PHƯƠNG PHÁP XÁC THỰC TRONG MẠNG CẢM BIẾN KHÔNG DÂY BẰNG WATERMARKING

Hoàng Thị Thu
Học viện Công nghệ Bưu chính Viễn thông

***Tóm tắt*:** Vấn đề an toàn mạng cảm biến đã và đang là một vấn đề thu hút nhiều nhà nghiên cứu, triển khai hệ thống trước hàng loạt các yêu cầu và ứng dụng mới được đặt ra trong thời gian gần đây. Trong đó, tính xác thực đảm bảo dữ liệu không bị thay đổi trong quá trình truyền là một vấn đề có nhiều thách thức khi số lượng thiết bị cảm biến tăng rất nhanh và đa dạng kéo theo nhiều điều kiện ràng buộc khác biệt với các hạ tầng đã có. Bài báo này tập trung nghiên cứu các vấn đề liên quan tới xác thực trong mạng cảm biến không dây và mong muốn đề xuất một giải pháp xác thực dựa trên watermark để phù hợp với một số yêu cầu của mạng cảm biến không dây.

Từ khóa:Mạng cảm biến không dây, Watermarking, xác thực, trạm gốc.

I. MỞ ĐẦU

Cách tiếp cận xác thực bằng phương pháp watermark đã được rất nhiều các nhà khoa học trên thế giới quan tâm do tính gọn nhẹ của tiếp cận. Tuy nhiên, tại Việt Nam hướng đi này còn khá mới mẻ, và chưa có các nghiên cứu có hệ thống về khả năng và phương pháp ứng dụng giải pháp này trong mạng cảm biến không dây. Với mong muốn nghiên cứu tiềm năng xác thực của một giải pháp cụ thể. Từ đó, xây dựng khung lý thuyết về cách xác thực trong mạng cảm biến không dây trên cơ sở nghiên cứu các công trình khoa học của nước ngoài và khảo sát thực trạng ứng dụng giải pháp watermark của các nước trên thế giới.

Bài báo này trình bày giải pháp nhằm phân tích, đánh giá các giải pháp sử dụng xác thực bằng phương pháp watermark ứng dụng cho mạng cảm biến không dây, trên cơ sở đó đề xuất cải tiến một phương pháp xác thực trong mạng cảm biến không dây.

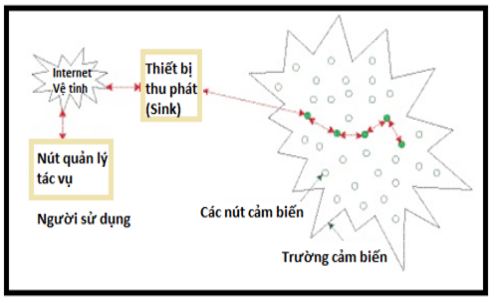
II. MẠNG CẢM BIẾN KHÔNG DÂY VÀ ỨNG DỤNG ĐIỂN HÌNH

A. Mạng cảm biến không dây

Mạng cảm biến không dây là một mạng không dây mà các nút mạng sử dụng các vi điều khiển, cảm biến, bộ truyền *RF* với kích thước tương đối nhỏ, đa chức năng, tiêu thụ năng lượng ít, có khả năng tự tổ chức, tự bảo trì, giá thành thấp để thực hiện nhiệm vụ thu thập thông tin. Thông tin được truyền về một trạm gốc thông qua các nút cảm biến khác và thông qua Internet truyền về trung tâm dữ liệu để lưu trữ, phân tích và xử lý. Nút cảm biến bao gồm các bộ vi xử lý rất nhỏ, bộ phận cảm biến, bộ thu phát không dây, bộ nhớ có giới hạn và nguồn nuôi. Khi nút cảm biến hoạt động, các nút này sẽ thu nhận tín hiệu từ môi trường và bản thân thiết bị, tín hiệu có thể là tín hiệu vật lý, sinh học, hóa học hay chuyển thành tín hiệu điện năng để đưa vào vi điều khiển. Thiết bị vi điều khiển sẽ thu nhận tín hiệu từ cảm biến và xử lý chúng. Sau đó, bộ truyền nhận tín hiệu thiết lập giao tiếp truyền dữ liệu đã được xử lý đến các nút trong mạng.

Mỗi nút cảm ứng được cấu thành bởi 4 thành phần cơ bản gồm: bộ cảm nhận (a sensing unit), bộ xử lý (a processing unit), bộ thu phát (a transceiver unit) và bộ nguồn (a power unit). Khi xây dựng mạng cảm biến trước hết phải chế tạo và phát triển các nút cấu thành mạng- nút cảm biến. Các nút phải có kích thước nhỏ, giá thành rẻ, hoạt động hiệu quả về năng lượng, có các thiết bị cảm biến chính xác có thể cảm nhận, thu thập các thông số môi trường, có khả năng tính toán, có bộ nhớ đủ để lưu trữ, và phải có khả năng thu phát sóng để truyền thông với các nút lân cận.

Các nút cảm ứng được phân bố trong một trường cảm biến (sensor field) như hình 1. Mỗi một nút cảm ứng có khả năng thu thập dữ liệu và định tuyến lại đến các nút *sink*. Dữ liệu được định tuyến lại đến các nút sink bởi một cấu trúc đa điểm, các nút sink có thể giao tiếp với các nút quản lý nhiệm vụ (task manager node) qua mạng Internet hoặc vệ tinh.



Hình 1. Cấu trúc mạng cảm biến không dây

Một số đặc điểm của mạng cảm biến không dây là:

Tác giả liên hệ: Hoàng Thị Thu
Email: thuht@ptit.edu.vn
Đến tòa soạn: 10/2019, chỉnh sửa 12/2019, chấp nhận đăng 12/2019.

- *Kích thước vật lý nhỏ gọn*: các nút cảm biến có kích thước nhỏ với phạm vi hạn chế. Khả năng truyền thông thấp do kích thước và năng lượng có hạn.

- Hoạt động với độ tập trung cao: WSN (mạng cảm biến không dây) giao tiếp sử dụng sóng vô tuyến qua một kênh không dây với phạm vi giao tiếp ngắn, băng thông rộng. Kênh truyền thông có thể là hai chiều hoặc đơn hướng.

- *Chi phí thấp*: có hàng trăm ngàn nút cảm biến được triển khai để đo bất kỳ mô trường vật lý nào, để giảm tổng chi phí của toàn bộ mạng lưới chi phí của nút cảm biến phải được giữ ở mức khả thi khi sử dụng.

- *Năng lượng hiệu quả*: nguồn năng lượng sử dụng trong mạng cảm biến với các mục đích khác nhau như tính toán, truyền thông và lưu trữ.

- *An ninh và bảo mật*: mỗi nút cảm biến có cơ chế bảo mật đủ để ngăn chặn truy cập trái phép, tấn công và thiệt hại không chủ ý của thông tin bên trong nút cảm biến.

- *Nền mạng liên kết động*: các nút cảm biến có thể bị hỏng do pin cạn kiệt hoặc các trường hợp khác, kênh truyền thông có thể bị gián đoạn cũng như nút cảm biến bổ sung có thể được thêm vào mạng dẫn đến thay đổi cấu trúc mạng.

- *Truyền thông đa chiều*: phần lớn các nút cảm biến giao tiếp với nút sink hoặc trạm cơ sở để có sự trợ giúp của một nút trung gian thông qua đường truyền dẫn định tuyến. Khi giao tiếp với các nút khác hoặc trạm cơ sở vượt ngoài tần số vô tuyến thì phải thông qua các định tuyến đa chiều bằng nút trung gian.

Công nghệ truyền dẫn trong WSN (mạng cảm biến không dây) gồm: bluetooth, zigbee, z-wave, 6LoWPAN, Thread, Wifi, Cellular, NFC, Sigfox, Neul, Lora.

B. Ứng dụng trong WSN

WSN (mạng cảm biến không dây) được ứng dụng rộng rãi trong đời sống của con người, dưới đây là các ứng dụng cơ bản WSN mang lại như:

- ***Trong quân đội***: *giám sát lực lượng, trang thiết bị và đạn dược* gắn liền với các thiết bị cảm biến nhỏ để có thể thông báo về trạng thái. *Giám sát địa hình và lực lượng quân địch* ở những địa hình then chốt và một vài nơi quan trọng, các nút cảm biến cần nhanh chóng cảm nhận các dữ liệu và tập trung dữ liệu gửi về trong vài phút trước khi quân địch phát hiện để ngăn chặn lại chúng. *Giám sát chiến trường* các tuyến đường mòn và các chỗ eo hẹp có thể nhanh chóng được bao phủ bởi mạng cảm biến và theo dõi các hoạt động của quân địch.

- ***Trong môi trường***: nhiệt độ, độ ẩm; theo dõi và cảnh báo sớm các hiện tượng thiên tai như động đất, núi lửa phun trào, cháy rừng, lũ lụt. *Phát hiện cháy rừng* mỗi nút cảm ứng thu thập nhiều thông tin khác nhau liên quan đến cháy như nhiệt độ, khói. Các dữ liệu thu thập được truyền multihop tới nơi trung tâm điều khiển để giám sát, phân tích, phát hiện và cảnh báo cháy sớm. *Giám sát và cảnh báo các hiện tượng địa trấn*: cảm biến về độ rung được đặt rải rác ở mặt đất hay trong lòng đất những khu vực hay xảy ra động đất, gần các núi lửa để giám sát và cảnh báo sớm hiện tượng động đất và núi lửa phun trào.

- ***Trong y học***: giám sát và chẩn đoán từ xa, các nút cảm ứng được gắn vào cơ thể, thí dụ như ở dưới da và đo các thông số của máu để phát hiện sớm các bệnh như ung thư, nhờ đó việc chữa bệnh sẽ dễ dàng hơn.

- ***Trong gia đình***: tự động hóa nhà ở, các nút cảm ứng được đặt ở các phòng để đo nhiệt độ. Hơn nữa, chúng còn được dùng để phát hiện những sự dịch chuyển trong phòng và thông báo lại thông tin này đến thiết bị báo động trong trường hợp không có ai ở nhà.

- ***Trong công nghiệp***: quản lý kinh doanh, công việc bảo quản và lưu giữ hàng hóa sẽ được giải phóng. Các kiện hàng sẽ bao gồm các nút cảm ứng mà chỉ cần tồn tại trong thời kì lưu trữ và bảo quản. Trong mỗi lần kiểm kê, một truy vấn tới kho lưu trữ dưới dạng bản tin quảng bá, tất cả các kiện hàng sẽ trả lời truy vấn đó để bộc lộ các đặc điểm của chúng.

- ***Trong nông nghiệp***: cảm biến được dùng để đo nhiệt độ, độ ẩm, ánh sáng ở nhiều điểm trên thửa ruộng và truyền dữ liệu mà chúng thu được về trung tâm để người nông dân có thể giám sát và chăm sóc, điều chỉnh cho phù hợp.

- ***Trong giao thông***: các cảm biến được đặt trong ô tô để người dùng có thể điều khiển, hoặc được gắn ở vỏ của ô tô, các phương tiện giao thông để chúng tương tác với nhau, với đường và các biển báo để giúp các phương tiện đi được an toàn, tránh tai nạn giao thông, giúp việc điều khiển luồng tốt hơn.

III. XÁC THỰC TRONG MẠNG CẢM BIẾN KHÔNG DÂY

Các kỹ thuật xác thực được sử dụng phổ biến nhất là mật mã khóa công khai hoặc mã khóa riêng tư. Trong một số mạng, một nút sẽ được chọn làm đầu cụm sẽ liên lạc với cơ sở trạm thông qua một máy chủ đáng tin cậy. Trong trường hợp này các nút phải được xác thực để đảm bảo tính bảo mật. Xác thực đảm bảo an ninh các nút trong một mạng. Trong mạng cảm biến việc bảo mật, toàn vẹn, tính xác thực, không từ chối và thỏa hiệp nút là các tính năng chính.

A. Nguyên lý xác thực

Quá trình xác thực là cần thiết để duy trì quyền riêng tư, tính toàn vẹn và dữ liệu sai vào mạng. Sự thay đổi của thông điệp có thể là trong quá trình truyền tin nhắn trong mạng, xác thực là cần thiết để dừng thay đổi tin nhắn. Nút trong mạng có thể bị xâm phạm bởi đối thủ và họ có thể thực hiện bất kỳ thay đổi nào trong thư được chuyển tiếp đến nút sink hoặc trạm gốc hoặc một dữ liệu bổ sung có thể được thêm vào dữ liệu đang được được chuyển giao.

Xác thực cung cấp tính chính xác theo một quá trình xác định nguồn của nó bằng một số kỹ thuật xác thực. Các vấn đề chính về bảo mật trong một mạng lưới như sau:

- Tính xác thực - đích của một tin nhắn có thể kiểm tra danh tính của nguồn.

- Bảo mật - nội dung chỉ được truy cập bởi các nút được ủy quyền.
- Tính toàn vẹn - kiểm tra sửa đổi nội dung trong khi truyền tải thông điệp.

Các biện pháp bảo mật trong mạng cảm biến không dây bao gồm:

- Sự khả dụng - các dịch vụ mạng có sẵn khi cần.
- Sự ủy quyền - chỉ người dùng hoặc các nút được ủy quyền gửi tin nhắn, xác thực, bảo mật, chính trực.
- Không từ chối - nút không thể ngừng gửi một thư đã gửi, khả năng mở rộng.

Giai đoạn xác thực gồm hai giai đoạn cơ bản sau:

- *Giai đoạn đăng nhập*: Người dùng nhập tài khoản và mật khẩu. Hệ thống kiểm tra tài khoản và mật khẩu với những người được lưu trữ trong đó. Nếu đã nhận dạng và mật khẩu chính xác thì người dùng đã được xác thực.
- *Giai đoạn xác minh*: Khi nhận được yêu cầu đăng nhập tại thời điểm *T*, nút xác thực người dùng và xác thực người dùng tại thời điểm *T*.

B. Các giải pháp xác thực trong WSN

Một số giải pháp dùng để xác thực trong WSN (mạng cảm biến không dây) là:

- *Xác thực dựa trên khóa công khai*: hoạt động khóa công khai là khả thi cho cả một nút cảm biến rất nhỏ. Tất cả khóa công khai lược đồ sử dụng do BS (trạm gốc) tạo ra và được sử dụng để xác thực người dùng [4]. Tuy nhiên, hoạt động khóa công khai chậm hơn và tiêu thụ nhiều hơn năng lượng hơn là hoạt động chính đối xứng. Vì vậy, nếu một kẻ tấn công khởi động tấn công DoS, kẻ tấn công có thể dễ dàng làm cạn kiệt năng lượng hạn chế của nút cảm biến.
- *Xác thực dựa trên khóa đối xứng*: một sơ đồ phân phối chính là phương pháp phân phối các thông tin cá nhân riêng lẻ cho một tập hợp [5]. Sau đó, mỗi thành phần của bất kỳ nhóm sử dụng nào của một kích thước cụ thể có thể tính toán khóa nhóm bảo mật chung. Trong phần này, bất kỳ nhóm nào của *t* sử dụng có thể tính toán một khóa chung bởi mỗi máy tính chỉ sử dụng phần ban đầu riêng thông tin của mình và danh tính của các gamma khác *t*.
- *Xác thực sử dụng cấp hai TTUA*: trong sơ đồ TTUA, *CH* (Cluster Head): nút chủ được sử dụng trong mạng để dữ liệu cảm nhận, sau khi được thu thập, được truyền qua CH về phía yêu cầu người dùng. Giữa CH và người dùng họ cấp SKC (Symmetric Key Cryptography): mật mã khóa đối xứng để xác thực. Ngoài ra, trong SKC không bao gồm phần hiện tại từ mạng và phần mới vào mạng, yêu cầu thu hồi khóa và phân phối chính lại.
- *Xác thực sử dụng cấp cao hai cao cấp TTUA*: *CH* có khả năng xử lý cao và lâu dài nguồn cung cấp năng lượng lâu dài, chẳng hạn như *PDA* (Personal Digital Assistant): thiết bị trợ giúp cá nhân. Nút cảm biến có khả năng xử lý thấp và sức mạnh hạn chế nguồn cung cấp. *CH* được giả định là cổng tin cậy cho các nút cảm biến. Vì vậy, giữa *CH* và người dùng thuật toán *PKC* (Public Key Crypto): mật mã khóa công khai được sử dụng cho các mục đích *UA* [10]. Một lần người dùng được xác thực vào *CH* khi được phép truy cập các nút cảm biến thông qua *CH* đó. Với yêu cầu công suất thấp giữa *CH* và nút cảm biến *SKC* thuật toán được sử dụng. *WSN* bao gồm *CH* và cảm biến các nút, đại diện cho một cấu trúc mạng không đồng nhất. *CH* có sức mạnh truyền thông cao hơn các nút cảm biến và do đó có phạm vi phủ sóng vô tuyến nhiều hơn. *CH* có thể giao tiếp với nhau và với *BS (trạm gốc)*, theo thứ tự để bảo vệ các vật liệu khóa, *CH* được trang bị phần cứng chống giả mạo.

IV. XÁC THỰC BẰNG PHƯƠNG PHÁP WATERMARKING

Phương pháp Watermarking là một phương pháp hiệu quả, cho phép chủ sở hữu nội dung số có thể nhúng và giấu những bằng chứng về bản quyền của mình, sau đó, có thể xác định được quyền sở hữu, phát hiện ra việc sử dụng trái phép mà không làm ảnh hưởng đến nội dung đó. Watermarking với kịch bản dựa trên cụm trong WSN (mạng cảm biến không dây) nhằm xác thực node và luồng dữ liệu một cách minh bạch với độ tin cậy cao. Cách phân tích lý thuyết và kết quả mô phỏng số sẽ được trình bày chi tiết để góp phần khẳng định khả năng ứng dụng giải pháp Watermarking để xác thực trong WSN (mạng cảm biến không dây).

A. Giải pháp Watermarking

Khi có một đối tượng cần xác thực là *K* như: một văn bản, một chuỗi bit, một tập tin âm thanh, một bức ảnh. Nếu dùng phương pháp mã hóa để xác thực *K*, ta sẽ thu được xác thực của *K* là *K′*. Do vậy, *K′* mang giá trị vô nghĩa và làm cho đối phương nghi ngờ, tìm mọi cách thám mã. Ngược lại, nếu dùng phương pháp Watermarking giấu *K* vào một đối tượng khác, một bức ảnh *F* ta sẽ thu được bức ảnh *F′* có nội dung không sai khác gì với *F*. Khi đó, chỉ cần gửi ảnh *F* cho người nhận, để lấy ra bản tin *K* từ ảnh *F′* ta có thể cần hoặc không cần ảnh gốc *F* tùy theo từng phương pháp. Cho nên, khi đối phương bắt được tấm ảnh *F′* nếu là ảnh lạ như ảnh cá nhân, ảnh phong cảnh thì khó nảy sinh nghi ngờ về khả năng chứa tin mật trong *F*.

Watermark là một kỹ thuật nhúng (giấu) một lượng thông tin nào đó vào trong một đối tượng dữ liệu mà thông tin này có thể được phát hiện và tách sau đó nhằm xác thực nguồn gốc hay chủ sở hữu của thông tin đó. Trong kỹ thuật đánh dấu hình ảnh gồm hai loại: theo vùng không gian và vùng tần số. Các kỹ thuật trong vùng không gian biến đổi trực tiếp các giá trị cường độ, màu sắc của một số điểm ảnh chọn trước, còn kỹ thuật vùng tần số biến đổi các giá trị của các hệ số biến đổi. Trong Watermarking, mỗi nút cảm biến nhúng một watermark duy nhất vào dữ liệu và *BS (trạm gốc)* có thể xác minh tính toàn vẹn dữ liệu. Các nút cảm biến có khả năng cảm nhận các tham số khác nhau như chiều dài dữ liệu, tần suất xuất hiện gói tin, thời gian nhận dữ liệu của các nút cảm biến. Mỗi nút cảm biến nhúng một hình mờ duy nhất để cảm biến dữ liệu và gửi nó đến *BS (trạm gốc)* cùng với các dữ liệu. Sau đó, *BS* (*trạm gốc)* xác minh tính toàn vẹn của dữ liệu bằng cách nhúng Watermark.

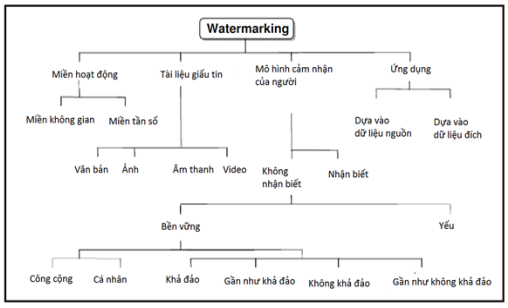
Kỹ thuật đánh dấu hình ảnh vùng không gian điển hình là nhúng một mã đánh dấu vào các bit có trọng số nhỏ nhất (LSB) của một số điểm ảnh chọn ngẫu nhiên. Mã đánh dấu thực sự không thể nhìn thấy đối với mắt người, nhưng dễ bị phá hủy nếu hình ảnh có mã đánh dấu bị lọc thông thấp hay bị nén JPEC.

Kỹ thuật vùng tần số là quá trình biến đổi hình ảnh thành một tập các hệ số vùng tần số. Phép biến đổi có thể là DCT, biến đổi Fourier hay Wavelet,.. Các mã đánh dấu sau đó được nhúng vào các hệ số biến đổi của hình ảnh sao cho ít nhìn thấy được nhất và bền vững hơn trước các thao tác xử lý ảnh. Các hệ số được biến đổi ngược lại để tạo thành hình ảnh có mang mã đánh dấu. Độ nhạy tần số hệ thống thị giác của con người được dùng để đảm bảo mã đánh dấu không thể nhìn thấy và bền vững trước mọi nguy cơ tấn công.

Kỹ thuật watermarking là quá trình nhúng thông tin cho phép một cá nhân thêm thông báo bản quyền ẩn hoặc các tin nhắn xác minh khác vào âm thanh, video hoặc hình ảnh kỹ thuật số tín hiệu và đối tượng tài liệu. Thông điệp ẩn là một nhóm các bit mô tả thông tin liên quan đến tín hiệu hoặc tác giả của tín hiệu. Tín hiệu có thể là âm thanh, hình ảnh hoặc video nếu tín hiệu được sao chép, thì thông tin cũng được thực hiện trong sao chép. Hệ thống watermarking bao gồm ba giai đoạn chính: quá trình tạo watermark, quá trình nhúng watermark bao gồm truyền thông tin và các cuộc tấn công có thể xảy ra thông qua các kênh truyền thông và quá trình phát hiện watermark thu hồi.

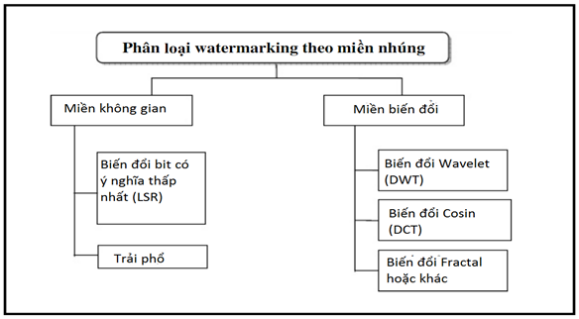
B. Phân loại và một số giải pháp xác thực WSN

Có nhiều cách phân loại kỹ thuật Watermarking



Hình 2. Phân loại Watermarking

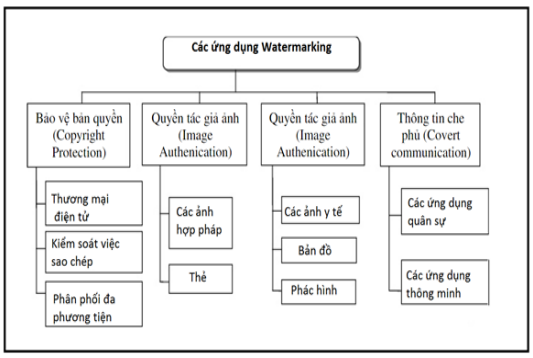
Phân loại theo miền nhúng gồm: miền không gian, miền tần số, miền DFT, miền DCT, miền DWT, miền hỗn hợp, ví dụ như là miền hình học, miền Fourier-Mellin, đặc tính Histogram, miền biến đổi Wavelets phức tạp.



Hình 3. Phân loại các thuật toán Watermarking dựa trên miền biến đổi khi nhúng dữ liệu

Kỹ thuật Watermarking có thể chia thành 4 loại theo đúng tài liệu nhúng watermark bao gồm: ảnh, video, văn bản, âm thanh, định dạng đa phương tiện đặc biệt. Theo hệ thống nhìn của con người kỹ thuật watermarking số có thể chia thành các loại sau: watermark có thể nhìn thấy, watermark bền vững không nhìn thấy, watermark yếu không nhìn thấy, watermark kép.

Phương pháp thay đổi dữ liệu chủ gồm: cộng tuyến tính của tín hiệu trải phổ, tổng hợp ảnh, thay thế và lượng tử hóa không tuyến tính.



Hình 4. Phân loại Watermarking dựa vào ứng dụng cụ thể

Một số giải pháp xác thực WSN

Để đảm bảo tính toàn vẹn và xác thực của dữ liệu trong WSN (mạng cảm biến không dây), nhiều nhà nghiên cứu đề xuất các kỹ thuật watermarking thông qua các công trình khoa học điển hình như:

Ding et al.[11] và Shi et al.[16] đề xuất phương pháp watermarking đảo ngược dựa trên sự mở rộng lỗi khác nhau để giải quyết vấn đề sửa đổi không thể đảo ngược trong dữ liệu watermark. Mặc dù, các chương trình này bảo đảm tính toàn vẹn dữ liệu và hoàn thiện khôi phục dữ liệu ban đầu trong trường hợp bị tấn công sửa đổi, tuy nhiên, tại các chi phí của phí trên về lưu trữ và tính toán ở phía người gửi.

Sun et al.[15] giải quyết vấn đề toàn vẹn dữ liệu trong WSN bằng cách sử dụng watermarking. Đề án cung cấp bảo vệ chống lại các kiểu tấn công khác nhau, chẳng hạn như gói tin giả mạo tấn công, chuyển tiếp chọn lọc, phát lại gói tin, truyền tải gói tin trì hoãn, và gói tin giả mạo.

Panah et al.[1] khám phá vấn đề về toàn vẹn dữ liệu bằng cách nhúng một số mã chữ ký trong luồng dữ liệu sử dụng kỹ thuật số watermarking. Mục đích chính của chữ ký mã là để bảo vệ các thuộc tính thống kê của luồng dữ liệu trước khi chuyển sang các kỹ thuật watermark.

Zhang et al.[13] đã sử dụng một chương trình watermarking số để xác thực dữ liệu trong WSN (mạng cảm biến không dây), cung cấp hỗ trợ cố hữu để xử lý trong mạng và kết thúc quá trình xác thực. Đề án thành công có thể phát hiện các sửa đổi dữ liệu.

Zhouet al.[18] đã đề xuất kế hoạch watermarking để ngăn chặn dữ liệu cảm quan từ nghe trộm và tấn công giả mạo nhằm tăng hiệu quả về mặt lưu trữ cũng như phát hiện tấn công mất gói và tấn công giả mạo.

Kamel et al.[6] đề xuất một mô hình watermarking cho truyền thông dữ liệu cảm giác an toàn trong WSN (mạng cảm biến không dây). Trong sơ đồ này, watermarking sẽ chống lại các loại tấn công như tấn công sửa đổi, tấn công chèn và xóa tấn công.

Trong một nghiên cứu khác, Kamel et al.[7] đề xuất một sơ đồ watermarking, có tên gọi là watermarking trong chuỗi trọng lượng nhẹ để bảo đảm tính toàn vẹn của dữ liệu trong WSN (mạng cảm biến không dây). Đề án đề xuất phát hiện các sửa đổi trái phép trong luồng dữ liệu và không cung cấp bảo mật dữ liệu.

Wang et al.[2] đề xuất một kỹ thuật giấu thông tin để đảm bảo truyền dữ liệu trong WSN (mạng cảm biến không dây) với thiết kế đặc biệt để ngăn chặn các cuộc tấn công với danh tính giải mạo bởi kẻ tấn công. Một cấu trúc dữ liệu không gian hiệu quả gọi là bộ lọc Bloom, được sử dụng để nhúng thông tin bí mật vào dữ liệu ban đầu. Kết quả thực nghiệm và đánh giá kết quả cho thấy thông tin nhúng có thể phát hiện nút độc hại với danh tính giả mạo. Tuy nhiên, đề án đề xuất không hiệu quả để phát hiện các cuộc tấn công được thực hiện bởi các nút độc hại đối với tính toàn vẹn của dữ liệu.

Xiao et al.[12] đã đề xuất một thuật toán watermarking để bảo vệ bản quyền của dữ liệu. Watermark nhúng bao gồm các thuộc tính số của gửi thời gian của gói. Hiệu suất của đề xuất mạnh mẽ được đánh giá dựa trên ba tham số, không có phương pháp khóa, với phương pháp chiều dài khóa 8-bit, độ dài khóa 16 bit.

Wang et al.[19] đề xuất một kỹ thuật watermark để bảo vệ bản quyền của dữ liệu trong WSN (mạng cảm biến không dây). Watermark được nhúng trong dữ liệu ban đầu bằng cách sử dụng cả LSB và MSRB bit của trường dữ liệu. Cả hai dữ liệu gốc và watermark đều được gửi tới *BS (trạm gốc)* để xác minh bản quyền của dữ liệu. Ngoài bản quyền, một bảng tra cứu được sử dụng để nâng cao hiệu quả phân tích cú pháp dữ liệu.

C. Mô phỏng hệ thống xác thực bằng Watermarking

a. Ý tưởng giải pháp

Tính toàn vẹn dữ liệu là điều quan trọng thách thức an ninh, một trong các yêu cầu chính trong WSN (mạng cảm biến không dây) là tính toàn vẹn và xác thực được dữ liệu tại *BS (trạm gốc)*. Tôi đề xuất một phương pháp để xácc thực dữ liệu trong cảm biến được dựa trên một mô hình zero watermark technique (ZWT) kết hợp với phân tích lưu lượng truy cập. Trong kỹ thuật watermarking, mỗi nút cảm biến nhúng một watermark duy nhất vào dữ liệu cảm biến và BS (trạm gốc) có thể xác minh tính toàn vẹn của dữ liệu. Kỹ thuật ZWT sử dụng chính những đặc tính của dữ liệu để tạo nên watermark, điều này giúp hệ thống trở nên đơn giản về mặt tính toán, tiêu tốn năng lượng cho quá trình xác thực thấp [8]. Kỹ thuật ZWT có thể tránh được kiểu tấn công làm thay đổi bản tin do nó sẽ làm thay đổi đặc tính dữ liệu, tuy nhiên với kiểu tấn công làm thay đổi lưu lượng thì phương pháp này tỏ ra không hiệu quả.

Với kiểu tấn công nhằm vào lưu lượng, kẻ tấn công có thể chiếm giữ luồng lưu lượng tới 1 khu vực nhất định và loại bỏ những gói tin mang nội dung đặc biệt để tránh cho *BS (trạm gốc)* sớm phát hiện được. Một node trên mạng có thể bị chiếm đóng và có thể liên tục gửi đi những gói tin giả theo phương thức DoS để làm tăng lưu lượng trên mạng. Chúng ta giả sử rằng có một node bị chiếm đóng trong mạng và lần lượt cắt bỏ 20%, 50%, 80% và 100% lưu lượng từ 1 node con, hoặc gửi thêm những bản tin rác làm tăng lưu lượng theo tỉ lệ tưởng ứng. Kẻ tấn công không thể thay đổi nội dung các bản tin vì tính toàn vẹn của dữ liệu sẽ được xác thực bằng phương pháp ZWT. Chúng ta giả sử rằng bất kì node nào cũng có thể là đối tượng bị tấn công, ngoại trừ trạm gốc. Khoảng thời gian giữa 2 gói tin liên tiếp nhận được tại trạm gốc (*IAT*) là tham số ta dùng để phát hiện hành vi bất thường. Những sự kiện ngẫu nhiên gây lỗi trong mạng như là tắc nghẹn hoặc đứt liên kết tạm thời có thể dẫn đến phát hiện tấn công sai. Vì vậy ta cần kết hợp phân tích nhiều đặc tính về lưu lượng để tăng tỉ lệ phát hiện lỗi chính xác và giảm những cảnh báo sai. Chúng ta đưa ra những giả thiết ban đầu cho mô hình mạng và lưu lượng như sau:

- Các node cảm biến thu thập dữ liệu từ môi trường xung quanh, sau đó có truyền thẳng tới *BS* (trạm gốc) hoặc sẽ thông qua những node cụm chủ tương ứng.
- Trạm gốc hoạt động như một trung tâm xác thực, không thể bị tấn công hoặc chiếm đóng.

Trong bài báo này, chúng ta sẽ chỉ xem xét mô hình điểm - điểm (one- to -one), mạng cảm biến sẽ bao gồm các node cảm biến và một trạm gốc duy nhất. Mô hình điểm- điểm được mô tả trong hình 5. Tất cả bản tin được truyền từ node cảm biến tới trạm gốc sẽ không đi qua bất kỳ node trung gian nào (truyền dẫn đơn bước). Trạm gốc nhận được dữ liệu cảm biến và thực hiện các quá trình xử lý.

b. Kịch bản thử nghiệm

Kịch bản 1: Xác thực điểm -điểm trong WSN

Quá trình truyền dữ liệu one to one (điểm-điểm) bao gồm các bước: tạo watermark, nhúng watermark vào dữ liệu, phân tách watermark và thuật toán xác thực. Phần tiếp theo, chúng ta sẽ phân tích chi tiết hoạt động của kĩ thuật watermark dựa trên phân tích lưu lượng dữ liệu. Những kí hiệu và ý nghĩa của chúng được trình bày ở bảng 1 dưới đây:

Bảng 1. Ký hiệu các tham số

d	Dữ liệu cảm biến
SK	Khóa bí mật
w_l	Độ dài của gói tin dữ liệu
w_0	Tần xuất xuất hiện bit 1
w_t	Thời gian thu thập gói tin
w_f	Watermark
$\|\|$	Phép nối bit
E	Mã hóa
E_{wf}	Watermark đã được mã hóa
d^w	Dữ liệu đã được watermark
ID	Mã định danh của node
IAT	Khoảng thời gian giữa 2 gói tin liên tiếp nhận được tại trạm gốc

- *Tạo Watermarking*

Quá trình tạo watermark sử dụng dữ liệu cảm biến *d* làm đầu vào cho cho mỗi node cảm biến và tạo ra watermark dựa trên những đặc tính của dữ liệu như là: mã nhận diện node ID, chiều dài gói tin wi, tần xuất xuất hiện của bit 1 w0 và thời gian node thu thập được gói tin để tạo nên một watermark wf gửi đi cùng dữ liệu. Giả thiết khi mạng cảm biến hình thành, trạm gốc cấp cho mỗi node một ID dài 4 byte, trạm gốc lưu trữ một cơ sở của những ID đó để xác minh gói tin tới. Thời gian thu thập gói tin là một tham số quan trọng để xác thực gói tin đó, trạm gốc có thể dựa vào trường thời gian được ghi trong watermark giữa 2 gói tin liên tiếp và so sánh với thời gian đến thật của các gói tin để phát hiện tấn công. Thuật toán 1 mô tả chi tiết quá trình tạo ra watermark.

- *Nhúng Watermarking*

Trong quá trình nhúng watermark, phải mất dữ liệu cảm quan d, watermark cuối w_f, và phím bí mật *SK* làm đầu vào và tạo ra một dữ liệu được đánh dấu là d^w ở phía đầu ra. Trong thuật toán 2, một watermark w_f cuối cùng được mã hóa với khóa bí mật *SK* (dòng 4). Sau đó, nó được nhúng dữ liệu cảm giác *d* với watermark được mã hóa E_{wf} để tạo ra một dữ liệu watermarked d^w và gửi tới trạm gốc (*BS)* thông qua kênh truyền dẫn (các dòng 5-6) như thể hiện trong thuật toán 2. *BS* phân phối các khóa bí mật tới các nút cảm biến thông qua giao thức Hellman để đảm bảo độ dài bit cho khóa bí mật.

Thuật toán 1: Tạo Watermark

1: Thủ tục: Watermark

2: Đầu vào: d

3: Đầu ra: w_f

4: $w_l \leftarrow$ Chiều dài gói tin (*d*)

5: $w_0 \leftarrow$ Tần xuất xuất hiện bit 1 của gói tin (*d*)

6: $w_t \leftarrow$ Thời gian bắt được gói tin (*d*)

7: ID $\leftarrow$ Mã định danh node

8: $w_f \leftarrow$ ID + ($w_i||w_0||w_t$)

9: Kết thúc quá trình

Thuật toán 2:Nhúng Watermark

1: Thủ tục: Nhúng Watermark

2: Đầu vào: d, w_f, SK

3: Đầu ra: d^w

4: $E_{wf} \leftarrow$ Mã hóa (w_f, SK)

5:$d^w \leftarrow d||E_{wf}$ Nhúng Watermark

6: Gửi dữ liệu Watermark được đánh dấu (d^w)

7: Thủ tục quá trình.

Thuật toán 3: Khai thác và xác minh Watermark

1: Thủ tục: Phân tách và xác thực watermark

2: Đầu vào: d^w, SK

3: Kết quả: đã được xác minh/chưa được xác minh

4: Nhận dữ liệu đánh dấu (d^w)

5: Trích xuất watermark từ gói tin nhận được *d* và E_{wf}

6:$w_f \leftarrow$ Giải mã (E_{wf}, S_k) Trích xuất Watermark

7: $w'_f \leftarrow$Chạy lại thuật toán 1 Watermark được tạo lại

8: Nếu $w_f == w'_f$ và ID thuộc {*ID*}

9: Xác mình toàn vẹn dữ liệu

10: Nếu $IAT_{min} < IAT < IAT_{max}$

11: Xác mình toàn vẹn lưu lượng

12: Thủ tục kết thúc

- *Thu thập và thẩm định Watermark*

Thuật toán 3, mô tả hoạt động của thuật toán phân tách và xác minh tại trạm gốc. Tại *BS*, thuật toán trích xuất và xác minh watermark qua thuật toán sử dụng dữ liệu đã được watermark d^w và khóa bí mật *SK* làm đầu vào và tái tạo lại watermark w'_f từ dữ liệu được bóc tách để xác minh tính toàn vẹn dữ liệu. BS (trạm gốc) nhận dữ liệu đã watermark dw và trích xuất thành d và watermark đã mã hoá E_{wf} như trong các dòng 4-5 của thuật toán 3. Ở dòng 6, hoạt động giải mã được thực hiện với khoá bí mật SK trên watermark đã được mật mã E_{wf} để lấy watermark w_f. Trong phần xác minh, thuật toán tạo watermark được thực hiện lại trên dữ liệu d để tái tạo watermark w'_f. Thực hiện so sánh để kiểm tra tính toàn vẹn của dữ liệu bằng cách so sánh watermark w_f và w'_f như trong các dòng 8-11 của thuật toán 3. Sau đó dựa trên trường thời gian thu thập gói tin wt trên 2 gói liên tiếp, ta tính được tốc độ gửi gói tên từ node cảm biến. Dựa trên kĩ thuật phân tích lưu lượng, ta xác định một khoảng giá trị cho khoảng thời gian giữa 2 gói liên tiếp (từ cùng 1 nguồn) đến trạm gốc. Nếu khoảng thời gian thực tế đo được nằm trong khoảng này thì ta xác mình được thêm tính toàn vẹn của lưu lượng.

Kịch bản 2: Phân tích lưu lượng luồng dữ liệu dựa trên thời gian đến hai gói tin liên tiếp (IAT)

Trong phần khởi tạo, các nút chuyển tiếp lấy mẫu các giá trị IAT của các nút tham gia. Nếu chất lượng liên kết là tốt, tỷ lệ đến gói trung bình từ một nút gần với tốc độ gửi của nó thì phương sai của IAT là nhỏ và IAT T có thể xấp xỉ bằng số mũ phân phối:

$$P(T < t) = \begin{cases} 1 - e^{-\lambda t}, t \geq 0 \\ 0, t < 0 \end{cases} \quad (1)$$

Trong đó λ là tham số tốc độ và được ước tính là $\hat{\lambda} = \frac{1}{\overline{T}}$.

Với $\overline{T} = w_{t_1} - w_{t_2}$ và α là các ngưỡng *T*, tương ứng với các phương trình sau:

$$P(T < T_{high}) \approx 1 - e^{-\frac{T_{high}}{\overline{T}}} = 1 - \frac{\alpha}{2} \Rightarrow T_{high} = -\overline{T}.\ln\left(\frac{\alpha}{2}\right) \quad (2)$$

$$P(T < T_{low}) \approx 1 - e^{-\frac{T_{low}}{\overline{T}}} = \frac{\alpha}{2} \Rightarrow T_{low} = -\overline{T}.\ln\left(1 - \frac{\alpha}{2}\right) \quad (3)$$

Do đó, khoảng thời gian cho IAT là:

$$T_{low} = -\overline{T}.\ln\left(1-\frac{\alpha}{2}\right) < T < -\overline{T}.\ln\left(\frac{\alpha}{2}\right) = T_{high} \quad (4)$$

Nếu IAT nhận giá trị ngoài khoảng thời gian (4), sẽ xuất hiện cuộc tấn công với xác suất (1-α) và có cảnh báo. Trong khoảng thời gian (4) rất lớn và chỉ phát hiện giá trị cực đoan của IAT với khoảng tin cậy chính xác dựa trên thực tế là mức trung bình $\overline{T}$ có phân phối Erlang với tham số nλ, trong đó n là kích thước mẫu và λ là tham số tốc độ phân phối theo hàm số mũ. Do đó, 100(1-α) % khoảng tin cậy trung bình cho IAT có dạng sau:

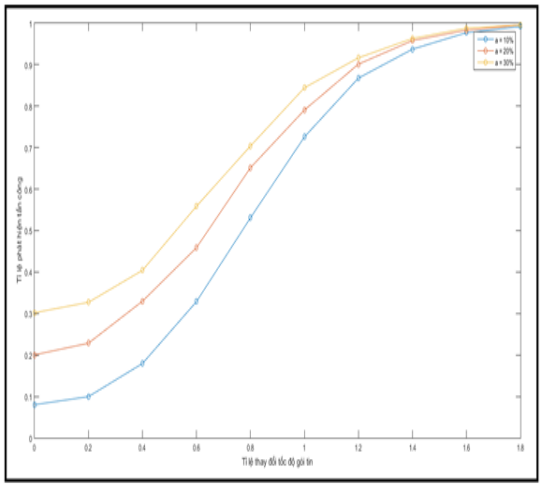
$$T'_{low,\alpha} = 2n\overline{T}/\chi^2_{2n,\alpha/2} < T < 2n\overline{T}/\chi^2_{2n,1-\alpha/2} = T'_{high,\alpha'} \quad (5)$$

c. Mô phỏng kiểm chứng kịch bản tấn công lưu lượng

Mô phỏng kịch bản WSN one to one được thực hiện trên phần mềm mô phỏng MATLAB. Lưu lượng gói tin từ một node cảm biến tới trạm gốc được giả sử tuân theo phân bố hàm mũ do các yếu tố ảnh hưởng đến kênh truyền như mất gói, tắc nghẽn, những tham số sau được chọn dựa trên thực tế để làm thiết lập môi trường mô phỏng:

- Diện tích 100x100 m^2
- Mô hình một trạm gốc.
- Số lượng node: 100
- Các node được phân bố theo phân bố đều
- Tỉ lệ gửi gói tin: 1 gói/1.5s
- IAT của luồng tin nhận tại trạm gốc tuân theo phân bố mũ.
- Chiều dài gói tin: 10B-100B trong đó sử dụng 4B cho watermark
- Mức tin cậy α =10%
- Giả sử có 1 node đang bị tấn công
- Kẻ tấn công chặn gói hoặc thêm 20%, 50%, 80%, 100% số lượng gói tin.

Hình 5 cho thấy tỉ lệ phát hiện tấn công trung bình của kĩ thuật phân tích lưu lượng dựa trên IAT thay đổi theo mức độ thay đổi lưu lượng của kẻ tấn công lần lượt là 20% 50% 100% đến 200% với tốc độ gói tin gửi đi từ node cảm biến là 1 gói mỗi 1.5s. Tỷ lệ phát hiện lỗi còn phụ thuộc vào mức tin cậy chúng ta chọn trong công thức (5). Mức tin cậy quyết định khoảng giới hạn của IAT, nếu khoảng giới hạn quá nhỏ có thể dẫn tới phát hiện sai trong trường hợp lưu lượng dữ liệu bị thay đổi do những yếu tố ngẫu nhiên về kênh truyền chứ không phải do tấn công. Tuy nhiên nếu khoảng giới hạn quá lớn sẽ dẫn tới việc không phát hiện được sự thay đổi lưu lượng bất thường. Ta lần lượt thay đổi mức tin cậy lần lượt là 10% 20% và 30%.



Hình 5. Tỷ lệ phát hiện tấn công lưu lượng dựa trên tỷ lệ thay đổi tốc độ gói tin và khoảng tin cậy

Trong đó:

Trục hoành biểu diễn: Tỷ lệ thay đổi tốc độ gói tin

Trục tung biểu diễn: Tỷ lệ phát hiện tấn công

a = 10%, 20%, 30% với đường cong tăng dần từ dưới lên trên.

D.Đánh giá giải pháp

Trong phần này, tôi đã đề xuất một mô hình để xác minh tính toàn vẹn của dữ liệu cảm biến, dựa trên kỹ thuật zero watermark kết hợp với xác minh tính toàn vẹn của lưu lượng dựa trên phân tích đặc tính về thời gian giữa 2 gói liên tiếp. Watermark được tạo ra trên đặc trưng của dữ liệu cảm biến như độ dài, tần suất xuất hiện và thời gian của dữ liệu cảm biến giữa các nút cảm biến. Phương pháp sử dụng chính là đặc tính của dữ liệu để tạo ra watermark (hay zero watermark) đơn giản hơn nhiều so với những phương pháp khác, ví dụ như sử dụng hàm băm để tạo watermark. Hàm băm có tính toán tốn kém và mất nhiều thời gian hơn trong quá trình tạo băm. Kết quả thực nghiệm và phân tích hiệu suất cho thấy rằng đề xuất này đạt được hiệu quả tính toán tốt hơn so với sơ đồ hiện có.

V. KẾT LUẬN

Trong phần này, tôi đã đề xuất một mô hình để xác minh tính toàn vẹn của dữ liệu cảm biến, dựa trên kỹ thuật Watermark kết hợp với xác minh tính toàn vẹn của lưu lượng dựa trên phân tích đặc tính về thời gian giữa 2 gói tin liên tiếp. Watermark được tạo ra trên đặc trưng của dữ liệu cảm biến như độ dài, tần suất xuất hiện và thời gian của dữ liệu cảm biến giữa các nút cảm biến. Phương pháp sử dụng chính là đặc tính của dữ liệu để tạo ra watermark đơn giản hơn nhiều so với những phương pháp khác, chẳng hạn như sử dụng hàm băm để tạo ra watermark. Hàm băm có tính toán tốn kém và mất nhiều thời gian hơn trong quá trình tạo băm. Kết quả thực nghiệm và phân tích hiệu suất cho thấy rằng đề xuất này đạt được hiệu quả tính toán tốt hơn so với sơ đồ hiện có.

Kỹ thuật phát hiện dựa trên phân tích lưu lượng truy cập đến từ các node cảm biến đến. Trong giai đoạn khởi tạo, khi không có kẻ tấn công nào được giả định là hoạt động trong vùng mạng cảm biến không dây (WSN), trạm gốc (BS) thu thập dữ liệu từ các nút hàng xóm và tạo dữ liệu về hành vi của nút. Trong suốt thời gian hoạt động

của mạng, khi xảy ra bất thường về kết nối thì sẽ sử dụng cách so sánh dữ liệu mới thu được với dữ liệu ban đầu. Vì phương pháp dựa trên ước tính thống kê về phân phối xác suất các thuộc tính được giám sát rất hiệu quả và đáng tin cậy. Kể từ khi kỹ thuật dựa trên các phương pháp thống kê đơn giản và không yêu cầu các mẫu lớn để ước tính các tham số, các giá trị các ngưỡng được cập nhật dễ dàng khi thay đổi môi trường hoặc ứng dụng.

Bài viết này xem xét việc phát hiện một cuộc tấn công trong WSN, khi số lượng thiết bị độc hại giảm hoặc tiêm các gói trong lưu lượng truy cập mạng. Kỹ thuật được đề xuất dựa trên giám sát tốc độ tiếp nhận gói tin và thời gian đến gói tin được ứng dụng logic fuzzy để giảm thiểu tỷ lệ dương giả và tối đa hóa tỷ lệ phát hiện. Các kỹ thuật được đề xuất có bản chất phân tán và nó có thể được sử dụng trong các mạng lớn. Nó không yêu cầu cài đặt bất kỳ phần cứng bổ sung hoặc bất kỳ chi phí liên lạc bổ sung nào. Các phương pháp đề xuất là nhẹ, hiệu quả, cho kết quả đáng tin cậy nhanh chóng, vì nó sử dụng các phương pháp thống kê đơn giản và tăng cường sức mạnh. Bài viết cung cấp đề xuất tính toán ngưỡng cho mỗi tham số. Chi phí tính toán thấp, yêu cầu bộ nhớ thấp để lưu trữ dữ liệu và thời gian trễ ngắn để tính ngưỡng cho phép thích ứng trong quá trình hoạt động của mạng thời gian.

Kết quả mô phỏng cho thấy rằng, kỹ thuật được đề xuất có tỷ lệ phát hiện cao các cuộc tấn công. Khi kẻ tấn công cố gắng hoạt động theo cách "lén lút" và giảm hoặc tiêm nhỏ một phần của các gói bất thường, vẫn sẽ được phát hiện một cách đáng tin cậy phương pháp được đề xuất, trong khi các quy tắc thường được đề xuất dựa trên giả định về sự phân bố bình thường của sự xuất hiện tỷ lệ (10, 11), cho thấy độ chính xác thấp hơn. Kết quả của sự phát hiện xâm nhập không phụ thuộc vào số lượng thiết bị độc hại.

Việc kết hợp 2 phương pháp Zero watermarking và phân tích đặc tính lưu lượng của dữ liệu cho ta một giải pháp xác thực an toàn khi có tỉ lệ phát hiện tấn công cao cùng với đó là ít tiêu tốn năng lượng tính toán của hệ thống. Trong tương lai tôi dự định sẽ nâng cao hiệu quả an ninh của mạng bằng cách phân tích những thuộc tính khác của dữ liệu cũng như lưu lượng như là: tỉ lệ gói tin nhận được (packet delivery ratio) và tỉ lệ gói tin nhận sai (bad packet ratio).

TÀI LIỆU THAM KHẢO

[1] A. S. Panah, R. v. (2015). "In the shadows we trust: A secure aggregation tolerant watermark for data streams," IEEE 16th International Symposium on a, In World of Wireless, Mobile and Multimedia Networks (WoWMoM). pp. 1-9.

[2] B. Wang, H. Q. (2015). " A Secure Data Transmission Scheme Base on Information Hiding in Wireless Sensor Networks," In International Journal of Security and Its Applications 9, No.1. pp. 125-138.

[3] B. Wang, J. S. (2015). " A Copyright Protection for Wireless Sensor Networks based on Digital Watermarking," International Journal of Hybrid Information Technology. 8, No.6. pp. 257-268.

[4] Cremers, C. (2008). The scyther tool: Verification, falsification, and analysis of security protocols. In International Conference on Computer Aided Verification; Spring: Berlin/Heidelberg, Germany. pp. 414-418.

[5] Das, M. (2009, 8). Two-Factor user authentication in wireless sensor networks. IEEE Trans. Wirel. Commun. pp. 1086-1090.

[6] I. Kamel, O. A. (2009). "Distortionfree watermarking scheme for wireless sensor networks," in International Conference on Intelligent Networking and Collaborative Systems (INCOS) . pp. 135-140.

[7] Juma, I. K. (2010). "Simplified watermarking scheme for sensor networks," In International Journal of Internet Protocol Technology 5, No.1-2. pp. 101-111.

[8] Khizar Hameed, M. K. (2016). A Zero Watermarking Scheme for Data Integrity in Wireless Sensor Networks. trang 119-126.

[9] Ko, L. (2008, October). A novel dynamic user authentication scheme for wireless sensor networks. In Proceedings of the IEEE International Symposium on Wireless Communication Systems, Reykjavik, Iceland. pp. 21-24.

[10] Kumar, P., Gurtov, A., Ylianttila, M., Lee, S., & Lee, H. (2013). A strong authentication scheme with user privacy for wireless sensor networks. ETRI J. , pp. 889-899.

[11] Kumari, S., Khan, M., & Atiquzzaman, M. (2015). User authentication schemes for wireless sensor networks: A review. Ad Hoc Netw. trang 159-194.

[12] Q. Ding, B. W. (2015). " A reversible watermarking scheme based on difference expansion for wireless sensor network," International Journal of Grid Distribution Computing Vol.8, No.2. pp. 143-154.

[13] R. X. Xiao, X. S. (2008). " Copyright Protection in Wireless Sensor Networks by Watermarking," in 8th International Conference Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP) 08. pp. 7-10.

[14] W. Zhang, Y. L. (2008). "Secure data aggregation in wireless sensor networks: a watermark based authentication supportive approach," Pervasive and Mobile Computing, vol. 4, no. 5. pp. 658-680.

[15] Wong, K., Zheng, Y., Cao, J., & Wang, S. (2006, June). A dynamic user authentication scheme for wireless sensor networks. In Proccedings of the IEEE International Conference on Sensor Networks, Ubiquitous and Trustworthy Computing, Taichung, Taiwan. pp. 5-7.

[16] X. Sun, J. S. (2013). " Digital watermarking method for data integrity protection in wireless sensor networks," International Journal of Security and Its Applications, vol.7, no.4. pp. 407-416.

[17] Xiao, X. S. (2013). "A reversible watermarking authentication scheme for wireless sensor networks," Information Sciences, vol.240. pp. 173-183.

[18] Yoo, S., Park, K., & Kim, J. (2012). A security-performance-balanced user authentication scheme for wireless sensor networks. Int.J.Distrib.Sens.Netw. 2012. pp. 10-38.

[19] Zhang, L. Z. (2012). "A secure data transmission scheme for wireless sensor networks based on digital watermarking," in 9th International Conference on Fuzzy System and Knowledge Discovery (FSKD). pp. 2097-2101.

[20] Zhou, Q., Tang, C., Zhen, X., & Rong, C. (2015, Appl). A secure user authentication protocol for sensor network in data capturing. J. Cloud Comput. Adv. Syst, pp. 4, 6.

AUTHENTICATION METHOD FOR WIRELESS SENSOR NETWORK BY WATERMARKING

Abstract: The issue of sensor network security has been an issue attracting many researchers and deploying the system before a series of new requirements and applications. In particular, the authenticity to ensure that data is not changed during transmission is a challenging issue when the number of sensor devices increases very

quickly and diversely, leading to many different binding conditions with different infrastructure already. This paper focuses on issues related to authentication in wireless sensor networks and desires to propose a watermark-based authentication solution to suit a number of wireless sensor network requirements.

Keyword: WSN, Watermarking, Authentication, Base station.

Hoàng Thị Thu, ThS (2019). Hiện công tác tại Viện Công nghệ thông tin và truyền thông CDIT. Học viện Công nghệ Bưu chính Viễn thông. Lĩnh vực nghiên cứu: IoT, WSN, Mạng di động, Blockchain, AI.