2014 7th International Conference on Advanced Software Engineering & Its Applications

A Survey on Encryption Schemes in Wireless Sensor Networks

Haythem Hayouni[1], Mohamed Hamdi[1], Tai-Hoon Kim[2]
[1]School of Communication Engineering (Sup'Com) University of Carthage, Tunisia
[2]Dept. of Convergence Security, Sungshin W. University, South Korea
{hayouni.haythem, mmh}@supcom.rnu.tn,taihoonn@daum.net

Abstract

As Wireless Sensor Networks (WSN) continue to grow, so does the need for effective security mechanisms. Enhancing the efficiency of these networks requires more security to provide integrity, authenticity and confidentiality of the data flowing through the network. Encryption is one of the most common tools used to provide security services for WSNs. There has been an enormous research potential in the field of encryption algorithms in WSNs. Algorithms, protocols, and implementations consist the main aspects the security specialist should consider to assess the efficiency of the protection approaches. In this survey, we review the most significant approaches that have been proposed to provide encryption-based security services for WSNs. We also emphasize on the weaknesses of these approaches.

Keywords

Wireless sensor networks, security, encryption.

I. Introduction

A wireless sensor network A (WSN)[1] is a wireless network composed of a large number of sensor nodes. A WSN consists of sensor nodes that capture information from an environment, processing data and transmitting them via radio signals. Preserving privacy in data transmission in WSN is challenging, since this type of network allows remote access, where data *encryption* [2] is an important aspect of applying *security*. Sensor networks are typically characterized by limited power supplies, low bandwidth, small memory sizes and limited energy. This leads, to a very demanding environment to provide security [3]. In addition, there are many attacks designed to exploit the unattended operation of wireless sensor networks. However, several obstacles make the achievement of the objectives of security, not trivial in wireless sensor networks: the very limited resources, wireless communication and tight coupling with the environment. Therefore, attacker can extract cryptographic information of sensor nodes. As the mission of a WSN is usually unattended, the potential attack nodes, retrieve the contents or inject erroneous data is important. Because sensor networks are controlled remotely, it is also very difficult to know whether the sensor node has been physically manipulated or reprogrammed. In many WSNs, the confidentiality of data is often critical since the information transmitted by a sensor node may contain private information, such as the health condition of a patient. For this purpose, we focus on exploring cryptographic algorithms and schemes for the basic communication behavior of a sensor node.

The data encryption algorithms used in WSNs are generally divided into three major categories [4-6]:*symmetric-key* (or private-key) *algorithms* (AES, RC6, Skipjack), *asymmetric-key* (or public-key) *algorithms* (Elliptic curve, RSA), and *hash algorithms*. When using public keys, the source node simply encrypts data using the public key of the sink node. In this case, only the sink node can correctly decrypt the data. Private Key algorithms are based on symmetric key encryption because both communicating nodes use the same keys for encrypting and decrypting data. Due to limitations of WSNs, it was believed that the public key cryptography was not suitable for WSNs because it was required high processing power, but through studies of encryption algorithms based on *c elliptic urves* was verified the feasibility of that technique in WSN. We are interested in this survey in the study of the encryption algorithms applied to sensor networks.

The reminder of this paper is organized as follows. Section 2 details the requirements for the sensor network security. Section 3 includes literature survey of various encryption approaches in wireless sensor networks, and presents their limits. Finally, Section 4 concludes the paper.

II. Security in wireless sensor network: Issues and Goals

A. Security requirements

To determine the safety objectives it will know what to protect. Sensor networks share some features of mobile ad hoc networks, but also have specific properties discussed above. So the security objectives include those of traditional networks and objectives from the constraints inherent to WSN. Among the main objectives of safety in WSN [7][8], we consider:

978-1-4799-7761-1/14 $31.00 © 2014 IEEE
DOI 10.1109/ASEA.2014.14

Authentication The most obvious need is authentication: for example, a node needs to know and verify the legitimacy of the node which tries to establish a connection with him. Therefore, authentication is a fundamental mechanism for access control in the network. If authentication is mismanaged, an attacker can join the network and inject the wrong messages.

Confidentiality Its means keeping information secret from unauthorized parties. Once authenticated parties, confidentiality is an important point, because given the wireless communication of WSN. It is to preserve the secret of the exchanged messages and not reveal to the opponents.

Integrity It ensures that data received where not altered during transit of the network. This may be achieved through the use of cryptographic hash functions which allow obtaining a hash value for each message.

Freshness This service ensures that data transferred over the network are recent and are not a reinjection of previous exchanges intercepted by an attacker. The idea is to include a monotonically increasing counter with every message and reject messages with old counter values, where every recipient must maintain a table of the last value from every sender it receives.

Availability It means that the network is available to provide services and to authorize the communicating parties. This property is difficult to ensure in WSN given the constraints on these networks, namely: dynamic topology, limited resources of transit nodes, wireless communications can easily be disturbed.

B. Attacks in wireless sensor networks

WSN may be a large number of attacks, each with own goals. We discuss in the following the most famous attacks in WSNs [9].

Sybil Attacks In this attack, a malicious node can claim different identities to participate in distributed algorithms such as the election and take advantage of the legitimate nodes. A malicious node may be able to determine the outcome of any vote by vote all its multiple identities for the same entity. The authentication and encryption algorithms can prevent a foreign launch a Sybil attack on the sensor network.

Denial of Service Attacks Denial of Service is denials as malfunctioning sensors by malicious action. Denial of service may not be the result of an attack, but a simple event that prevents the normal functioning of its services. A simple denial of service is to prevent the normal operation of the sensor victim by sending a lot of unimportant messages, and denying access to other users.

Physical Attacks As WSN are often deployed in areas without any protection, they are very vulnerable to physical attacks. Under these conditions, an attack will aim to recover the cryptographic hardware such as keys used for encryption. Another objective would be to reprogram the sensor to disrupt the network and the application voluntarily causing abnormal behavior of the node.

Data corruption attacks The attacker repeat, delay or alter the content of messages in transit. Messages can contain data collected perception and configuration data or routing. These types of attacks are among others to create loops, or draw him away from the traffic, generate false errors.

III. Existing encryption algorithms for wireless sensor networks

In this section, we present some encryption algorithms, in the literature, that aim to improve data security and discuss their limits. In [11], the authors present an identity-based key agreement and encryption scheme *IDKE* for wireless sensor networks. The scheme is an elliptic curve cryptography type algorithm. The algorithm is composed of three phases: initialization, encryption and decryption. In the initialization phase, the algorithms determined all public parameters and private keys, and contribute them to sensors. The algorithm uses a function to get all system-wide parameters. Among these parameters, there are four hash functions. Then, the algorithm determines the private keys. The public key could be an arbitrary string. The private key will be distributed to a sensor. In [12], the authors have proposed an scalable encryption algorithm *SEA* in use for a secure communication in WSNs, which is based on symmetric block cipher approach, are small memory size, small code size, and limited instruction set. SEA uses basic bit operations such as XOR, bit/word rotations, modular addition, and s-box. This algorithm is an improvement of both AES and RC6 algorithms [30], in fact, it has very flexible structure. It can operate on different plaintext and key sizes. In addition, SEA has Feistel structure with variable number of rounds. It uses 144-bit key sizes (128-bit in AES and 128-bit in RC6) with 134 rounds (10 in AES and 20 in RC6). The results obtained show that SEA has better performance than AES and RC6 in respect of memory requirements and bandwidth. In [13], the authors address the problems of symmetric and asymmetric encryption, which have security limitations in WSN. However, the authors propose a *hybrid-encryption* algorithm *HEA* where elliptical curve cryptography (ECC) [31] and advanced encryption standards (AES) are combined and operated with the same key size of ECC, to provide node authentication and secure key exchange. In this hybrid encryption method the sensitive information which has to be secured will be first encrypted by the AES algorithm. This encrypted information will be then act as the input for the

ECC algorithm. This cipher will be sent from the source node to the receiver node. The receiver will first decrypt the information using the ECC algorithm and then decrypts the same information with the AES algorithm. The security offered by this hybrid encryption is also very high. In [14], the authors evaluate a *chaos* algorithm, which is an improvement of the AES algorithm, in WSN. The algorithm is based on the essential functions of the encryption/decryption operation. This function takes as an entry 128 bytes of data. In [15], the authors have proposed an effective mechanism *DES-Blow* using a combination of DES and Blowfish [10] in CBC mode for security enhancement which provides high data confidentiality and authentication.The results show the Blowfish algorithm is strong enough to break. As using Block cipher encryption it is hard to break the security by intruder as compare to that of stream cipher. Also CBC block cipher mode of operation is most efficient as it effectively scrambles the plaintext prior to each encryption steps.

In [16], the authors present a lightweight high-level encryption algorithm *IAES* for Wireless Sensor Network. The algorithm conducted a variety of improvements form AES, mainly in three areas. At first, fewer algorithm rounds from 10 to 7; secondly, the polynomial coefficients transformation in Mix Column operations; finally, utilization of polynomial generator of the finite field designs and implements a look-up table methods to improve the speed multiplication of polynomial. The authors compare the performance of this algorithm with AES algorithm. The results obtained show that SEA has better performance than AES in respect of security requirements. In [17],the authors propose a new embedded encryption algorithm *AEEA*. The algorithm is only composed by some basic operations such as the XOR and the data to be encrypted is divided into several texts. The encryption algorithm is realized in four steps. In [18], the authors present a *Tiny Dragon* encryption algorithm for wireless sensor networks. In Tiny Dragon, a cipher that uses an 80- bit key in conjunction with a 34-byte state to provide joint encryption and authentication for messages of any length. Tiny Dragon uses an invertible 48-to-48 bit mapping F that produces output from a given input. In addition, the authors integrate the Message Authentication Code (MAC) [32] component that has no practical limit on message size. Compared with other algorithm, the performance results show that Tiny Dragon has a greatly improved per-bit security and is more suitable for WSN.

In [19], an encryption scheme and efficient key agreement *EKAES* for wireless sensor networks is proposed. EKAES is executed in four steps. The first step defines setup system parameters, where the base station run the initialization phase and distributes all the parameters to nodes. When a new sensor is needed to add or to replace one node in a network, the base station completes the initialization process and puts it into the networks. This enhances effectively the security of the sensor networks. In [20], the authors propose a robust and secure encryption scheme called *LWT-PKI*. This scheme uses public key encryption only for some specific tasks as session key setup between the base station and sensors giving the network an acceptable threshold of confidentiality and authentication. LWT-PKI tries to solve the problem of security in WSN by the use of public key cryptography as a tool for ensuring the authenticity of the base station. In [21], a dynamic encryption algorithm *DEA* to provide security to the wireless sensor network by securing the individual nodes of the network is proposed. This scheme uses a symmetric encryption with a 64-bit block length, 128-bit key length and 32 rounds iterative structure. In [22], this paper we have presented a Public Key encryption scheme *PKES* for wireless sensor networks is presented. The scheme tries to solve the problem of security in WSN by the use of public key cryptography as a tool for ensuring the authenticity of the base station. In [23], the authors propose a compact encryption algorithm *CEA*, which adopt minor encryption rounds, longer encryption key, improved ciphertext iteration algorithm and cycle-exchange method to generate child-key. In [24], the authors propose an encryption data aggregation *RSAED*.The goal of this scheme is to guarantee the essential security needs with various aggregation [25] functions (sum, average, max, min etc.). In this scheme, base station starts the sensing process by sending a broadcast message to those sensor nodes which are located in the area of interest. Sensor nodes then report back with their readings to the base station through aggregator. Aggregator then processes the received readings of sensors. In [26], a secure end-to-end encrypted-data aggregation scheme *SEDA* is proposed. It is based on elliptic curve cryptography [10] that exploits a smaller key size, which using elliptic curve does not demand high keys sizes. This approach supports homomorphic properties [27], which gives us the ability to execute operations on values even though they have been encrypted. In [28], a secure encrypted data aggregation scheme *EDAS* is proposed. The main EDAS is to eliminate redundant sensor readings without using encryption and maintains data secrecy and privacy during transmission. There are two phases in EDAS: data encryption phase and data aggregation phase. The encryption phase provides an encryption algorithm that supports data aggregation property [33]. EDAS uses random keys to encrypt data and uses only XOR operations and an irreversible hash function in encryption.

IV. Conclusion

As WSNs grow in capability and are used more frequently, the need for security in them becomes more apparent. In this paper, we reviewed the schemes proposed for securing data transmission with encryption in WSNs. We also discussed the limitations of these schemes and present the open problems that we believe need to be addressed for the problems of WSN security. Indeed, the selection of the appropriate encryption algorithm depends on the processing capability of sensor nodes,

indicating that there is no unified solution for all sensor networks. In addition, Network security for WSNs is still a very fruitful research direction to be further explored.

Some future trends in WSN security research are identified such as the exploitation of new powerful encryption techniques compared to previous approaches, such as *homomorphic encryption* and *data aggregation*. However, the previous algorithms are still very expensive to realize in sensor nodes and do not always cause powerful security. For this reason, it would be interesting to propose a new homomorphic encryption schemes to enhance the level of WSN security.

References

1. I.F.Akyildiz, W.Su, Y.Sankarasubramaniam, and E.Cayirci,"Wireless Sensor Networks: A Survey," *Elsevier Computer Networks*, volume 38, Issue 4, pp. 393-422, March 2002.
2. Y.W.Law, J.M.Doumen, and P.H.Hartel, "Bench-marking block ciphers for wireless sensor networks," *1st IEEE Int. Conf. on Mobile Ad-hoc and Sensor Systems (MASS)*, page electronic edition, Fort Lauderdale, Florida, *IEEE Computer Society Press*, Los Alamitos, California,Oct 2004.
3. E.Sabbah, and K.D.Kang,"Security in Wireless Sensor Networks," *Guide to Wireless Sensor Networks, Computer Communications and Networks*, pp. 491-512, Springer London, 2009.
4. T.C.Aysal, and K.E.Barner,"Sensor data cryptography in wireless sensor networks," *IEEE Trans.Inf.Forensics Security*, vol.3, no.2, pp. 273-289,2008.
5. P.Ganesan, and all. ,"Analyzing and Modelling Encryption Overhead for sensor Network Nodes," *2nd ACM International Conference on Wireless Sensor Networks and Applications*,2003.
6. K.Gupta, and S.Silakari,"ECC over RSA for Asymmetric Encryption: A Review," *International Journal of Computer Science Issues (IJCSI)*,Vol.8 Issue 3, pp. 370-375, 2011.
7. J.P.Walters, and all.," Wireless Sensor network security: A survey," *Security in Distributed, Grid, and Pervasive Computing, Auerbach Publications*, CRC Press, pp. 1-49, 2007.
8. X.Guo, and J.Zhu,"Research on security issues in Wireless Sensor Networks," *EMEIT*, pp. 636-639, 2011.
9. G.Padmavathi, and D.Shanmugapriya,"A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks," *(IJCSIS'09) International Journal of Computer Science and Information Security*, Vol.4, No.1&2, 2009.
10. Q.CHEN, Z.TANG, Y.LI, Y.NIU, and J.MO,"Research on Encryption Algorithm of Data Security for Wireless Sensor Network," *Journal of Computational Information Systems* , pp. 369-376, 2011.
11. G.Yang, C.Rong, C.Veigner, J.Wang, and H.Cheng,"Identity-Based Key Agreement and Encryption For Wireless Sensor Networks," *IJCSNS International Journal of Computer Science and Network Security*, VOL.6 No.5B, pp. 182-189, May 2006.
12. M.Cakroglu,C.Bayilmis,A.T.Ozcerit,and O.Cetin,"Performance evaluation of scalable encryption algorithm for wireless sensor networks," *Scientific Research and Essays*,Vol.5(9),pp. 856-861,4 May,2010.
13. A.R.Ganesh,"An improved AES-ECC hybrid encryption scheme for secure communication in cooperative diversity based Wireless Sensor Networks ," *International Conference on Recent Trends in Information Technology (ICRTIT'2011)*, pp. 1209 - 1214, India, 2011.
14. I.Mansour, G.Chalhoub, and B.Bakhache,"Evaluation of a Fast Symmetric Cryptographic Algorithm Based on the Chaos Theory for Wireless Sensor Networks," *the 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom'2012)*, pp. 913-919, June 2012.
15. G.Kumar, M.Rai, and G.Lee,"Implementation of Cipher Block Chaining in Wireless Sensor Networks for Security Enhancement,"*International Journal of Security and Its Applications*, Vol.6, January 2012.
16. Q.Chen, Q.Y.Chen, M.Yao, and J.Mo,"Design of encryption algorithm of data security for Wireless Sensor Network," *International Conference on Electrical and Control Engineering (ICECE'2011)*, pp. 2983-2986, Sept 2011.
17. L.Wei, X.Jianbo, T.Mingdong, and H.Li,"A New Embedded Encryption Algorithm for Wireless Sensor Networks," *International Forum on Information Technology and Applications (IFITA'09)*, Vol.1, pp. 119-122, May 2009.
18. M.Henricksen,"Tiny Dragon - an Encryption Algorithm for Wireless Sensor Networks," *10th IEEE International Conference on High Performance Computing and Communications (HPCC'08)*, pp. 795-800, Sept 2008.
19. C.Hongbing, Y.Geng,"EKAES: An efficient key agreement and encryption scheme for wireless sensor networks," *Journal of Electronics (China)*, Vol.25, pp. 495-502, 2008.
20. J.Lokesh, E.Munivef,"Design of Robust and Secure Encryption Scheme for WSN using PKI (LWT-PKI)," *First International Communication Systems and Networks and Workshops (COMSNETS'09)*, pp. 1-2, 2009.
21. N.Mukherjee,"A Dynamic Cryptographic Algorithm To Provide Nodal Level Security In Wireless Sensor Net-

work," *International Conference on Innovative Computing, Communication and Information Technology (CICC-ITOE'2010)*, pp. 189-194, 2010.
22. X.Chungen Xu, G.Yanhong,"The Public Key Encryption to Improve the Security on Wireless Sensor Networks," *Second International Conference on Information and Computing Science (ICIC '09)*, Vol.1, pp. 11-14, May 2009.
23. H.Hua.Wu, C.W.Lu, Z.Y.Liu,"A Compact Encryption Algorithm Suited for Resource-Restrained WSNs," *Journal of Information Technology Applications in Industry*, pp. 849-852, December 2012.
24. M.Boudia, O.Rafik , and F.Mohamed,"RSAED: Robust and Secure Aggregation of Encrypted Data in Wireless Sensor Networks," *International Journal of Network Security and Its Applications (IJNSA)*, Vol.4, November 2012.
25. N.S.Patil, P.R.Patil,"Data Aggregation in Wireless Sensor Network," *International Conference on Computational Intelligence and Computing Research*, 2010.
26. J.M.Bahi, C.Guyeux, and A.Makhoul,"Efficient and Robust Secure Aggregation of Encrypted Data in Sensor Networks," *Fourth International Conference on Sensor Technologies and Applications (SENSORCOMM'10)*, pp. 472-477, Italy, July 2010.
27. B.Patel,D.Jinwala,"Exploring Homomorphic Encryption in Wireless Sensor Networks," *International Conference on Informatics Engineering and Information Science (ICIEIS'2011)*, pp. 400-408,2011.
28. S.I.Huang, S.Shieh, and J.D.Tygar,"Secure encrypted-data aggregation for wireless sensor networks," *Published in Journal of Wireless Networks*, Vol.6, pp. 915-927,May 2010.
29. J.Lee, K.Kapitanova, and S.H.Son,"The price of security in wireless sensor networks," *The International Journal of Computer and Telecommunications Networking*, pp. 2967-2978, December 2010.
30. G.Guimaraes, E.Souto, D.Sadok, and J.Kelner,"Evaluation of Security Mechanisms in Wireless Sensor Networks," *Proceedings of the Systems Communications*, pp. 428-433, 2005.
31. A.R.Mishra, M.Singh,"Elliptic Curve Cryptography (ECC) for Security in wireless Sensor Network," *International Journal of Engineering Research and Technology (IJERT)*, Vol.1, May 2012.
32. R.Tahir, M.Y.Javed, and A.R.Cheema,"Rabbit-MAC: Lightweight Authenticated Encryption in Wireless Sensor Networks," *International Conference on Information and Automation (ICIA'2008)*, pp. 573-577, June 2008.
33. J.Karaki, R.Mustafa, and A.Kamal,"Data aggregation in wireless sensor networks - exact and approximate algorithms," *In Proceedings of the Workshop on High Performance Switching and Routing*, pp. 241-245, 2004.
34. V.Jariwala, D.Jinwala,"Evaluating Homomorphic Encryption Algorithms for Privacy in Wireless Sensor Networks," *International Journal of Advancements in Computing Technology*. Vol.3, pp. 215-223, 2011.
35. M. Sliti, M. Hamdi, N. Boudriga"An Elliptic Threshold Signature Framework for k-Security in Wireless Sensor Networks," *15th IEEE ICECS,.*, 2008..