LƯỢC KHẢO VỀ BẢO MẬT TRONG MẠNG CẢM BIẾN KHÔNG DÂY

● LÊ HOÀNG ANH

TÓM TẮT:

Mạng cảm biến không dây ra đời đã góp phần quan trọng trong cuộc cách mạng công nghệ thông tin và truyền thông, với nhiều ứng dụng mạng cảm biến không dây trong các lĩnh vực, hệ thống như: hệ thống giám sát ứng dụng trong chiến trường quân đội, theo dõi các đối tượng; hệ thống theo dõi môi trường sống; hệ thống phát hiện cháy rừng và hệ thống theo dõi bệnh nhân. Do vậy, bài viết khảo sát các phương pháp bảo mật khác nhau cho mạng cảm biến không dây, các loại tấn công khác nhau và kỹ thuật tương ứng để giải quyết nhằm góp phần hạn chế các lỗ hổng, các cuộc tấn công khác nhau về bảo mật trong mạng. Từ đó, đề xuất các giải pháp và cách tiếp cận đã được đề xuất cho các lỗ hổng, các cuộc tấn công khác nhau để đảm bảo yêu cầu bảo mật.

Từ khóa: Mạng cảm biến không dây, an ninh mạng, mật mã, phát hiện xâm nhập.

I. Giới thiệu

Việc sử dụng mạng cảm biến không dây để liên lạc và xử lý dữ liệu đang phát triển nhanh chóng. Mạng cảm biến không dây được xây dựng dựa trên số lượng lớn các nút cảm biến và trạm gốc. Trạm gốc đóng vai trò là cổng kết nối vào mạng khác. Nút sink thường phục vụ cho trạm gốc. đó có thể là máy tính xách tay hoặc hệ thống máy tính thu thập thông tin và phân tích, từ đó nó đưa ra quyết định phù hợp [5]. Mạng cảm biến có thể kết hợp nhiều loại nút cảm biến khác nhau như: từ tính, nhiệt, hình ảnh, hồng ngoại và âm thanh [5]. Mỗi nút cảm biến có thể cảm biến ánh sáng, áp suất, nhiệt.... [11]. Nút cảm biến được trang bị một pin nhỏ để cung cấp năng lượng, nghĩa là hiệu suất mạng phụ thuộc rất nhiều vào tỷ lệ tiêu thụ năng lượng.

Mạng cảm biến không dây được ứng dụng trong rất nhiều lĩnh vực quan trọng như: quân sự, giám sát môi trường, chăm sóc sức khỏe, robot.... Các ứng dụng trong lĩnh vực quân sự có thể bao gồm sử dụng trong chiến trường, theo dõi các đối tượng như kẻ địch và các loại phương tiện. Mạng cảm biến không dây cũng có thể được sử dụng trong môi trường trong nhà để kiểm soát năng lượng tiêu thụ trong làm mát, chiếu sáng, khí đốt và nước [1]. Việc sử dụng mạng cảm biến không dây trong y học ngày càng trở nên quan trọng vì nhiều thiết bị y tế được trang bị chức năng cảm biến. Một số ứng dụng trong lĩnh vực này như: theo dõi nhiệt độ, theo dõi huyết áp, theo dõi lượng đường, theo dõi điện tâm đồ và theo dõi điện não đồ [6]. Mạng cảm biến không dây cũng được sử dụng trong giám sát các hiện tượng môi

trường như động đất, cháy rừng và lũ lụt. Ngoài ra, mạng cảm biến không dây còn đóng một vai trò quan trọng trong các ứng dụng động vật hoang dã và động vật học như theo dõi động vật và giám sát hành vi của động vật. Tuy nhiên, vấn đề bảo mật là một trong những yếu tố quan trọng nhất cần xem xét khi thiết kế và triển khai mạng cảm biến không dây do những hạn chế của các nút cảm biến. Hầu hết các cuộc tấn công vào mạng cảm biến không dây tương tự như các cuộc tấn công trong các mạng có dây, nhưng do những hạn chế của các nút cảm biến nên các cơ chế bảo mật trên mạng có dây khó áp dụng trên mạng cảm biến không dây. Bảo mật trong mạng nghĩa là mạng phải đảm bảo các yếu tố về bảo mật như: tính bảo mật, tính toàn vẹn và tính sẵn có của dữ liệu. Mật mã học là một trong những kỹ thuật cơ bản để bảo mật dữ liệu và thông tin. Hầu hết các phương pháp mã hóa truyền thống không phù hợp cho mạng cảm biến không dây do sự hạn chế về tính toán và năng lượng của các nút cảm biến. Do đó phải lựa chọn và đánh đổi giữa các phương pháp mã hóa khác nhau để đạt được một giải pháp bảo mật tương xứng với từng ứng dụng của mạng.

Bài viết trình bày lược khảo một số tài liệu về bảo mật trong mạng cảm biến và thảo luận về một số giải pháp bảo mật cho các loại tấn công khác nhau cùng với những điểm mạnh và điểm yếu của chúng.

2. Lược khảo tài liệu

JeongGil Ko và các cộng sự [8] đã thực hiện thuật toán mã hóa bằng AES để bảo mật dữ liệu trong mạng cảm biến không dây. Họ đã tập trung vào phương pháp khóa đối xứng dựa trên AES để mã hóa và giải mã cùng một khóa chung. Thuật toán này tạo ra bản mã bằng cách tính toán 10 vòng trong một khoảng thời gian ngắn [8].

Sekhar và Sarvabhatla [11] đã đề xuất một giao thức dựa trên mã hóa sử dụng khóa công khai để xác thực tác nhân bên ngoài và thiết lập khóa phiên. Tác nhân bên ngoài giao tiếp thông qua một khóa công khai với trạm gốc, giao tiếp với các nút cảm biến thông qua việc chia sẻ khóa bí mật. Giao thức này được chia thành ba giai đoạn: đăng ký, xác thực và thiết lập khóa phiên.

Praveena và Smys [10] đề xuất chuẩn mã hóa phiên bản II (MES V-II - Modern Encryp Standard Version-II). MES V-II là loại mã khóa đối xứng. Thuật toán này được phát t bởi Nath và các cộng sự, sử dụng thuật t TTJSA và DJSA trong phương pháp ngẫu nh (randomised method). Trong phương pháp phương pháp mã hóa Vernam tổng quát và h chỉnh sử dụng các kích thước khối khác nhau khóa khác nhau cho mỗi khối. Để tăng tính mật, thông tin phản hồi cũng được thêm vào tr phương pháp này. Sau khi hoàn thành giai đ mã hóa, toàn bộ tệp tin được chia thành hai p hoán đổi cho nhau và phương pháp mã Vernam được hiệu chỉnh với thông tin phản và một khóa mới sẽ được lặp lại. Hoạt động được lặp đi lặp lại một số lần để hệ thống có an toàn.

Theo Jain, Kant và Tripathy [4], các yếu quan trọng để đảm bảo chống lại các cuộc mạng là hệ thống phải đảm bảo các yêu tố cầu bảo mật:

- Xác thực dữ liệu: xác thực tin nhắn rất q trọng đối với các mạng cảm biến. Nghĩa là p xác minh được danh tính của tin nhắn.

- Tính toàn vẹn: điều này tập trung vào chính xác của dữ liệu để đảm bảo rằng không thay đổi nào được thực hiện bằng cách thêm, t đổi hoặc xóa thông tin trong quá trình truyền

- Bảo mật dữ liệu: điều này đảm bảo rằng kỳ thông điệp nào cũng chỉ có người gửi và ng nhận biết. Để đảm bảo điều này thường thì p sử dụng các kỹ thuật mã hóa.

- Tính khả dụng: điều này đảm bảo rằng liệu luôn có sẵn tại mọi thời điểm hoặc bất khi nào có yêu cầu. Một số cuộc tấn công mật như từ chối dịch vụ sẽ ảnh hưởng đến khả dụng của dữ liệu, nhưng nếu thiết kế m và cơ chế bảo mật yếu có thể dẫn đến không dữ liệu khả dụng.

- Độ tươi dữ liệu: điều này đảm bảo r không có tin nhắn cũ nào bị phát lại bởi kẻ công. Nhãn thời gian có thể được áp dụng để được mục tiêu này.

Navin và các cộng sự [7] đã giới thiệu mô chế bảo mật đa cấp bằng cách tạo ra một số n nhiều để mã hóa thẻ của khung. Cấp độ đầu sẽ được bắt đầu với một phương pháp xen

Cấp độ thứ hai, giá trị của một bộ tạo số giả ngẫu nhiên được khởi tạo. Cấp độ thứ ba, một ngăn hàng số được khởi tạo phân phối. Cấp độ cuối cùng được bắt đầu bằng cách áp dụng các hoạt động cho ngăn hàng số.

Biswas, Muthukkumarasamy và Singh [2] đề xuất một cơ chế mã hóa sử dụng bản đồ hỗn loạn và các hoạt động di truyền. Nó tích hợp các ưu điểm của phương pháp đường cong elip, bản đồ hỗn loạn và di truyền mã hóa để bảo mật dữ liệu. Có 3 giai đoạn để tạo thành khối mật mã như sau:

- Giai đoạn thiết lập khóa: sau khi chọn ngẫu nhiên một khóa bí mật từ nhóm khóa, bên gửi và nhận trao đổi khóa với nhau. Giai đoạn này sẽ sử dụng phương pháp đường cong elip dựa trên một trường nguyên tố để tạo ra một nhóm khóa lớn để xác thực nút.

- Tạo chuỗi bít giả ngẫu nhiên: trong giai đoạn này, chuỗi bít giả ngẫu nhiên được tạo ra bằng phương pháp bản đồ hỗn loạn.

- Quá trình mã hóa: nhầm lẫn và khuếch tán là các khái niệm chính được sử dụng trong mật mã khối. Để đạt được sự nhầm lẫn là phải đảm bảo bảo mật mối quan hệ giữa bản mã và khóa dối xứng. Mặt khác, khuếch tán đạt được bằng cách phân tán sự lặp lại của bản rõ bằng cách truyền nó trên bản mã. Ba hoạt động khác có thể được thực hiện bằng kỹ thuật mã hóa này: XOR, đột biến (mutation) và chéo (crossover).

Celestine và cộng sự [3] đã giới thiệu một kỹ thuật định tuyến chống ngập phụ thuộc vào nguồn dữ liệu giả. Ý tưởng chính của kỹ thuật này là mỗi nút có thể được coi là nguồn dữ liệu giả gửi dữ liệu thực sau khi một sự kiện cảm biến dữ liệu đến nút đích. Tất cả các nút hàng xóm sẽ nhận được dữ liệu giả. Mặc dù cách tiếp cận này có ưu điểm là gây khó khăn cho kẻ tấn công để phân biệt giữa gói thật và giả, nhưng nó tiêu tốn băng thông và tiêu thụ điện năng. Một giải pháp mới được đề xuất với việc sử dụng các gói giả. Các gói giả có kích thước khác với các gói thực, do đó tiết kiệm năng lượng. Tuy nhiên, kẻ tấn công vẫn khó phân biệt gói thực với những gói giả.

Prathap, Shenoy và Venugopal đề xuất giải pháp là bắt các nút độc hại với sự hỗ trợ tin cậy trong mạng cảm biến không dây, mục tiêu này nhắm vào các cuộc tấn công bằng nút độc hại, bao gồm sửa đổi gói, thêm gói, tấn công Sybil, gói sai và tấn công nói xấu [9]. Giải pháp này khởi tạo xử lý bằng cách tạo cây cha-con chứa thông tin liên quan trong nút ẩn. Dữ liệu được truyền theo nhiều vòng với cùng thời gian cho mỗi vòng. Nút cha được chọn bởi các nút của nó. Phương pháp hỗ trợ tin cậy trong mạng cảm biến không dây phát hiện các nút xấu sau mỗi vòng.

3. Thảo luận

Nhiều phương pháp bảo mật đã được giới thiệu trong bài viết này, giải pháp cho các loại tấn công khác nhau và các mối đe dọa ảnh hưởng đến mạng cảm biến không dây. Mặc dù những kỹ thuật này có những điểm mạnh riêng nhưng nó cũng có một số yếu điểm.

Khi xem xét công nghệ mã hóa và do bản chất của các nút cảm biến bị giới hạn về tính toán và năng lượng thì sử dụng các phương pháp khóa đối xứng như AES có những lợi thế về tốc độ, hiệu quả và bảo tồn năng lượng [8]. Mặt khác, việc thiết lập và chia sẻ khóa đối xứng cần có một kênh trao đổi an toàn.

So với mã hóa khóa đối xứng, mã hóa sử dụng khóa công khai an toàn hơn vì nó yêu cầu hai khóa: khóa chung được sử dụng để mã hóa và khóa riêng được sử dụng để giải mã [11]. Tuy nhiên, mã hóa khóa công khai đi kèm với những nhược điểm như tính toán nặng nề, chậm và tiêu thụ năng lượng cao. Một giải pháp mới cho nhược điểm này là sử dụng trạm gốc thay vì các nút cảm biến để áp dụng kỹ thuật khóa chung, trạm gốc có khả năng tính toán lớn hơn so với các nút cảm biến [11].

Chuẩn mã hóa hiện đại phiên bản II (MESV-II) được mô tả là linh hoạt và các khả năng khác, nhưng nó chỉ được sử dụng để mã hóa byte phản đoán [10]. Kỹ thuật này nên được áp dụng đối với bit để thêm độ phức tạp.

Jain, Kant và Tripathy đã cung cấp các hướng dẫn có giá trị cho các yêu cầu bảo mật, cũng như cho các cuộc tấn công và giải pháp thích hợp để giải quyết [4]. Tuy nhiên, nó thiếu tập trung vào khía cạnh thực tiễn. Đảm bảo an ninh trong mạng cảm biến không dây yêu cầu phân tích sâu hơn, thử nghiệm và đánh giá liên tục trong thực tế.

Navin và các cộng sự đã sử dụng trình tạo số ngẫu nhiên hướng dữ liệu như một cách để tăng

tính bảo mật bằng cách mã hóa thông tin ở nhiều cấp độ [7]. Tuy nhiên, kiểm tra phần cứng và phần mềm là cần thiết cho các thiết bị tạo số ngẫu nhiên để đảm bảo không có sự thỏa hiệp với bên thứ ba. Các chức năng nội bộ cũng phải được phân tích để đảm bảo số ngẫu nhiên là không thể đoán trước và không thể bị phát hiện bởi những kẻ tấn công.

Bằng cách sử dụng bản đồ hỗn loạn và các hoạt động di truyền được mô tả, mã hóa hình ảnh cũng như văn bản có thể đạt được [2]. Kỹ thuật này cung cấp các cải tiến để mức tiêu thụ năng lượng thấp và giảm nhu cầu tính toán. Tuy nhiên, sử dụng thuật toán này cũng có 2 nhược điểm: i) khi được sử dụng với các khối văn bản gốc, cần có phần đệm nếu kích thước của bản rõ nhỏ hơn kích thước khối được xác định trước; ii) cần có một kênh bảo mật để phân phối tham số khởi tạo.

Celestine đưa ra giao thức chống ngập có thể tăng cường bảo mật trong khi bảo tồn năng lượng bằng cách thêm độ phức tạp gây khó khăn cho kẻ tấn công trong việc xác định các gói thực [3]. Mặc dù có tính mới, nhưng tính chính xác và hiệu quả của giao thức này cũng như sử dụng trong các mạng cảm biến lớn và quan trọng vẫn còn chưa chắc chắn vì nó chỉ được thử nghiệm trong m mạng có kích thước hạn chế.

Prathap, Shenoy và Venugopal đề xuất h đồ hỗ trợ tin cậy để xác định các nút độc hại tỷ lệ phát hiện cao và tỷ lệ phát hiện sai thấp Tuy nhiên, nó chỉ mới tập trung vào các cuộc công liên quan đến gói tin, nhiều loại tấn c khác chưa được xem xét.

Tóm lại, khảo sát này cho thấy không có g pháp cụ thể và lý tưởng để giải quyết tất cả loại các cuộc tấn công vào mạng cảm biến khô đây. Do đó, các giải pháp nên được đánh giá tích hợp để đáp ứng mong muốn yêu cầu bảo m mà không ảnh hưởng đến hiệu suất và hiệu q

4. Kết luận

Các mối lo ngại về bảo mật trong mạng c biến không dây là do khả năng hạn chế của nút cảm biến, thiết bị được sử dụng trong nh các ứng dụng quan trọng. Qua lược khảo, đá giá và phân tích thì các nghiên cứu này đã trung vào các giải pháp bảo mật khác nhau. C giải pháp này được áp dụng chống lại các cu tấn công phổ biến vào mạng cảm biến không d và trong bài báo cũng đã chỉ ra những ưu nhược điểm của từng kỹ thuật ■

TÀI LIỆU THAM KHẢO:

1. A. H. Navin, Z. Navadad, B. Aasadi and M. Mirnia (2010). Encrypted Tag by Using Data-Oriented Random Number Generator to Increase Security in Wireless Sensor Network. *2010 International Conference on Computational Intelligence and Communication Networks*, (pp.335-338). Bhopal, India:

2. A. Jain, K. Kant and M. R. Tripathy (2012). Security Solutions for Wireless Sensor Networks. *2012 Second International Conference on Advanced Computing & Communication Technologies*, (pp.430-433). Rohtak Haryana, India

3. A. Praveena and S. Smys (2016). Efficient cryptographic approach for data security in wireless sensor network using MFS V-U. *2016 10th International Conference on Intelligent Systems and Control (ISCO)*, 2016 (pp.1-6 Coimbatore, India.

4. J. Celestine, K. Vallepalli, T. Vinayaraj, J. Almotiri and A. Abuzneid (2015). An energy efficient flooding protocol for enhanced security in Wireless Sensor Networks. *2015 Long Island Systems, Applications and Technology* (pp.1-6). Farmingdale, NY, the US

5. J. Ko, C. Lu, M. B. Srivastava, J. A. Stankovic, A. Terzis and M. Welsh (2010). Wireless Sensor Networks for Healthcare. *Proceedings of the IEEE*, 98(11), pp. 1947-1960. DOI: 10.1109/JPROC.2010.2065210.

6. K. Biswas, V. Muthukkumarasamy and K. Singh (2015). An Encryption Scheme Using Chaotic Map and Genetic Operations for Wireless Sensor Networks. *IEEE Sensors Journal*, 15(5), pp. 2801-280. DOI: 10.1109/JSEN.2014.2380816.

7. Kifayat K., Merabti M., Shi Q., Llewellyn-Jones D. (2010). Security in Wireless Sensor Networks. In Tavroulakis P., Stamp M. (eds), *Handbook of Information and Communication Security* (pp.513-552). Heidelberg, Germany: Springer. DOI: https://doi.org/10.1007/978-3-642-04117-4_26

8. M. Panda (2015). Data security in wireless sensor networks via AES algorithm. *2015 IEEE 9th International Conference on Intelligent Systems and Control (ISCO)*, 2015 (pp.1-5). Coimbatore, India.

9. T. Arampatzis, J. Lygeros and S. Manesis (2005). A Survey of Applications of Wireless Sensors and Wireless Sensor Networks, Proceedings of the 2005 IEEE International Symposium on. *Mediterrean Conference on Control and Automation Intelligent Control, 2005* (pp.719-724). Limassol, Cyprus

10. U. Prathap, P. D. Shenoy and K. R. Venugopal (2016). CMNTS: Catching malicious nodes with trust support in wireless sensor networks. *2016 IEEE Region 10 Symposium (TENSYMP), 2016* (pp.77-82). Bali, Indonesia.

11. V. C. Sekhar and M. Sarvabhatla (2012). Security in Wireless sensor networks with public key techniques. *International Conference on Computer Communication and Informatics, 2012* (pp.1-16). Coimbatore, India

Ngày nhận bài: 8/4/2020
Ngày phản biện đánh giá và sửa chữa: 18/4/2020
Ngày chấp nhận đăng bài: 28/4/2020

Thông tin tác giả:
ThS. LÊ HOÀNG ANH
Khoa Công nghệ thông tin
Trường Đại học An Giang, Đại học Quốc gia thành phố Hồ Chí Minh

A SURVEY ON SECURITY IN WIRELESS SENSOR NETWORKS

● Msc. **LE HOANG ANH**
Faculty of Information Technology,
An Giang University, An Giang, Vietnam
Ho Chi Minh City Vietnam National University, Vietnam

ABSTRACT:

The emergence of wireless sensor networks (WSNs) is considered one of the most important revolutions in the field of information and communications technology with many WSNs applications such as surveillance systems, battleground applications, object tracking, habitat monitoring, forest fire detection and patient monitoring. This paper surveys different security approaches for WSNs, and examines various types of attacks and corresponding techniques for tackling these, thereby proposing solutions to strengthen the security in WSNs.

Keywords: Wireless sensor networks, network security, cryptography, intrusion detection.