc Networks 2011.

[48] H.J. Zimmermann, "Fuzzy set theory and its applications", Third Edition, Kluwer Academic Publishers, 1996.

[49] M. Maksimovic., "Fuzzy logic and Wireless Sensor Networks – A survey", Journal of Intelligent and Fuzzy Systems, vol. 27, pp. 877-890, 2014.

[50] A. H. Hamamoto, L. F. Carvalho, L. D. H. Sampaio, T. Abrão, and M. L. Proença., "Network Anomaly Detection System using Genetic Algorithm and Fuzzy Logic", Expert System Application, vol. 92, 390-402, 2018.

[51] K. Angrishi et al., "Fuzzy Based Detection and Prediction of DDoS Attacks in IEEE 802.15.4 Low Rate Wireless Personal Area Network", IEEE Network, 24(2), pp. 943-983, 2013.

[52] Falsafain, S. M. Taheri, and M. Mashinchi., "Fuzzy Estimation of Parameters in Statistical Models", International Journal of Computing Science and Mathematics, 2(2), pp. 7-85, 2008.

[53] S. N. Shiaeles, V. Katos, A. S. Karakos, and B. K. Papadopoulos., "Real time DDoS detection using fuzzy estimators", Computer Security, 31(6), pp. 782-790, 2012.

[54] Chi, S.H. and T.H. Cho, "Fuzzy Logic Anomaly Detection Scheme for Directed Diffusion Based Sensor Networks", Proceedings of the 3rd International Conference on Fuzzy Systems and Knowledge Discovery, (FSKD' 26), Springer- Verlag Berlin, Heidelberg, pp: 725-734, 2006.

[55] Moon, S.Y. and T.H. Cho, "Intrusion detection scheme against sinkhole attacks in directed diffusion based sensor networks", Int. J. Comput. Sci. Netw. Security, 9, pp. 118-122, 2009.

[56] Ponomarchuk, Y.A. and Seo D.W., "Intrusion detection based on traffic analysis and fuzzy inference system in wireless sensor networks", J. Convergence, 1, pp. 35-42, 2010.

[57] A. Barati, S.J. Dastgheib, A. Movaghar and I. Attarzadeh, "An effective fuzzy based algorithm to detect faulty readings in long thin wireless sensor networks", International Journal on Technical and Physical problems of Engineering – IJTPE, Issue 10 4(1), pp. 52-58, 2012.

[58] H. Malazi, K. Zamanifar and S. Dulman, FED, "Fuzzy Event Detection model for Wireless Sensor Networks", International Journal of Wireless & Mobile Networks (IJWMN), 2011.

[59] T.K. Kim and H.S. Seo, "A trust model using fuzzy logic in Wireless Sensor Network", Proceedings of world academy of science, engineering and technology 32 (2008).

[60] M. Malik, E. Naryan and A. Preet Singh, "Rule based technique detecting Security attack for Wireless Sensor network using fuzzy logic", International Journal of Advanced Research in Computer Engineering & Technology 1(4) (2012).

[61] D. HevinRajesh and B. Paramasivan, "Fuzzy based secure data aggregation technique in Wireless Sensor Networks", Journal of Computer Science 8(6), pp. 899-907, 2012.

[62] K. Kapitanova et al., "Using fuzzy logic for robust event detection in wireless sensor networks", Ad Hoc Netw 2011.

[63] Pintu Chandra Shill, M. A. H. Akhand, MD. Asaduzzaman and Kazuyuki Murase, "Optimization of Fuzzy Logic Controllers with Rule Base Size Reduction using Genetic Algorithms", International Journal of Information Technology & Decision Making, Vol. 14, 2015.

## INTRUSION DETECTION SYSTEM AND ENERGY OPTIMIZATION FOR AN ANOMALY TRAFFIC DETECTION BASED ON FUZZY LOGIC APPROACH IN WIRELESS SENSOR NETWORK

***Abstract:*** Wireless sensor network (WSN) is one of the promising technologies with an extremely diverse range of applications, from healthcare to military. And as the WSN becomes more and more common, security threats are also increasingly diversified and intentional. Prevention-based security approaches such as cryptography, authentication, and key management have been used to protect WSNs from various types of attacks, but these approaches are not sufficient to protect the network from internal attacks which can extract sensitive information. As a result, the intrusion detection system (IDS) turns into the second most important layer of defense to protect and keep the network safe from the malicious attacks. Anomaly detection is one of the typical intrusion protection methods, in which the abnormal flow current method based on fuzzy inference has been studied previously and has yielded some good results. However, it also faces some typical challenges such as the number of input variables increases, so processing power also increases, which affects network performance. Therefore, in this paper, we present a comprehensive view of intrusion detection systems and use several techniques for energy optimization to anomaly traffic detection method based on Fuzzy Logic approach. Simulation results and comparative analysis prove that after being optimized, our method can still retain accuracy for warning index and false detection rate while consuming less memory power to process compared with the original.

***Keywords:*** Wireless Sensor Network (WSN), IoT, Security, Fuzzy Inference, Intrusion Detection.

**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.

**Email: nvtruong.dhkh@gmail.com**

**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.

**Email: anhdt.hue@gmail.com**

**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.

**Email: synq@ptit.edu.vn**