Lightweight Authentication System for Software-Defined Wireless Sensor Networks

Amado Illy[1](✉), Youssou Faye[2], and Tiguiane Yelemou[1]

[1] Université Nazi BONI, Bobo Dioulasso, Burkina Faso
amedilly65@gmail.com
[2] Université Assane Seck de Ziguinchor, Ziguinchor, Senegal
yfaye@univ-zig.sn

Abstract. Sybil attack consists to generate several false identities in order to bypass access control and thus produce false messages to seriously undermine the normal operation of Wireless Sensor Networks (WSN). It is considered one of the major threats to WSNs. The problem has been widely taken into account by researchers. However, detecting this attack and effectively countering it in the context of resource-constrained connected objects remains a challenge. In this paper, we propose a lightweight authentication system based on elliptic curve cryptography to counter this attack. This asymmetric encryption system uses smaller encryption keys than RSA and EL-Gamal, but offers the same level of security.

Keywords: Resource-constrained networks · Sybil attack · Authentication · Elliptic curves

1 Introduction

A Wireless Sensor Network (WSN) is a group of nodes which main function is to collect information about its environment and transmit it to a server for further processing. These nodes may be used in a multi-hop context, where each node plays the role of collector for its own environment and router for others neighboring peers. Ease of deployment of this type of network is an asset, enabling them to be easily integrated into a variety of application domains such as environmental monitoring, home automation, industry, etc. [1]. For reasons of concealment and cost, these nodes are often small in size. Their capacities, notably in terms of computing power, memory, storage and energy, are therefore limited. These constraints have a negative impact on the ability of these nodes to support robust security mechanisms or quality of service [2–4]. The aim of new proposals and protocols dedicated to (WSN) is to make a compromise between the security and quality of service provided by these solutions and the resource constraints of these nodes [5, 6]. In this context, an efficient security key management mechanism is a major asset for the smooth operation of these networks. In this paper, we propose an efficient authentication solution based on elliptic curve cryptography. This solution integrates efficient security key management to face Sybil attack. This protocol is less power-hungry and easy to

A. Sere et al. (Eds.): AFRICOMM 2023, LNICST 587, pp. 155–162, 2025.
https://doi.org/10.1007/978-3-031-81570-6_10

implement in WSN. The remainder of the manuscript is organized as follows. In Sect. 2, we present the Sybil attack and highlight previous work concerning proposed solutions to counter this attack. In Sect. 3, we present our lightweight authentication approach. In Sect. 4, we present results of a performance evaluation of our approach. Finally, we conclude in Sect. 5.

2 Related Works

In many cases, sensors in a network must cooperate to perform tasks. New sensors can use the identities of other legitimate sensors, defining Sybil attacks, which degrade data integrity, security and resources availability. Sybil attacks target routing mechanisms, resource allocation, data aggregation, privileged node election, distributed storage and misbehavior detection [7, 8]. While all ad hoc networks are vulnerable to Sybil attacks, WSNs can be protected using appropriate protocols. In the absence of a central authority, a Sybil attack is easy to carry out, unless large resources are used. However, detecting Sybil attacks is difficult. In the Sybil attack, malicious node has several identities and can appear in several places at the same time, and the probability of selecting such false sensors is high, leading to a reduction in the quality assurance provided by the multi-hop protocol [9]. As a rule, protocols assume a sensor have unique key, and since a central element of Sybil attacks is identity theft, authentication is the main defence. A trusted key server or base station can authenticate a sensor for other sensors on the network. If a unique key is used, the discovery of this key is critical for the whole network [10, 11]. In the field of WSN, the issue of Sybil attacks has been widely explored by researchers.

In [12], the authors propose a new strategy based on machine learning to detect spoofing attacks in wireless sensor networks. The proposed algorithm combines two classifiers to process and analyse instantaneous strength samples of the received signal to detect attacks. This solution is suitable in the context of WSN, but does not take into account all possible cases related to impersonation attacks. It is optimized for scenarios where the legitimate node and the malicious node are at the same distance or very close to each other in relation to the landmark.

Shantala Devi Patil et al. [13] have proposed a security solution to thwart impersonation attacks and node compromise in a WSN. They have implemented an authentication mechanism called PAW (Provisioning authentication on demand in WSN). This solution is based on the authentication of external users wishing to access network resources. The proposed PAW system is divided into four phases: The preparation phase, carried out by the base station, which is the point of contact for external network users. The registration phase, in which users and cluster leaders register with the base station. In the authentication phase, a three-stage authentication is performed and a session key is established between the user and the cluster leader to secure data exchanges. In the final phase, a common session key is generated for the user and the cluster leader. Due to the resource constraints of WSN, this authentication solution is effective, but its complexity induces a high energy consumption. Authentication and establishment of the session key between the sensor nodes and the user is made up of several hash operations.

In [14], the authors proposed a protocol for sensor node authentication and key distribution. This solution makes it possible to combat impersonation attacks and modification or replay of routing information in a WSN. The protocol consists of five steps:

The first consists of exchanging neighbor discovery information. The next step establishes a well-to-well relationship. The third step involves sharing group authentication keys, followed by initial node authentication. The final step involves re-authenticating the nodes. This solution can counter several types of attack, but its authentication process is very time-consuming. The number of messages exchanged in this protocol is high, generating high energy consumption.

Neha Badetia et al. [15] have proposed a distributed mechanism for authenticating nodes in WSN. Sensor nodes are logically arranged as a binary tree with the base station. A token is generated by the parent node for its child node. This token is then used by a child node for mutual authentication of the sensor nodes. This algorithm comprises two phases: a registration phase and an authentication phase. During the registration phase, each parent node generates a token for its child node, and these tokens are then used by the nodes for mutual authentication. The token contains the node's identity, public key, pseudo-random number and lifetime. This solution has a good level of security, but the amount of information stored in sensor nodes using this protocol is high. The nodes don't have enough resources and their storage capacity is limited.

Aishwarya Vardhan et al. [16] have proposed a mutual node authentication scheme that promotes secure exchange between sensor nodes. This solution combats identity theft attacks. It is based on double encryption of identification data, using both symmetric and asymmetric encryption algorithms. This solution offers an acceptable level of security, but the encryption mechanisms used generate high energy consumption. The asymmetric encryption algorithm is one of the most energy-intensive. The encryption process for this algorithm requires very high computing power.

Most of the proposed solutions, even if they provide acceptable security, are energy-intensive and provide significant system resources. They are thus unsuited to the context of resource-constrained networks.

3 Proposed Solution

In this section, first we present a network context and the threat and then the components of the solution.

3.1 Network Functional Architecture and Threat Presentation

3.1.1 Functional Architecture of the Network

Our architecture consists of an SDN controller, a base station and a set of nodes deployed in the observation environment. In our architecture, a sensor node collects data in its surrounding environment and transmits it to the base station. The base station receives the data collected in the field of observation. It uses the controller in the background to ensure the authenticity of the sensor nodes and the integrity of the data received. The controller is responsible for managing and authenticating each sensor node wishing to join the network.

3.1.2 Presentation of the Threat

In the sybbil attack, for the case of our architecture, a malicious node uses several identities simultaneously or non-simultaneously to disrupt network operation. By using multiple identities, an attacker can take control of the network and consequently carry out different types of attack. It can also bypass a decision on a particular agreement. Communications take place in a one-hop neighborhood, so it's not possible for an attacker to replay, and nodes won't need to decipher certain message fields to perform routing.

3.2 Our Solution Presentation

We propose an authentication system based on elliptic curve cryptography. This is an asymmetric encryption system, using smaller key sizes than other cryptographic algorithms, but offering the same level of security. The controller generates two keys for each node, a public key and a symmetric key, before deployment. Node identifiers are supplied by the provider. A range of identifiers is provided for a large number of nodes. This range of node identifiers will be stored at the base station before the nodes are deployed. The controller is also responsible for generating the elliptic curve parameters. Initially, the controller selects an elliptic curve EC over a finite field Fq and opts for a base point P with large order p (where p and q are prime numbers). The controller then makes it public to the base station, which in turn transmits it to all the sensor nodes in the network. The implementation of our authentication solution comprises three phases (see Fig. 1): first, registration phase, which consists of gathering the security identification information for each node. This information will be used during the authentication phase. The second, called the authentication phase, enables communication to be initiated between the sensor node and the controller based on the security credentials obtained. The third, called the re-authentication phase, requires sensor nodes that have been in standby mode for a long period to re-authenticate.

3.2.1 Registration Phase

Before launching the authentication process between two network entities, it is necessary for each part of the communication to go through a registration process in order to provide security credentials that will be used for the authentication phase. We will now illustrate the message flows exchanged during the registration and authentication phases. The registration phase takes place in three (03) stages.

Step 1: the sensor node sends a registration request to the controller via the base station. The message contains the symmetrical key, encrypted using the controller's public key. The encrypted message is concatenated with the node ID before being sent.

Step 2: on receipt, the base station checks the node's identity against the identity stored at its level. If this is the case, the base station forwards the encrypted message to the controller.

Step 3: After receiving the message from the base station, the controller first verifies the certificate, then decrypts the node's message using its private key to check the conformity of the key stored at its level. After verification, the controller will retransmit a new symmetrical key for the sensor node, which will be used during the authentication phase. This new key will be encrypted with the node's public key and transmitted to the

base station, which in turn transmits it to the sensor node. On receipt, the node decrypts the message and checks that it has been registered when it has the new symmetrical key.

3.2.2 Authentication Phase

Step 5: when the node wants to authenticate, it generates a random number N1 using the elliptic curve parameter. It then encrypts this value using the new symmetrical key. The encrypted message is concatenated with the node ID, and the whole set is signed using the node's private key. It sends the set to the base station.

Step 6: on receipt, the base station checks the signature and the node ID. It then forwards the encrypted message to the controller.

Step 7: the controller decrypts the message and replies to the node, returning the N1 value concatenated with a new N2 value it generates. The message is encrypted using the new symmetrical key and transmitted to the base station.

Step 8: the base station transmits the encrypted message to the node.

Step 9: the node must send back the N2 value encrypted with the new symmetrical key to be authenticated.

Step 10: the base station transmits the encrypted message to the controller to complete the authentication process. By receiving the N2 value, the controller is certain that the node is not malicious and can be trusted.

3.2.3 Re-authentication Phase

This phase forces sensor nodes that have been in standby mode for a long time to re-authenticate (Table 1).

Table 1. Scoring table.

Symbols	Description
EpubC	Controller public key
EpubN	Node public key
EprivN	Node private key
CS	Symmetric key
ECso	New symmetric key
N1	Random number
IDN	Node identity
||	Concatenation operator
Certif	Certificate

4 Analytical Evaluation

In this section, we present an analytical assessment of the security level of our protocol in the face of attacks and certain security constraints defined in WSNs.

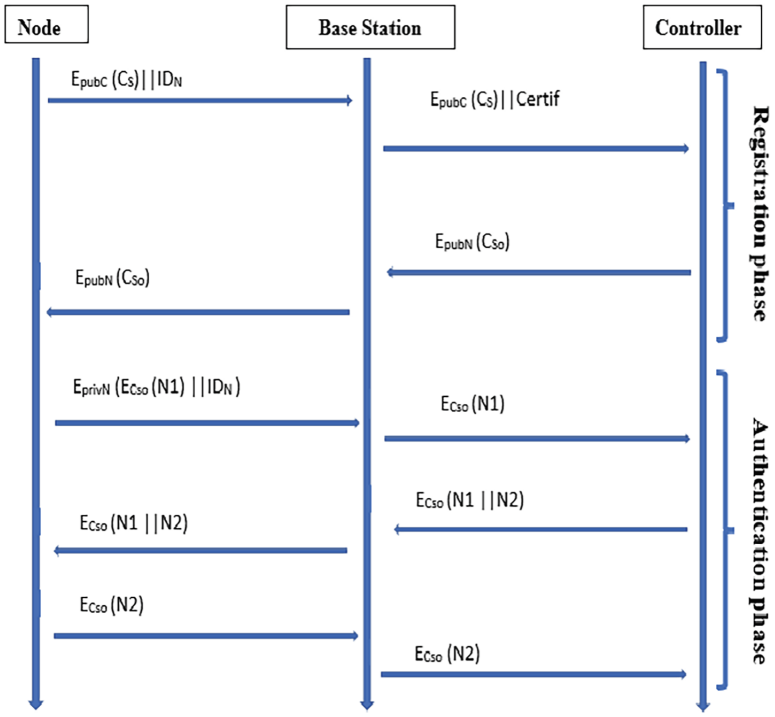

Fig. 1. Authentication system

4.1 Safety Analysis

This analysis is based on certain security constraints defined in WSN: access control, confidentiality and authentication.

Access control: the solution we propose prevents any element outside the system from accessing the network. For a node N wishing to join the network, it must necessarily go through a process of authentication and confidential data exchange. In our case, node N must send its authentication data to the controller via the base station. This authentication data is integrated into each node before it is deployed. If node N hasn't this authentication data, access control will fail and it will not be able to integrate into the network.

Confidentiality: this guarantees that information from a sensor node is only made accessible or revealed to its intended recipient. Our authentication system also ensures the confidentiality of authentication data exchanged between the node and the controller. Nodes have their own preliminary keys, such as the controller's public key, the base station's symmetrical key and their own public and private keys. When a node I wants to authenticate itself to the controller, it sends its authentication data encrypted with the corresponding public key. This mechanism guarantees the confidentiality of authentication data.

Authentication: our solution ensures the authentication of every node wishing to communicate in the network. The identity of each node is verified by the base station, and final authentication takes place at the controller. The elliptic curve parameters are

used to generate unique keys for each node. These keys are used during the authentication process to ensure effective security.

4.2 Security Against Known Attacks

The different characteristics of WSNs expose them to numerous security threats [20, 21]. Denial of service and impersonation attacks are easier to carry out in this type of wireless, infrastructure-free network. In this section, we evaluate the security of our protocol against a few types of attack.

Attacks such as spoofing, modifying or replaying routing information fail against our protocol if the content of messages exchanged in the network is unknown. In our protocol, an attacker must not be able to usurp the identity, the public keys embedded in a node, or the values of the elliptic curve parameter. Since the usurpation of all this information is complex, our protocol offers an acceptable level of security against these types of attacks.

The proposed protocol is also resistant to sybil attacks, thanks to the verification of node identity by the base station. The nonces generated from the elliptic curve parameters remain secret and are transmitted securely between the node and the controller. It is very difficult to carry out such an attack against this protocol, if you don't know the random values generated by the node and controller.

5 Conclusion

With the rapid development of the Internet of Things (IoT), SDN technology is attracting increasing attention from researchers. Its centralized control improves device management efficiency and security. In this article, we have proposed a lightweight authentication system to combat identity theft attacks such as the sybil attack. This protocol is based on elliptic curve cryptography, which is an asymmetric encryption system that consumes less energy than others. In this contribution, a controller is responsible for managing and authenticating network nodes.

References

1. Gite, P., Chouhan, K., Murali Krishna, K., Kumar Nayak, C., Soni, M., Shrivastava, A.: ML based intrusion detection scheme for various types of attacks in a WSN using C4. 5 and CART classifiers. Mater. Today Proc. **80**, 3769–3776 (2023). https://doi.org/10.1016/j.matpr.2021.07.378
2. Numan, M., et al.: A systematic review on clone node detection in static wireless sensor networks. IEEE Access **8**, 65450–65461 (2020). https://doi.org/10.1109/ACCESS.2020.2983091
3. Lakshmi Narayanan, K., Santhana Krishnan, R., Golden Julie, E., Harold Robinson, Y., Shanmuganathan, V.: Machine learning based detection and a novel EC-BRTT algorithm based prevention of DoS attacks in wireless sensor networks. Wirel. Pers. Commun. **127**(1), 479–503 (2022). https://doi.org/10.1007/s11277-021-08277-7

4. Bala, P.M., Usharani, S., Abarna, V.: Detect the replication attack on wireless sensor network by using intrusion detection system. J. Phys. Conf. Ser. **1717**(1) (2021). https://doi.org/10.1088/1742-6596/1717/1/012023
5. Dhanaraj, R.K., Jhaveri, R.H., Krishnasamy, L., Srivastava, G., Maddikunta, P.K.R.: Blackhole attack mitigation in medical sensor networks using the enhanced gravitational search algorithm. Int. J. Uncertain. Fuzziness Knowl.-Based Syst. **29**, 297–315 (2021). https://doi.org/10.1142/S021848852140016X
6. Batna, D., Constantine, D., Batna, D.: Protocoles pour la Sécurité des Réseaux de Remerciements (2018)
7. Patel, S.T., Mistry, N.H.: A review: sybil attack detection techniques in WSN. In: Proceedings of 2017 4th International Conference on Electronics and Communication Systems, ICECS 2017, vol. 17, pp. 184–188 (2017). https://doi.org/10.1109/ECS.2017.8067865
8. Zhang, K., Liang, X., Lu, R., Shen, X.: Sybil attacks and their defenses in the internet of things. IEEE Internet Things J. **1**(5), 372–383 (2014). https://doi.org/10.1109/JIOT.2014.2344013
9. Newsome, J., Shi, E., Song, D., Perrig, A.: The Sybil attack in sensor networks: analysis & defenses. In: Third International Symposium on Information Processing in Sensor Networks, IPSN 2004, pp. 259–268 (2004)
10. Badetia, N., Hussain, M.: Distributed mechanism for authentication of nodes in wireless sensor networks. In: 2017 2nd International Conference for Convergence in Technology (I2CT), Mumbai, India, pp. 471–474 (2017). https://doi.org/10.1109/I2CT.2017.8226173
11. Furtak, J., Zielinski, Z., Chudzikiewicz, J.: Security domain for the sensor nodes with strong authentication. In: 2019 International Conference on Military Communications and Information Systems, ICMCIS 2019, no. D, pp. 1–6 (2019). https://doi.org/10.1109/ICMCIS.2019.8842766
12. Pinto, E.M.D.L., Lachowski, R., Pellenz, M.E., Penna, M.C., Souza, R.D.: A machine learning approach for detecting spoofing attacks in wireless sensor networks. In: Proceedings - International Conference on Advanced Information Networking and Applications, AINA, vol. 2018-May, pp. 752–758 (2018). https://doi.org/10.1109/AINA.2018.00113
13. Patil, S.D., Patil, K.K.: Provisioning authentication on demand in wireless sensor networks: PAW. In: 2018 6th Edition of International Conference on Wireless Networks & Embedded Systems, WECON 2018 - Proceedings, pp. 116–121 (2018). https://doi.org/10.1109/WECON.2018.8782063
14. Pathak, G.R., Edake, G.M., Patil, S.H.: Untraceability of sensor node authentication in wireless sensor networks. In: Proceedings - 2014 6th International Conference on Computational Intelligence and Communication Networks, CICN 2014, pp. 893–897 (2014). https://doi.org/10.1109/CICN.2014.188
15. Badetia, N., Hussain, M.: Distributed mechanism for authentication of nodes in wireless sensor networks. In: 2017 2nd International Conference on Convergence in Technology, I2CT 2017, vol. 2017-January, pp. 471–474 (2017). https://doi.org/10.1109/I2CT.2017.8226173
16. Vardhan, A., Hussain, M.: Dynamic and resilient protocol for mutual authentication of nodes in wireless sensor networks. In: 2017 International Conference on Advances in Computing, Communications and Informatics, ICACCI 2017, vol. 2017-January, pp. 2010–2015 (2017). https://doi.org/10.1109/ICACCI.2017.8126140
17. Mishra, A.K., Tripathy, A.K., Puthal, D., Yang, L.T.: Analytical model for sybil attack phases in internet of things. IEEE Internet Things J. **6**(1), 379–387 (2019). https://doi.org/10.1109/JIOT.2018.2843769
18. Al-Naeem, M.A.: Prediction of re-occurrences of spoofed ACK packets sent to deflate a target wireless sensor network node by DDOS. IEEE Access **9**, 87070–87078 (2021). https://doi.org/10.1109/ACCESS.2021.3089683