MỘT LƯỢC ĐỒ BẢO MẬT NHẸ ĐỂ CUNG CẤP CƠ CHẾ NHẬN THỰC NÚT MẠNG CẢM BIẾN KHÔNG DÂY WSN

A LIGHT WEIGHT SECURE SCHEME TO PROVIDE NODE AUTHENTIFICATION IN WIRELESS SENSOR NETWORKS

Bùi Văn Hậu[1], Châu Thanh Phương[1], Hoàng Trọng Minh[2], Đinh Thị Hằng[3], Phạm Ngọc Sâm[3]

[1]Khoa Điện tử, Trường Đại học Kinh tế - Kỹ thuật Công nghiệp

[2]Khoa Viễn thông, Học Viện Công nghệ bưu chính viễn Thông

[3]Khoa Điện, Trường Đại học Kinh tế - Kỹ thuật Công nghiệp

Đến Tòa soạn ngày 02/7/2019, chấp nhận đăng ngày 22/7/2019

Tóm tắt: Vấn đề bảo mật trong mạng cảm biến không dây (WSNs) đã và đang trở thành tâm điểm trong những năm gần đây cùng với các giải pháp internet vạn vật tăng mạnh. Trong kỹ thuật bảo mật, kỹ thuật thùy vân (watermark) là một cách tiếp cận hứa hẹn để xác thực và quản lý các thực thể trong mạng cảm biến không dây do tính phổ biến và đơn giản. Trong bài báo này, chúng tôi đề xuất một lược đồ sử dụng watermark để chống lại việc giả mạo hoặc nhân bản nút mạng, đồng thời cung cấp cách bảo vệ dữ liệu nhạy cảm trong mạng cảm biến không dây. Dựa trên tiếp cận sử dụng watermark động, lược đồ đề xuất được phân tích an ninh để chứng minh năng lực bảo mật mạnh mẽ và dễ dàng kết hợp với giao thức định tuyến thực tế. Thêm vào đó, các kết quả minh chứng ưu điểm của đề xuất được được mô phỏng bằng bộ công cụ mô phỏng số.

Từ khóa: Mạng cảm biến không dây, bảo mật, watermark, nhận thực.

Abstract: Security in wireless sensor networks (WSNs) in the Internet of Things era has been become enormously attracted to research in recent years. To reach security aims, the watermarking technique is a promising approach to authenticate and manage the entities of wireless sensor networks due to its popular use and lightweight. In this paper, a novel watermarking scheme is proposed against fake or clone node ID (IDentification) attacks and provide protection for classified data simultaneously. Based on a dynamic watermark approach, the proposed scheme can bring robust security and easily incorporate with a practical routing protocol that proves through security analysis. Moreover, performances of the scheme are validated by numerical results.

Keywords: Wireless sensor networks, security, watermarking technique, authentication.

1. GIỚI THIỆU

Mạng cảm biến không dây (WSNs) đóng vai trò là một trong những công nghệ hạ tầng chính yếu trong kỷ nguyên Internet vạn vật (IoT). Mạng này có thể được coi là cơ sở hạ tầng truyền thông để kết nối thế giới mạng với các trung tâm xử lý dữ liệu thông minh. WSNs thường được triển khai trong các môi trường không kiểm soát bởi con người và đôi khi ngay cả trong các môi trường thù địch để cung cấp một loạt các ứng dụng với các yêu cầu khác nhau. Bên cạnh lợi thế có được, các WSNs phải đối mặt với rất nhiều thách thức liên quan đến hiệu suất mạng hoặc các vấn đề bảo mật, bị tấn công đến từ cả bên trong lẫn bên ngoài. Do đó, vấn đề bảo mật trong WSNs thu hút được rất nhiều công trình nghiên cứu trong những năm gần đây.

Trong các mạng cảm biến không dây điển hình, các nút trong WSNs có các ràng buộc

tài nguyên chặt chẽ do thiếu khả năng xử lý, bộ nhớ và năng lượng hạn chế. Thật không may, các cơ chế bảo mật truyền thống có chi phí hoạt động cao là không khả thi đối với các nút cảm biến bị hạn chế tài nguyên. Do đó, một sơ đồ bảo mật nhẹ là cách tiếp cận có lợi nhất để chống lại các cuộc tấn công trong WSNs trong khi vẫn tiết kiệm năng lượng. Theo cách tiếp cận này, các kỹ thuật watermark đang được coi là một cách tiếp cận hiệu quả để cung cấp một số mức độ bảo mật như phát hiện giả mạo, xác thực sở hữu dữ liệu và nội dung dữ liệu. Để bảo mật các dữ liệu nhận được, kỹ thuật watermark có thể được sử dụng để xác thực hoặc bảo vệ luồng dữ liệu và dữ liệu. Mặt khác, chúng có thể được sử dụng để xác thực ID (Identification) nút hoặc phát hiện các cuộc tấn công ID nút nhân bản [1].

Tuy nhiên, một sơ đồ bảo mật nhẹ dựa trên kỹ thuật watermark để đảm bảo an toàn cả dữ liệu và xác thực ID nút không được xem xét đầy đủ trong các đề xuất trước đây. Do đó, trong nghiên cứu này, chúng tôi đề xuất một sơ đồ watermark mới để chống lại cả giả mạo tấn công ID nút và đảm bảo tính toàn vẹn dữ liệu trong các mạng cảm biến không dây. Hơn nữa, kế hoạch được chúng tôi đề xuất có thể kết hợp với hệ thống phân tích thích ứng năng lượng thấp LEACH (Low-Energy Adaptive Clustering Hierarchy) để xác nhận các khía cạnh tiêu thụ năng lượng [2].

Để chống lại một cuộc tấn công nhân bản nút, các phương pháp dựa trên kỹ thuật watermark đã được đề xuất. Nhận dạng nút có thể được xác minh bằng các lược đồ dựa trên vị trí, phân phối trước khóa, phương thức trao đổi khóa, phương thức mã hóa và các phương thức nhận dạng duy nhất có thể kiểm chứng. Ngoài ra, để giảm mức tiêu thụ năng lượng của quá trình phát hiện bản sao nút, sơ đồ watermark trong [6] dựa trên khoảng thời gian lấy mẫu và được nhúng vào nhóm dữ liệu có kích thước cố định. Tuy nhiên, đề xuất này hạn chế các hành động thu thập dữ liệu do tần suất lấy mẫu cố định và nhóm dữ liệu có quy mô cố định đồng thời không liên quan đến các vấn đề bảo mật dữ liệu thu được. Hơn nữa, sơ đồ này không xem xét việc kết hợp với một giao thức định tuyến thực tế trong các mạng cảm biến không dây.

Trong các giao thức định tuyến trong mạng cảm biến không dây, giao thức phân cấp phân cụm thích ứng năng lượng thấp (LEACH) vẫn đang thu hút sự chú ý của cộng đồng nghiên cứu và nhà phát triển do lợi thế của việc tiêu thụ năng lượng. Một số giao thức LEACH khác nhau đã được đề xuất trong những năm gần đây. LEACH xem xét không chỉ các vấn đề năng lượng mà còn các vấn đề khác như liên quan đến an ninh. Giao thức Sec LEACH trong [3-4] cung cấp tính xác thực, toàn vẹn, bảo mật và làm mới cho các giao tiếp đầu nút đến cụm thông qua sơ đồ phân phối khóa ngẫu nhiên. MS-LEACH trong [5] cung cấp cả bảo mật dữ liệu và xác thực nút nguồn cho các nút cảm biến, nút đầu cụm bằng các cặp khóa. Tuy nhiên, sơ đồ phân phối khóa luôn là một vấn đề khó khăn trong môi trường hoạt động năng động. Hơn nữa, các phương pháp này đòi hỏi nhiều tiêu thụ năng lượng hơn để trao đổi khóa riêng.

Mặt khác, để đảm bảo tính toàn vẹn của dữ liệu thu được, các tác giả trong [6] đã đề xuất phương pháp watermarking-LEACH. Sơ đồ watermark này dựa trên chức năng phân tách dữ liệu thu được để đạt được hiệu quả năng lượng trong khi chống lại sự giả mạo dữ liệu. Các tác giả trong [7] đề xuất một lược đồ watermark có thể đảo ngược để xác thực dữ liệu thu được trong các mạng cảm biến không dây. Thông tin watermark được tạo bởi một khóa bí mật và thông tin thời gian của nó nên các bit được watermark thể hiện các giá trị

phân tách của dữ liệu thu được. Do đó, độ chính xác của sơ đồ này phụ thuộc vào việc xác định thời gian trên nút cảm biến và mẫu lưu lượng. Tất cả các đề xuất kể trên không xem xét tới vấn đề tấn công nhân bản nút (Clone), được bắt đầu từ vấn đề tấn công của nút có nguồn gốc giả mạo, trong mạng cảm biến không dây.

I. Kamel and H. Juma [8] cũng đề xuất một lược đồ bảo mật nhẹ dựa trên kỹ thuật watermark với hàm bảo mật HASH. Phương pháp này có ưu điểm là tiết kiệm năng lượng nhưng hàm bảo mật là cố định. Hệ thống sẽ bị tấn công nếu hàm này bị phát hiện.

Trong bài báo này, chúng tôi đề xuất một sơ đồ watermark mới để xác thực ID nút nhằm chống lại cuộc tấn công ID nút nhân bản trong các mạng cảm biến không dây. ID nút được ẩn bằng kỹ thuật watertermark đơn giản, động tại nút cảm biến. Sơ đồ cấu hình nhẹ này có thể dễ dàng tích hợp vào LEACH để nâng cao hiệu suất bảo mật mạng.

Bài viết này được tổ chức như dưới đây. Phần II minh họa về sơ đồ mã hóa, giải mã được chúng tôi đề xuất kèm theo các thuật toán chi tiết. Trong phần III, sơ đồ đề xuất của chúng tôi được phân tích về các khía cạnh bảo mật và đánh giá hiệu quả năng lượng bằng các kết quả mô phỏng. Các kết luận chính và các công trình trong tương lai được trình bày trong phần IV.

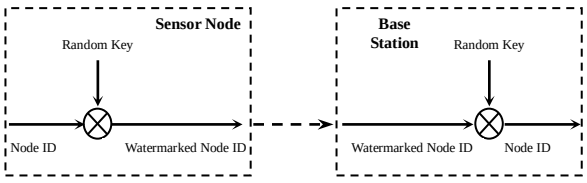
2. MÔ HÌNH WATERMARK ĐỀ XUẤT

Hãy xem xét một mạng cảm biến không dây được hình thành như kiến trúc mạng phân cấp điển hình. Trong đó, một số nút cảm biến được phân nhóm thành cụm và được bình chọn cho đầu cụm CH (Cluster Head). CH thu thập dữ liệu thu được sau đó chuyển tiếp chúng đến trung tâm xử lý dữ liệu được gọi là trạm gốc (Base Station). Phương thức giao tiếp truyền thông này mang lại hiệu quả sử dụng năng lượng tốt, trong đó giao thức LEACH là công cụ tiên phong trong WSNs [3]. Dựa trên qui trình hoạt động này của mạng, quá trình xử lý watermark chi tiết được trình bày dưới đây.

Trong pha ban đầu, mọi nút cảm biến được gán một ID nút gốc mà BS đã biết. ID nút ban đầu được ẩn bởi phương pháp watermark nút ID động được chúng tôi đề xuất tại một nút cảm biến theo một thuật toán đơn giản. Hơn nữa, phương pháp watermark này chứa những đặc điểm chính của dữ liệu cảm nhận được có nguồn gốc từ nút cảm biến. Nút BS xác minh ID nút và dữ liệu được cảm nhận đuộc để phát hiện các sự cố bất thường nếu xảy ra.

2.1. Sơ đồ watermark ID nút động

ID nút đóng vai trò quan trọng trong vấn đề bảo mật WSN để bảo vệ các nút mạng khỏi các cuộc tấn công dễ bị tổn thương tới nút như tấn công ID nút nhân bản hoặc tấn công ID nút giả. Trong trường hợp bình thường, ID nút là duy nhất và chỉ được nhận biết bởi BS. Kẻ tấn công có thể khai thác ID nút để với mục đích xấu. Do đó, một ID nút cần được ẩn cho mọi người trừ trạm gốc. Sơ đồ khối của phương pháp watermark ID nút động được minh họa trong hình 1. ID nút ban đầu được mã hóa bởi phương pháp watermark ID nút động sau đó nó được gửi đến BS thông qua CH của nút sau khi đã được phân. BS sẽ giải mã ra ID của nút gốc thông qua một quá trình đảo ngược.



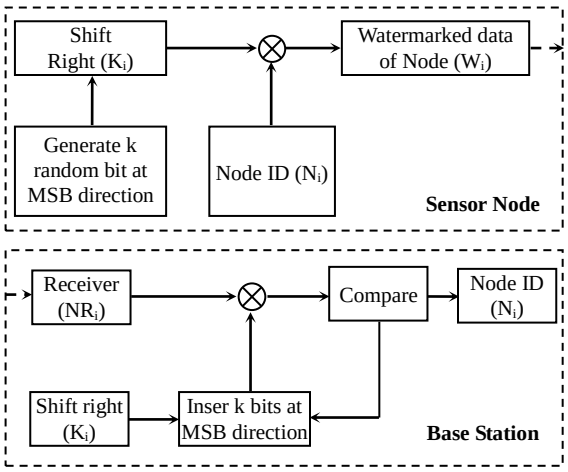
Hình 1. Sơ đồ nguyên lý watermark và giải watermark động

Giả sử rằng chúng ta có N nút cảm biến trong một khoảng không gian và được xác thực ID gốc. Mỗi nút cảm biến thứ i có một giá trị nhận dạng duy nhất (N_i). Tổng chiều dài bit

của ID nút là 28 bit nếu sử dụng xác thực địa chỉ MAC. Để watermark, ta sử dụng một chuỗi gồm 28 bít được chọn ngẫu nhiên làm khóa watermark, K_i ($i=1\rightarrow N$). Chúng tôi lựa chọn k ($k=1\rightarrow N$) bít bằng cách cách dịch phải K_i k lần và chèn k bít ngẫu nhiên vào phía ngoài cùng bên trái của K_i để tạo nên 28 bít ngẫu nhiên K_{ij} (đây là khóa bí mật của nút mạng thứ i tại vị trí bít thứ j). Dữ liệu sau khi watermark của N_i là W_i được tính như sau

$$W_i = \bigcup_{j=28}^{1} N_{ij} \otimes K_{ij} \quad (1)$$

Trong đó $\bigcup_{j=28}^{1}(.)$ là ký hiệu của phép hợp 28 bít riêng lẻ thành một giá trị nhị phân 28 bít. $\otimes$ là ký hiệu của phép XOR (Exclusive OR). N_{ij} là ID nút của nút N_i tại vị trí bít thứ j. ID của một nút có 28 bít, nếu ta coi 28 bít này là một số nhị phân thì sẽ hình thành một số gọi là giá trị của ID nút. W_i là ID của nút thứ i sau khi watermark. Sơ đồ khối của thuật toán mã hóa watermark và giải mã watermark được đề xuất được miêu tả chi tiết trong hình 2.



Hình 2. Sơ đồ khối của thuật toán watermark và giải watermark động

Giả sử giao thức LEACH được vận hành trong mạng cảm biến không dây được kiểm tra. Trước khi hình thành các cụm, khóa đầu tiên K_0 được cả nút cảm biến (SN-Sensor Node) và BS biết do chúng ta có thể giả sử pha ban đầu là an toàn. Nút BS chứa một bộ cơ sở dữ liệu ID nút gốc. Tại mỗi vòng của hoạt động phân cụm, khóa watermark K_{ij} được thay đổi động k bít tại SN. Do đó, nút BS thực hiện các thuật toán giải mã k bít để cập nhật khóa giải mã $\hat{K}_{ij}$ nhận được trong khi so sánh ID nút nhận được với ID nút gốc được lưu trữ trong cơ sở dữ liệu của BS. ID nút nhận được được giải mã theo công thức sau

$$\hat{N}_{ij} = \bigcup_{j=1}^{28} WR_{ij} \otimes \hat{K}_{ij} \quad (2)$$

Trong đó WR_{ij} là dữ liệu đã được watermark của ID nút N_i. $\hat{K}_{ij}$ là khóa watermark ngẫu nhiên K_i đã được dịch phải k bít và chèn một khả năng của k bít ngẫu nhiên trong 2^k khả năng vào phía ngoài cùng bên trái của K_{ij} hiện tại. Nếu ID nút được giải mã $\hat{N}_{ij}$ trùng với ID nút N_i có nghĩa là chúng ta đã thực hiện giải watermark thành công và $\hat{K}_{ij}$ chính là khóa bí mật K_{ij} hiện tại mà ta cần tìm. Thuật toán watermark động và giải watermark sẽ được giới thiệu sau đây.

Thuật toán 1: Watermark ID nút động

1:**function** Node ID Watermark Generation

2: Vào: N_i, K_i

3: Ra: W_i, K_i

4: Dịch phải K_i k bít

5: Chèn k bít ngẫu nhiên vào K_i để tạo khóa watermark ngẫu nhiên K_{ij}

6: $W_i = \bigcup_{j=28}^{1} N_{ij} \otimes K_{ij}$

7: $K_i = K_{ij}$

8: Return W_i, K_i

9: **end function**

Thuật toán 2: Giải Watermark ID nút

1: **function** Node ID Watermark Extraction

2: Vào: NR_{ij}, K_i

3: Ra: N_i, K_i

4: $\hat{N}_{\text{ij}} = 0$

5: Phát ra mọi khả năng của *k* bít ngẫu nhiên

6: Dịch phải K_i *k* bít

7: While $\hat{N}_{\text{ij}} \neq N_i$

8: Chèn một khả năng của *k* bít ngẫu nhiên vào K_i để tạo khóa ngẫu nhiên $\hat{K}_{\text{ij}}$.

9: $\hat{N}_{ij} = \bigcup_{j=28}^{1} NR_{ij} \otimes \hat{K}_{\text{ij}}$

10: end while

11: $N_i = \hat{N}_{\text{ij}}$

12: $K_i = \hat{K}_{\text{ij}}$

13: return N_i, K_i

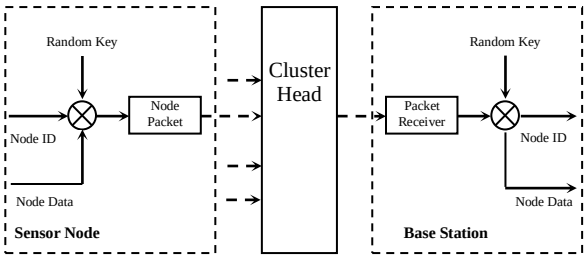
14: **end function**

Như sơ đồ mô tả, nút BS đã biết dữ liệu nào thuộc về nút nào khi nhận được dữ liệu đã watermark. Mặt khác, nút BS giữ trong cơ sở dữ liệu của nó khóa ngẫu nhiên trước đó của nút N_i. Do đó, nút BS luôn có thể giải mã ID nút đã được watermark thành công. Khóa watermark ngẫu nhiên của mỗi nút được thay đổi mỗi phiên truyền nhận dữ liệu, thuộc tính này làm cho hệ thống vận hành an toàn và hiệu quả.

Với sơ đồ watermark và giải watermark được chúng tôi đề xuất, sau 28/*k* vòng truyền dữ liệu, mọi nút cảm biến đều có 28 bít watermark hoàn toàn ngẫu nhiên. Khóa ngẫu nhiên này là không thể dự đoán được trong một thời gian ngắn bởi những kẻ tấn công, do vậy sẽ giữ cho hệ thống của chúng ta an toàn trước các cuộc tấn công.

2.2. Bảo vệ dữ liệu

Để tăng cường bảo mật dữ liệu mà các nút cảm biến thu nhận được chúng tôi đề xuất một sơ đồ watermark các dữ liệu này trong mạng cảm biến thực tế.



Hình 3. Sơ đồ khối thuật toán bảo vệ dữ liệu trong WSNs

Như chúng ta đã biết, hệ thống WSN ban đầu không sử dụng bất kỳ cơ chế bảo mật nào trong giai đoạn phân cụm. Đây là một lỗ hổng lớn để kẻ tấn công tạo ra các nút cảm biến giả và vi phạm tính toàn vẹn dữ liệu. Do đó, chúng tôi đề xuất một phương pháp để watermark cả ID nút và dữ liệu được cảm biến cảm nhận được của nút bằng thuật toán watermarking động. Sơ đồ khối của phương pháp đề xuất được trình bày trong hình 3.

Thuật toán 3: Watermark dữ liệu nút

1: **function** Watermark Node Data

2: Vào: D_i, N_i, K_i

3: Ra: PW_i

4: Dịch phải K_i k bít

5. Chèn k bít ngẫu nhiên vào K_i để tạo nên khóa watermark ngẫu nhiên K_{ij}

6: $P_i = D_i \square N_i$

7: $PW_i = P_i \otimes K_{\text{ij}}$

8: $K_i = K_{\text{ij}}$

return PW_i, K_i

10: **end function**

Trong đó D_i là dữ liệu thu nhận được, N_i là ID nút, K_i là khóa watermark ngẫu nhiên của nút cảm biến thứ i. Khóa ngẫu nhiên được dịch phải k bít như kịch bản của thuật toán một. Dữ liệu và ID của nút là duy nhất để tạo nên gói dữ liệu của nút là P_i và được

watermark và phát tới BS.

BS nhận được gói của nút dưới dạng PR_i và thực hiện phép toán XOR với khóa bí mật để tìm ra khóa watermark ngẫu nhiên ở phía phát. Từ khóa bí mật này chúng ta thực hiện giải mã để nhận được ID và dữ liệu của nút cảm biến thứ *i*. Khóa bí mật ngẫu nhiên của từng nút được cập nhật sau mỗi vòng truyền dẫn như được thể hiện trong thuật toán 4.

Thuật toán 4: Giải watermark dữ liệu nút

1: **function** Node Data Extraction

2: Vào: PR_i, K_i PR_i, K_i

3: Ra: N_i, D_i

4: $\hat{N}_{ij} = 0$

5: Dịch phải K_i k bít

6: Tách NR_i, DR_i từ PR_i

7: While $\hat{N}_{ij} \neq N_i$

8: Chèn k bít ngẫu nhiên vào K_i để tạo khóa ngẫu nhiên $\hat{K}_{ij}$

9: $\hat{N}_{ij} = \bigcup_{j=1}^{28} NR_{ij} \otimes \hat{K}_{ij}$

10: end while

11: $N_i = \hat{N}_{ij}$

12: $K_i = \hat{K}_{ij}$

13: $D_i = DR_i \otimes K_i$

return N_i, D_i

end function

Trong thuật toán trên, BS nhận được PR_i (được phát ở SN là PW_i) đồng thời đã biết K_i . NR_i và DR_i được tách ra từ PR_i theo cách ngược lại với tại SN. Tại thời điểm này chúng ta không biết chính xác là k bít nào đã được chèn vào K_i ở SN. Chúng ta cần thử tất cả các khả năng của k bít tại BS để tìm ra khóa bí mật. Nếu $\hat{N}_{ij} = N_i$ có nghĩa là chúng ta đã tìm ra giá trị chính xác của $\hat{K}_{ij}$, đây là chìa khóa để giải watermark dữ liệu tại nút cảm biến.

3. MÔ PHỎNG VÀ KẾT QUẢ

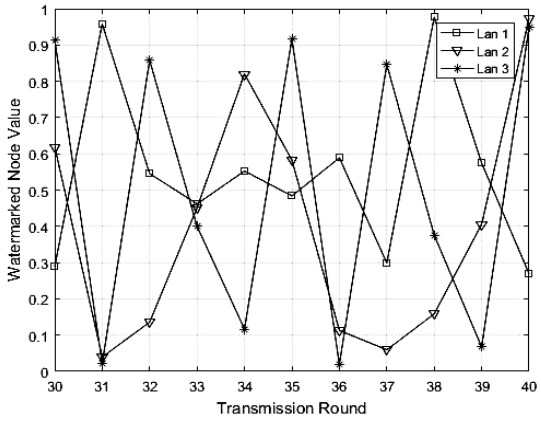
Để chống lại việc giả mạo hoặc clone ID nút mạng trong WSNs chúng tôi đã sử dụng một khóa động để watermark ID nút cũng như dữ liệu của nút đó. Trong trường hợp muốn tấn công mạng cảm biến này, kẻ tấn công sẽ phải tìm ra ID gốc của nút cảm biến nhưng khó hơn là phải tìm ra mã ngẫu nhiên 28 bít động. Với mã ngẫu nhiên 28 bít này ta có 2^{28} khả năng và không thể tìm ra trong một khoảng thời gian ngắn. Hơn nữa nếu tìm được khóa ngẫu nhiên này thì nội dung của khóa đã được thay đổi theo mỗi phiên truyền dẫn (động) và không thể tìm ra ngay cả với chúng tôi.

Trong phần này chúng tôi sẽ khảo sát sơ đồ watermark và giải watermark động thông qua một số thí nghiệm mô phỏng.

Chúng tôi tạo ra một cụm các cảm biến không dây trong một mạng WSNs. Mạng WSNs thử nghiệm chứa mười sáu cảm biến không dây. Chúng tôi lựa chọn giá trị này theo một quy luật trong ngành điện tử thường lựa chọn giá trị 2^n. Hơn nữa, trong thí nghiệm mô phỏng LEACH sử dụng 100 nút cảm biến trong bán kính $100m^2$. Với thí nghiệm này mạng không dây thường có khoảng 10 CH. Như vậy mỗi CH sẽ thường có ít hơn 16 nút mạng.

Trong chương trình thực nghiệm, chúng tôi chọn k = 1 cho mỗi phiên truyền dẫn. Rõ ràng, sau 28 vòng, khóa bí mật là hoàn toàn ngẫu nhiên. Chỉ có nút BS và nút cảm biến thực tế biết khóa bí mật hiện tại. Chúng tôi cũng giả thiết dùng chung một khóa động cho tất cả các nút mạng trong mạng WSNs thí nghiệm. Chúng tôi đã đo lường giá trị ID của một nút từ phiên truyền 30 đến 40 sau ba lần thử nghiệm. Chúng ta có thể lựa chọn bất cứ khoảng nào sau 28 lần truyền dẫn và khoảng

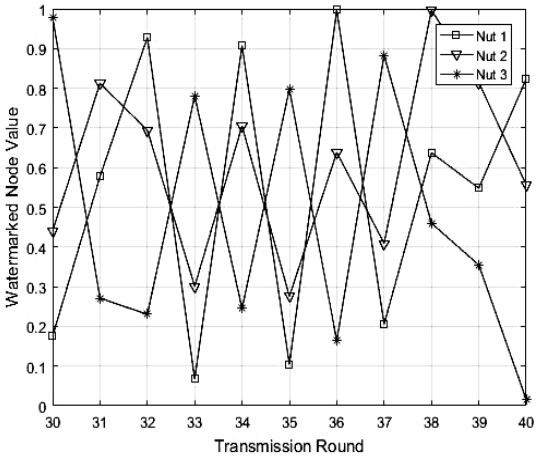
là tùy chọn do sau 28 lần thì giá trị của ID nút đã là ngẫu nhiên động. Chúng ta lựa chọn một khoảng nhỏ để có thể nhìn rõ giá trị của ID nút. Nếu lựa chọn quá nhiều phiên truyền thì sẽ khó phân biệt bằng mắt thường.



Hình 4. Giá trị của ID nút trong các lần thí nghiệm khác nhau

Trong hình 4, trục nằm ngang hiển thị vòng truyền (Transmission Round) từ vòng 30 đến vòng 40. Trục dọc hiển thị giá trị của ID nút (Watermarked Node Value) sau khi đã watermark động. Trong vòng đầu tiên, khóa ngẫu nhiên ban đầu được gán giá trị duy nhất cho tất cả các nút. Có thể thấy, với cùng một khóa bắt đầu, giá trị ID của một nút sau khi watermark trong các phiên truyền dẫn từ 30 đến 40 là hoàn toàn khác nhau trong ba lần thí nghiệm khác nhau. Điều này cho thấy tính ngẫu nhiên của phương pháp watermark được đề xuất. Giá trị ID của một nút trông có vẻ giống dao động hình sin nhưng với tần số ngẫu nhiên. Hãy xem xét giá trị ID của nút 01 trong lần truyền thứ hai trong hình 4, từ phiên truyền 36 sang 37 giá trị ID nút giảm nhưng liên tục tăng từ phiên truyền 38 đến 40.

Để xem xét tính duy nhất của các nút mạng sau khi được watermark chúng tôi tiến hành tính toán giá trị của ba nút mạng khác nhau trong một lần thí nghiệm và trong một phiên truyền dẫn. Kết quả thể hiện trong hình 5. Rõ ràng là giá trị sau khi watermark của mỗi nút mạng là hoàn toàn ngẫu nhiên và không thể dự đoán.



Hình 5. Giá trị của ba nút mạng trong một lần thí nghiệm

4. KẾT LUẬN

Trong nghiên cứu này chúng tôi đã đề xuất một thuật toán watermark động sử dụng trong mạng WSNs để chống lại các cuộc tấn công giả mạo hoặc clone đồng thời bảo vệ các dữ liệu thu thập được. Bằng cách sử dụng một khóa ngẫu nhiên động thay đổi sau mỗi phiên truyền dẫn hệ thống WSNs được bảo vệ mạch mẽ chống lại các cuộc tấn công từ bên ngoài. Một trong những vấn đề còn tồn tại là giao thức truyền dẫn thực tế kết hợp với thuật toán thực thi khi áp dụng phương pháp watermark động này sẽ được chúng tôi giới thiệu trong các nghiên cứu tiếp theo.

TÀI LIỆU THAM KHẢO

[1] T. Guan and Y. Chen, "A node clone attack detection scheme based on digital watermark in WSNs," 2016 First IEEE International Conference on Computer Communication and the Internet (ICCCI), Wuhan, 2016, pp. 257-260.

[2] W.B. Heinzelman, A.P. Chandrakasan, and H. Balakrishnan, “An application-specifc protocol architecture for wireless microsensor networks,” IEEE Transactions on Wireless Communications, vol. 1, no. 4, pp. 660–670, 2002.

[3] S.K. Singh, P. Kumar and J.P. Singh, "A Survey on Successors of LEACH Protocol," in IEEE Access, vol. 5, pp. 4298-4328, 2017.

[4] L.B. Oliveira, H.C. Wong, M. Bern, R. Dahab, and A.A.F. Loureiro, “SecLEACH-On the security of clustered sensor networks”, Signal Processing, Vol.87, I.12, 2007, Pages 2882-2895.

[5] T. Qiang, W. Bingwen, and D. Zhicheng, “Ms-leach: A routing protocol combining multi-hop transmissions and single-hop transmissions,” in Circuits, Communications and Systems, PACCS ’09. Pacific-Asia Conference on, May 2009, pp. 107–110.

[6] N. Rouissi, H. Gharsellaoui, “Improved Hybrid LEACH Based Approach for Preserving Secured Integrity in Wireless Sensor Networks”, Procedia Computer Science,Vol.112, 2017, Pages 1429-1438.

[7] W.R. Heinzelman, A. Chandrakasan and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, Maui, HI, USA, 2000, pp. 10 pp. vol.2.

[8] I. Kamel and H. Juma, "A Lightweight Data Integrity Scheme for Sensor Networks," Sensors 2011, *11*(4), 4118-4136.

Thông tin liên hệ: **Bùi Văn Hậu**

Điện thoại: 0912879002 - Email: bvhau@uneti.edu.vn
Khoa Điện tử, Trường Đại học Kinh tế - Kỹ thuật Công nghiệp

Hoàng Trọng Minh

Điện thoại: 0913259259 - Email: hoangtrongminh@ptit.edu.vn
Khoa Viễn thông, Học viện Công nghệ bưu chính viễn thông.